IT Policies

of

The Bihar State Cooperative Bank Ltd



IT Policies

The Bihar State Cooperative Bank Ltd

Ashok Rajpath,
Patna - 800004, Bihar.

Version 1.0

The Bihar State Cooperative Bank Ltd

Document Details

Version: 1.0

Formulation Details

Checked / Vetted by:

1. IT Department
2. IT Steering Committee

Contents

1 Purpose 19
2 Objective 19
3 Scope 19
4 Policies 20
4.1 Email Policy 20
4.1.1 Roles and Responsibilities 20
4.1.2 Risk Assessment 20
4.1.3 Basic requirements of BSCB e-mail Service 20
4.1.4 Responsibilities of Offices 23
4.1.5 Security Incident Management Process 24
4.1.6 Intellectual Property 24
4.1.7 Enforcement 24
4.1.8 Deactivation 24
4.1.9 Audit of E-mail Services 25
4.2 Internet Usage Policy 26
4.2.1 Policy Statement 26
4.2.2 Objective Purpose 26
4.2.3 Scope 26
4.2.4 Internet access to users 29
4.2.5 Policy Dissemination 30
4.2.6 Enforcement 30
4.2.7 Deactivation 30
4.3 Business Continuity Plan Policy 31
4.3.1 Roles and Responsibilities 31
4.3.2 Need for Policy 31
4.3.3 Requirements for Business Continuity Plan 32
4.4 Program Change Management Policy 38
4.4.1 Roles & Responsibilities 38
4.4.2 Procedures 39
4.4.3 Annexure 44
4.4.4 Impact of Program Change Management Policy 46
4.5 Logical Access & Review of Access Rights Policy 46
4.5.1 Roles and Responsibilities 46

4.5.2	Scope	46
4.5.3	Purpose	47
4.5.4	Applicability	47
4.5.5	Standard-Request logical Access	47
4.5.6	Grant Logical Access	48
4.5.7	User ID Management	49
4.5.8	User Responsibility	50
4.5.9	Access Rights to User IDs	50
4.5.10	Review of access rights	51
4.5.11	Frequency	52
4.5.12	Deviations	52
4.5.13	Operational Policies	52
4.5.14	Annexures	57
4.6	**Technology Refresh Policy**	**58**
4.6.1	Roles and Responsibilities	58
4.6.2	Purpose:	58
4.6.3	Policy Statement:	58
4.6.4	Definitions:	59
4.6.5	Standardization of Technology	59
4.6.6	Staggered Refresh	60
4.7	**Backup & Recovery Policy**	**61**
4.7.1	Roles and Responsibilities	61
4.7.2	Back-up of Data at Data Centre	61
4.7.3	Operational Policies	62
4.8	**Disaster Recovery Policy**	**67**
4.8.1	Roles and Responsibilities	67
4.8.2	Strategic Objectives of DRP	67
4.8.3	Relationship between Business Continuity and Disaster Recovery Plans	68
4.8.4	Disaster Recovery Plan: Key Components	68
4.8.5	Backup/Data Recovery	70
4.8.6	Maintenance and Testing	71
4.8.7	Recovery Strategy	74
4.8.8	Transition / Migration Back to the normal IT production environment	81
4.8.9	Vendor BCP	83
4.8.10	Operational Policies	84

4.9	**Hardware Acquisition, Maintenance & Upgradation Policy**	93
4.9.1	Roles and Responsibilities	93
4.9.2	Hardware Categorization	93
4.9.3	Capacity Planning	93
4.9.4	Environmental checks	95
4.9.5	Acquisition of Hardware	96
4.9.6	Disposal of IT Assets	98
4.9.7	Management and Operation of IT Assets	101
4.9.8	Annexure	107
4.10	**Incident Management Policy**	108
4.10.1	Roles & Responsibilities	108
4.10.2	Risk Assessment	108
4.10.3	Punitive Action for Violation	108
4.10.4	Operational Policies	109
4.10.5	Annexures	115
4.11	**License Management Policy**	118
4.11.1	Roles and Responsibilities	118
4.11.2	Operational Policies	118
4.11.3	Annexure	122
4.12	**Procurement Policy**	122
4.12.1	Methodology	122
4.12.2	Sundry Purchases	130
4.12.3	Procurement Procedure	130
4.12.4	Tendering Process	132
4.12.5	Identification & Disposal of Obsolete Equipment	137
4.12.6	Amendment Authority	138
4.12.7	Electronic Tender	138
4.13	**Version Control Policy**	139
4.13.1	Roles and Responsibilities	139
4.13.2	Version Management Functionality & Processes	139
4.13.3	Operational Policies	140
4.14	**Virus Protection Policy**	144
4.14.1	Roles & Responsibilities	144
4.14.2	Risk Assessment	144
4.14.3	Purpose	144

4.14.4 Scope 144
4.14.5 Procedures 145
4.15 ATM Policy 149
4.15.1 Policy Statement 149
4.15.2 Scope 149
4.15.3 Introduction: 149
4.15.4 Micro ATMs: - 149
4.15.5 Deployment Strategies: 150
4.15.6 Minimum Configuration 150
4.15.7 Multi-Lingual Screens 150
4.15.8 Site Security 151
4.15.9 Storage of Journal Print & Electronic Journal (EJ) Log 151
4.15.10 Provision of DVR / CCTV camera and storage of footage / images 151
4.15.11 ATM Monitoring 151
4.15.12 ATM Hardware Related Product Enhancements & Upgrades 151
4.15.13 Acquiring Policy 151
4.15.14 Networking / Connectivity of CDs/ATMs 152
4.15.15 On-Us ATM Transactions & Services at BSCB ATMs 152
4.15.16 Remote-On-Us (Issuer transactions) & Not-On-Us (Acquirer transactions) 152
4.15.17 Grouting of ATMs/Cash Recycler and other security norms 153
4.15.18 Robbery 153
4.15.19 Insurance 153
4.15.20 ATM Maintenance Service 154
4.15.21 Replacement of Machine / up-gradation with Biometric functionality and Chip card reader 154
4.15.22 Cassette Swap System 154
4.15.23 ATM Switch 154
4.15.24 Grievance Redressal: 154
4.15.25 Regulatory & Supervisory Issues 154
4.16 Debit Card Policy 155
4.16.1 Policy Statement 155
4.16.2 Scope 155
4.16.3 Debit Card 155
4.16.4 Personal Identification Number (PIN) 155
4.16.5 Types of Debit Cards 156
4.16.6 Eligibility for Issuance of Debit Cards 156

4.16.7	Responsibility of Bank	157
4.16.8	Responsibility of Cardholder(s)/Customers	157
4.16.9	Transaction Limit & Other Charges	158
4.16.10	Security and other aspects	158
4.16.11	Lost or Stolen Card	159
4.16.12	Issuance of Duplicate Cards on account of lost or Damaged	159
4.16.13	Issuance of Cards to Joint Accounts	159
4.16.14	Inventory management of cards	159
4.16.15	Prospective	160
4.16.16	Compliance to regulatory norms	160
4.17	**Data Retention & Archival Policy**	**160**
4.17.1	Data retention policies	160
4.17.2	The Importance of Data Retention Policies	161
4.17.3	Purpose	161
4.17.4	Scope	161
4.17.5	Acceptable Use	162
4.17.6	Place of Storage	163
4.17.7	Reference/Indexing	163
4.17.8	Procedure to be followed for storage, Retrieval and purging of old records	163
4.17.9	Regulatory Compliance	164
4.17.10	Data Restoration	165
4.17.11	Data categorization	165
4.17.12	Policy Review	165
4.17.13	Data Archival	165
4.17.14	Violations and Penalties	165
4.17.15	Records Management	165
4.17.16	Different types of information storage	167
4.17.17	Data Retention Period: --	176
4.18	**Data Migration Policy**	**178**
4.18.1	Introduction	178
4.18.2	Scope	178
4.18.3	Terms and Definitions	179
4.18.4	Roles and Responsibilities	179
4.18.5	Factors for consideration	179
4.18.6	Requirements for Effective Data Migration	180
4.18.7	Data Migration Life Cycle	180

4.18.8	Data Migration Strategy	180
4.18.9	Data Migration Approaches	183
4.18.10	Data Migration Process	183
4.18.11	Testing Strategy	185
4.18.12	Rollback & Reconciliation	186
4.18.13	Important point related to Data Migration	186
4.19	**Social Media Policy**	**187**
4.19.1	Introduction & Need for a Policy	187
4.19.2	Policy Statement	188
4.19.3	Who is covered by the Policy?	188
4.19.4	The Scope of the Policy	189
4.19.5	Using Work-related Social Media	189
4.19.6	Account Information/ Transaction Processing using Social Media Apps	189
4.19.7	Personal Use of Social Media Sites	189
4.19.8	Rules for Use of Social Media	190
4.19.9	Social Media Tips	191
4.19.10	Monitoring Use of Social Media Websites	192
4.19.11	Monitoring and Review of this Policy	193
4.20	**IT Skillset Development Policy**	**193**
4.20.1	Purpose	193
4.20.2	Objective	193
4.20.3	Roles & Responsibilities	193
4.20.4	Training Segments	194
4.20.5	Types of Training	194
4.20.6	Sanctioning Authority for IT Trainings	195
4.20.7	Strategic Areas identified for Training	195
4.20.8	Motivating employees to undergo IT Certifications	196
4.20.9	Center of Excellence	197
4.20.10	Outcome and benefit of IT Skill Development/training	197
4.21	**Mobile Banking Policy**	**198**
4.21.1	Policy Statement	198
4.21.2	Scope	198
4.21.3	Bank's responsibility	198
4.21.4	Registration of customers for mobile service	199
4.21.5	Technology and Security Standards	199
4.21.6	Inter-operability	199

4.21.7	Authentication	199
4.21.8	Eligibility for Mobile Banking:	200
4.21.9	Usage of Facility	200
4.21.10	Customers Responsibility	201
4.21.11	Fees	201
4.21.12	Termination of BSCB Mobile Banking Service	201
4.21.13	Grievance Redressal	202
4.21.14	Regulatory & Supervisory Issues	202
4.21.15	Amendment of the Policy	202
4.21.16	Disclaimer	202
4.22	**Internet Banking Policy**	**203**
4.22.1	Policy Statement	203
4.22.2	Scope	203
4.22.3	Introduction	203
4.22.4	Eligibility	203
4.22.5	Services Offered through Internet banking	204
4.22.6	Responsibility of Bank	205
4.22.7	Responsibility of Customer	205
4.22.8	Online Registration and password reset facility to retail customers	206
4.22.9	Customer Account blocking	206
4.22.10	Terms And Conditions	206
4.22.11	Termination of facility	207
4.22.12	Hyperlinks To and From Bank's Website	207
4.22.13	Two Factor Authentication System	207
4.22.14	Grievance Redressal	208
4.22.15	Transaction Limit Enhancement	208
4.22.16	Regulatory & Supervisory Issues	208
4.23	**Cloud Computing Policy**	**209**
4.23.1	Introduction	209
4.23.2	Scope	209
4.23.3	Guidance	209
4.23.4	Other Concerns to be addressed	210
4.23.5	Cloud deployment model and Cloud service usage	210
4.23.6	Selecting the cloud service provider	211
4.24	**Outsourcing of IT Technology**	**212**
4.24.1	Introduction	212

4.24.2	Objectives	212
4.24.3	Policy Framework	212
4.24.4	Activities to be Outsourced	212
4.24.5	Prohibited Outsourcing Activities	213
4.24.6	Legal obligations and regulatory and supervisory requirements	213
4.24.7	Management of Risk	214
4.24.8	Evaluation of the Risks	214
4.24.9	Liabilities of Principal employer	215
4.24.10	Appraisal of Service Provider	215
4.24.11	Evaluating the capability of Service provider	215
4.24.12	Materiality of outsourcing	216
4.24.13	The Outsourcing Agreement	217
4.24.14	Confidentiality and Security	217
4.24.15	Business Continuity and Management of Disaster Recovery Plan	217
4.25	**Policy for Amendment**	**222**
4.25.1	Introduction	222
4.25.2	Roles and Responsibilities	222
4.25.3	Procedure	222
4.25.4	Annexure	223
4.26	**IS Audit Policy and Procedures**	**224**
4.26.1	Introduction	224
4.26.2	Scope of Audit	224
4.26.3	Responsibilities of the owner of the business process	225
4.26.4	Reporting	226
4.26.5	Information System Audit Methodology	227
4.26.6	Framework for Conducting IS Audit	231
4.26.7	Standard Guidelines for IS Audit	238
4.26.8	Type of Audit Evidence/Information	252
4.26.9	Audit Documentation	255
4.27	**VPN Access and Remote Working Policy**	**257**
4.27.1	Introduction	257
4.27.2	Scope	257
4.27.3	Responsibility	258
4.27.4	Operating Guidelines	258
4.28	**IT Security Policy**	**260**

4.28.1	Policy Statement	260
4.28.2	Objective Purpose	260
4.28.3	Scope	260
4.28.4	Information Classification	261
4.28.5	Access Control	262
4.28.6	Data Protection	262
4.28.7	Password Management	264
4.28.8	Network Security	265
4.28.9	Physical Security	266
4.28.10	Incident Response	266
4.28.11	Security Awareness Training	266
4.28.12	Vendor Management	267
4.28.13	Compliances and Auditing	267
4.28.14	Review and Updates	268
4.28.15	Document Control	268
4.28.16	Training and Awareness	268

Definitions and Abbreviations

BSCB	THE BIHAR STATE CO-OPERATIVE BANK LTD. (hereinafter referred to as" BSCB", or "the organization" or "organization")
Bank	The Bihar State Co-operative Bank Ltd. or any successor or assign of it.
Functional Head	This term refers to the Team Head / Department / Division / Unit head who owns the project / process.
Group Leader	This term refers to the head of the team/department / Division / Unit who is the owner of the project / process.
Memory Leaks	The phenomena of programs not releasing memory after termination of processes invoked by them. Memory Leaks cause the program to abort when it runs short of memory.
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold
OEM	Original Equipment Manufacturer
SOC	Security Operations Center
Port Scan	Port Scanning is the technique used to identify open ports and services available on a network host

Malicious attacks	An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other intentionally harmful programs
Denial of Service	A type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
Sniffing	Unauthorized capture or interception of data travelling through the network
IPS	Intrusion Prevention System
IT	Information Technology
DC	Data Center
DRC	Disaster Recovery Center
WAN	Wide Area Network
NOC	Network Operations Center
LAN	Local Area Network
SAN	Storage Area Network
OS	Operating Systems
SOP	Standard Operating Procedure
SLA	Service Level Agreement
DDoS	Distributed Denial of Service
UTM	Unified Threat Management
Active Attacks	It is a network attack in which a hacker attempts to make changes to data on the target or data end route to the target.
Passive Attacks	It is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities but does not affect system resources.
SYN Flooding	It is a type of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic
ICMP	Internet Control Message Protocol
OEM	Original Equipment Manufacturer
IMAC	Install, Move, Add and Change
DMS	Document management System
Pre-shared Key	The Pre-shared Key or the Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) is a security mechanism used to authenticate and validate users on a wireless LAN (WLAN) or Wi-Fi connection. WPA-PSK works by configuring a WLAN passphrase or password of eight to 63 characters. Based on the password, access point (router) and connecting node credentials, a 256-character key is generated,

	shared and used by both devices for network traffic encryption and decryption. A connected user that provides correct credentials receives WLAN access.
Encryption -Decryption Algorithm	A mathematical procedure for performing encryption on data. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form (decryption).
Computer Virus	Acomputervirusisanunauthorizedandmaliciousprogram,whichreplicatesitselfand spreadsontovariousdatastoragemedia such as, magnetic disk, tapes, Thumb/Flash drive, External Hard drive, SD/Memory card andacrossthenetwork.Thevirusesaredesignedtospreadfromonefiletoanother,fro moneprogramtoanother,fromonemachinetoanother,andevenfromonenetworkt oanother.Virusesthreatentheintegrityandavailabilityofdata.Thesymptomsofvirus infectionincludeconsiderablyslowerresponsetimefromthesystem,inexplicablelos sofdata,erroneouschangeinfiledates,increase or decrease in file size or total failure of computer system.
Virus Signature	The unique pattern of virus activity is known as virus signature.
DAT files	These are the files, which contain the data on virus signatures.
Access Control	It is the process that limits and controls access to resources of a computer system.
System or Application Accounts	They are user IDs created on IT systems or applications, which are associated with specific access privileges on such systems and applications.
Account(s)	"Account(s)" shall mean any one or more accounts held and/or facilities provided to the Customer by BSCB including but not limited to savings accounts, current accounts, term deposits or such other accounts and/or facilities as may be determined by BSCB from time to time, for which the Facility is being offered or may be offered in future.
Alert(s)	This means the customized messages sent to the Mobile Phone Number as an SMS in response to the triggers set by the customer.
Alert/Push Facility	This means the service provided by BSCB wherein a customer can obtain specific information to the customer's Account on the customer's mobile phone number.
BSCB Contact Number	This refers to the number/s provided by BSCB to its Customers for availing of Request/Pull Facility or such other facilities which may be availed of through the BSCB Contact Number, as communicated by BSCB from time to time.
Service or Facility	This means mobile banking facility (which provides the Customers, services such as information relating to Account(s), details about transactions and such other services as may be provided on the Mobile Phone Number by BSCB, from time to time.
Registered Mobile Number	This means the number registered/provided by the Customer in writing (either through a printed form provided by BSCB or otherwise), or through ATM, website, through call center, for the purpose of availing the Facility.

Access Privileges	They are system permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.
OS	Operating System
Account	an account with BSCB
Customer	holder of an Account in BSCB
MPIN	Personal Identification Number (password) for the Mobile app Service.
TPIN	Transaction PIN for the Mobile app Service
OTP	One Time Password for the Mobile app Service.
IMPS	This means the Immediate Payment Service of NPCI offered by the Bank to its customers who are eligible for Mobile Banking Service of the bank and who are agreeable to the term and conditions of mobile banking set out herein.
UPI	Unified Payments Interface of NPCI.
NEFT	National Electronic Fund Transfer system of RBI.
RTGS	Real Time Gross Settlement System of RBI.
RBI	Reserve Bank of India
NABARD	National Bank for Agriculture and Rural Development.
Website	This refers to www.BSCB.in or any other website as may be notified by BSCB.
Personal Information	This means the information about the Customer obtained in connection with the Facility.
SMS	This means the Short Messaging Service, which is the transmission of short text messages to and from SMS enabled devices including but not limited to mobile phones.
MAS	Mobile Application Service of the organization.
Mobile Phone	A compatible handset along with the accessories and necessary software for GSM phones and handsets and software for CDMA phones, which is owned by the mobile subscriber.
Mobile Banking app	This means the mobile banking application which can be installed on the mobile phone handset to access information pertaining to the Account(s).
MBS	Mobile Banking Service of the Bank and includes the service over the application / USSD / WAP / SMS Banking.
WAP	Wireless Application Protocol
System Administrators	Thistermreferstothesystemadministratorsoftherespectivesystems/applications of BSCB.
IT Technical Team Leaders	IT Technical Team Leaders are responsible for managing & monitoring the following services processes: • Setting backup schedules for existing & new systems

	• Managing a backup failure • Maintaining the backup log • Restoration of Data and files Liaising with system administrators, information asset administrators on agreeing and reviewing backup & recovery strategies
Information Security Officer	He is responsible for providing support and advice on information governance and information security over the Guideline, supporting procedures and backup/recovery strategies
DC	Data Center
DRC	Disaster Recovery Center
EOD	End of Day
DRP	Disaster Recovery Plan
BCP	Business Continuity Plan
Incident	'Incident' is a term related to exceptional situations or a situation that warrants intervention of senior management. This may be result of unusual circumstances as well as the violations of existing guidelines and procedures of BSCB. An incident may relate to any of the following: • Attempts (either failed or successful) to gain an unauthorized access to a system or its data • Internet fraud or fishing • Loss of information due to unknown reasons • Hardware resources and components lost / stolen • Virus incidents pertaining to e-mail, internet, cd, diskette and others • Threat to physical safety of human beings. • Attacks originating from BSCB's network • Threats, harassment, and other criminal offenses involving individual user accounts. • Compromise of individual user accounts on multi-user systems. • Forgery and misrepresentation, and other security-related violations of local rules and regulations. • Compromise of desktop systems.
Incident Handling &Response	It refers to the set of actions taken to protect and restore the normal operating condition of computers and the information residing in it, when an adverse event or incident occurs. It involves contingency planning and contingency response.
Intrusion	It refers to an event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them.

Chain of Custody	It refers to verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and time. For a proven chain of custody to occur, the evidence is accounted for at all times.
Constituency	It is the group of users, sites, networks or organizations served by the Computer Security Incident Response Team (CSIRT).
Incident Response Team (IRT)	The IRT is a team of highly skilled personnel, designated by BSCB's Board, who are responsible for responding to computer security incidents.
Computer Security Incident Response Team (CSIRT)	A CSIRT is a team that coordinates and supports the response to security incidents that involves sites within a defined constituency. In order to be considered a CSIRT, a team must: • Provide a (secure) channel for receiving reports on suspected incidents. • Provide assistance to members of its constituency in handling these incidents. • Disseminate incident-related information to its constituency and to other involved parties. Note that no reference is being made to police or other law enforcement bodies which may investigate computer-related crime. CSIRT members, indeed, need not have any powers beyond those of ordinary citizens.
ISM	Information Security Manager
Recovery Point Objective (RPO)	Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance."
Recovery Time Objective (RTO)	The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.
OEM	Original Equipment Manufacturer
OSD	Original Software Developer
ACP	Authorized Channel Partner
AD	Authorized Dealer
PSE	Public Sector Enterprise
RFP	Request for Proposal
CEO	Chief Executive Officer
PBTD	Pre-Bid Technical Discussion
TPET	Tender Planning and Evaluation Committee
ITPAC	IT Purchase Approval Committee
EC	Eligibility Criteria

Functional Head	This term refers to the Team Head/Department head who owns the project/process, which in this case refers to the Heads of respective divisions / departments.
Project Leader	This term refers to the head of the team/department who is the owner of the project/process, which in this case refers to the Chief Officer/ AGM / GM – IT Division
System Administrator	This termreferstothesystemadministratorsoftherespectivesystems/applications of the organization.

1 Purpose

The Bihar State Cooperative Bank Ltd.(hereafter referred to as "BSCB" or "the organization" or "organization") has laid down the IT Policies so as to clearly highlight the framework and policies to be followed by BSCB employees, clients and customers wherever applicable.

2 Objective

All application systems and processes that are part of the BSCB must follow the operational policies mentioned in this document and the smooth running of the processes needs to be monitored by the personnel mentioned in each individual Policy.

3 Scope

This Policy applies to all its IT employees, respective Outsourced Parties and customers. The information resources covered under this Policy includes system and application software, servers, desktops, and network / security components.

4 Policies

4.1 Email Policy

4.1.1 Roles and Responsibilities

ROLE	RESPONSIBILITIES
Owner	
Custodian & Supervision	
Monitoring	
Implementation	

4.1.2 Risk Assessment

THREAT	IMPACT	LIKELIHOOD
Downloading of virus, worms, and Trojans via e-mail attachments	High	High
Compromise of sensitive data transmitted via e-mail	High	High
Harassment caused to others due to improper use of official e-mail ID (includes sending pornographic content, spam mails, chain letters that are not of official / organizational relevance)	Low	Low
Use of Office e-mail to spread rumors, hoaxes and fake terrorist threats.	Medium	Low

4.1.3 Basic requirements of BSCB e-mail Service

4.1.3.1 Security

a. Considering the security concerns regarding a sensitive deployment like e-mail, apart from the service provided by the IT division, there shall not be any other e-mail service under BSCB.

b. BSCB's E-mail access shall be given to users as per the access policy.

c. Vendor cannot access BSCB's domain email unless authorized by Manager(IT) /GM(IT) /DGM (IT) in writing.

d. Users shall have to adhere to E-Mail access policy as defined in this document.

e. Every user shall be provided with a fixed quota of disk space for email purpose.

f. Users shall not be allowed to send / receive emails as soon as mail file size exceeds the fixed quota. User shall archive / delete emails from the server to prevent the mail file size exceeding the fixed quota.

g. The maximum file size for email attachments shall be restricted to fixed size.

h. E-mail content filtering mechanism shall be deployed at gateway level.

i. E-mail content filtering reports shall be monitored by the Administrator and any significant violation shall be reported to the IT Manager/ DGM / AGM / Chief Officer.

j. All e-mails shall carry the standard BSCB footer banner.

k. Users shall not provide e-mails credentials of official e-mail account, configured on the BSCB mail server to any other e-mail service provider/organization. This implies that users should not provide their BSCB e-mail account details (id and password) of their accounts on private e-mail service providers/ any other organization.

l. Users shall not download e-mails from their official e-mail account, configured on the BSCB mail server, by configuring POP (protocol that allows downloading messages from inbox to local computer) on any public computer like internet café etc.

m. User shall not download or upload executable files (.exe) or any restricted extensions files from their official e-mail account.

n. Any official email id shall not be redirected manually or automatically to any other email address of any other domain.

o. The DGM / AGM / Chief Officer DGM / AGM / Chief Officer Division of BSCB shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User.

p. In case a spam email is generated from an e-mail id and is detected by the System Administrator, the System Administrator reserves the right to reset the password of that e-mail id under intimation to the DGM / AGM / Chief Officer DGM / AGM / Chief Officer Division.

q. In case of a situation, when spam email is generated from an e-mail id impacts a large user base or the data security of the deployment, the System Administrator shall deactivate that e-mail id

temporarily. This action shall be taken on an immediate basis, and the information shall be provided to the user and the office subsequently.

r. Official e-mail id provided by the IT Division can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

s. All users accessing the e-mail services must use strong passwords for security of their e-mail accounts. More details about the password Guideline are available in "Password Security and Control Policy".

t. Users should ensure that e-mails are kept confidential. Users must ensure that information regarding their password or any other personal information should not be revealed to anyone.

4.1.3.2 E-mail Account Management

a. Email ID is being provided to all Departments, Branches, corporate offices of BSCB and employees for official purpose.

b. Email id will be active for a maximum for one month after retirement or leaving the organization or by the order of the competent authority. Human Resource Management Division will communicate with IT division with regards to archiving of data or to delete or inactive the Email account after retirement, resignation, suspension, or termination of the employee.

c. For common email id and password in the name of office, department, branch etc. shall share amongst concern officials and maintain record. The common email id shall be configured for sending, receiving & viewing only.

d. It is to be noted and is strongly recommended that no emails should be deleted or removed from the common email ID.

e. If the department is using multiple email ids, it may be reviewed periodically for proper usage of email service.

f. Individual mail quota shall not exceed 30 GB and it is the responsibility of the user to seek assistance from IT support to archive files locally in their machine.

g. In case of investigation against an individual due to infringement of BSCB's service rule or otherwise determined by the BSCB's management, all electronic forensic evidential log will be disclosed without prior concern of the individual

4.1.3.3 Email Services & Usage Guidelines

a. External Mass Mailing: BSCB, with prior approval from competent authority and using third party application may send mass mails informing the existing and potential customer's email id, information about the organization, launch of new products and services, and such other matters that may be helpful in development of business of BSCB. Third party application is mandatory for external mass mailing solution. The electronic mailing list of BSCB including that of its customers and vendors will not be distributed to third parties for commercial purposes without the approval of the competent authority and the concerned of customer and vendor.

b. Disclaimer: All e-mail originating from the BSCB automatically added disclaimer as mentioned below. Do not append any other disclaimer manually.

**********Disclaimer**********

The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this e-mail and then delete it from your system. BSCB is neither liable for the proper and complete transmission of the information contained in this communication nor for any delay in its receipt. The opinions expressed in the e-mail may not be the opinion of BSCB. "

4.1.4 Responsibilities of Offices

4.1.4.1 Guideline Compliance

a. All Departments, Branches of BSCB and Employees shall implement appropriate controls to ensure compliance with the e-mail Guideline by their users.

b. All corporate department/offices shall ensure resolution of all incidents related to the security aspects of the e-mail Guideline. IT division shall give the requisite support in this regard.

4.1.4.2 Guideline Dissemination

a. User should ensure dissemination of the e-mail Guideline.

b. Orientation programs for new recruits shall include a session on the e- mail Guideline.

4.1.5 Security Incident Management Process

a. A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality, and authority of data. Security incidents can be due to factors like malware, phishing, loss of a device, compromise of an e-mail id etc.

b. It shall be within the right of the IT division to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

c. Any security incident noticed or identified by a user must immediately be brought to the notice of the IT Division.

4.1.6 Intellectual Property

Material accessible through e-mail service and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the email service and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

4.1.7 Enforcement

This "E-mail Policy" is applicable to all Departments, Regional Offices, branches.

Each office shall be responsible for ensuring compliance with the provisions of this Policy. ICT division would provide necessary technical assistance to the organizations in this regard.

4.1.8 Deactivation

In case of threat to the security of BSCB service, the email id being used to impact the service may be suspended or deactivated immediately by the IT division.

After deactivation, the concerned user and the competent authority of that respective office shall be informed.

4.1.9 Audit of E-mail Services

The security audit of BSCB email services shall be conducted periodically by certified IS Auditor at BSCB.

4.2 Internet Usage Policy

4.2.1 Policy Statement

Internet connectivity in an organization introduces new risks that must be addressed to safeguard the information assets. These risks include access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or surfing the Internet. Additionally, the Bank may face loss of reputation and possible legal action through other types of misuse. Further, the recent spate of cyber-attacks on financial institutions shows that the use of internet in high impact areas is fraught with risk. RBI guidance on cyber security has also cautioned the banks on the need to strengthen cyber security.

Accordingly, access to the Internet at workplace through bank's WAN/LAN will be provided only to approved personnel to support business activities and strictly on need-to-have basis to perform their jobs and professional roles.

4.2.2 Objective Purpose

The purpose of this policy is to define the appropriate uses of the Internet by employees.

4.2.3 Scope

This Policy applies to all Internet users (employees of the Bank and individuals working for the Bank including permanent contract workers, business partners and vendors) who access the Internet through the bank's computing or networking resources. The Bank's Internet users are expected to be familiar with and to comply with this policy.

4.2.3.1 Internet Services Allowed

Internet access is to be used for official and business purposes only. Access to the following standard Internet services will be provided to users as needed:

a. Only Corporate E-mail Send/receive E-mail messages to/from the Internet (with or without document attachments). Webmail services such as Gmail, Yahoo, Rediff Hotmail etc., will not be allowed through the bank's network.

b. General Browsing-- WWW services as necessary for business purposes, Will be allowed only in exceptional cases, through a centralized proxy. Users need to get approval from **CISO's Office** in this regard prior to its access. Hypertext Transfer Protocol service will be allowed only for secured pages(https).

c. Secure File Transfer Protocol (SFTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes to a dedicated SFTP server between pre-approved counterparties and bank.

d.Secured, encrypted Telnet (SSH)-- Secure Internet protocol for terminal emulation will be allowed on a case-by-case basis only for limited time. User Strong Authentication required for Internet initiated contacts into the Bank from pre-approved IP Addresses and named support personnel.

Management reserves the right to add or delete services as business needs change or conditions warrant.

All other services including chatting, surfing in social media sites, downloading media files, viewing streaming media, peer to peer downloading, etc. will be considered unauthorized access to/from the Internet and will not be allowed except for IT, Digital Marketing, Corporate Communication,
Customer Service Support (Strategic Planning) department.

4.2.3.2 Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Information Security Policy. The user must then sign the statements that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

4.2.3.3 Acceptable use

a. Access to the Internet is specifically limited to activities in direct support of official / business purpose.

b. In addition to access in support of specific work-related duties, the Internet connection may be used for limited study, educational, development and research purposes.

c. Communication between employees and non-employees for business purposes.

d. IT technical support downloading software upgrades and patches.

e. Review of possible vendors web sites for product information.

f. Reference regulatory or technical information.

Installation of antivirus & regular anti-virus definition update is a must in PCs with internet.

4.2.3.4 Personal Usage

Using Bank computer resources to access the Internet for personal purposes, without approval from the Head of the Branch /Office /department, may be considered cause for disciplinary action. All users of the Internet should be aware that the Bank network creates an audit log reflecting request for service, both in-bound and outbound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, debit/credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The Bank is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

4.2.3.5 Inappropriate use

a. The Bank, Internet access shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials, including visiting peer-to-peer file sharing torrent sites.

b. The Bank, Internet access shall not be used for private, recreational or other non-Bank related activity.

c. The Bank Internet connection shall not be used for commercial or political purposes.

d. Use of the Bank's Internet access shall not be used for personal gain such as selling access of Bank information. Internet access shall not be used for or by performing work for profit with Bank resources in a manner not authorized by The Bank.

e. User shall not attempt to bypass security measures on the Bank's network resources or any other system connected to or accessible through the Internet.

f. User shall not use Internet access for interception of network traffic for any purpose unless engaged in authorized network administration.

g. User shall not make or use illegal copies of copyrighted material, store such copies on Bank equipment, or transmit these copies over the Bank network.

h. Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

i. Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.

j. Downloading videos, songs, unauthorized software.

k. Any ordering (shopping) of items or services on the Internet, playing of any games, Forwarding of chain letters, Participation in any on-line contest or promotion, Acceptance of promotional gifts.

l. Try to access unauthorized site without any permission using anonymous proxies or other means.

4.2.4 Internet access to users

a. Bank's IT Department shall provide internet connection through centralized proxy server.

b. Firewall rules need to be dovetailed with the policy approach related to the use of proxy.

c. If the above is not available then, Standalone PC can be allowed internet connection at branches/corporate offices only after approval from head office. However, internet access at numbers of PCs may vary office to office after getting approval from next higher authority of that office.

d. Using both CBS (Intranet) and internet in same machine through dual network connection is totally prohibited. Violation of this could be subject to disciplinary action.

e. IT officials with privileged access rights as System Admins, DBA, Network administrators etc., shall not be provided with internet access from the systems used for accessing servers, databases and network devices, the risk is the greatest.

f. Internet access may be provided to users to support business activities and only as needed to perform their jobs and approval from higher authority.

g. Security related clearance should be obtained from the CISO for allowing internet access by whitelisting of any new website/portal.

h. CAPTCHA should be used for internet facing portals

i. Although the systems accessing Internet are routed through proxy servers, the entire chain of connecting nodes have to be regularly checked for malwares and kept updated with latest anti-virus protection.

j. All systems having access to Internet need to be checked for viruses, malware, cookies, unauthorized software etc., frequently, at least once in two months.

4.2.5 Policy Dissemination

a. User should ensure dissemination of the Internet usage policy.

b. Orientation programs for new recruits shall include a session on the Internet usage policy.

4.2.6 Enforcement

This policy is applicable to all Departments of Head Office, Zonal Office, Branches, and Employees. The Chief Officer/AGM/ Manager(IT) recommending approval for internet access to an employee shall be primarily responsible for the employee's use or misuse of the facility. Each corporate office shall be responsible for ensuring compliance with the provisions of this policy. IT would provide necessary technical assistance to the organizations in this regard.

4.2.7 Deactivation

a. In case of threat to the security of the Bank service, the internet used to impact the service may be suspended or deactivated immediately by the Head of the Branch/Office / Department.

b. Subsequent to deactivation, the concerned user and the competent authority of that respective office shall be informed.

4.3 Business Continuity Plan Policy

4.3.1 Roles and Responsibilities

Role	Responsibilities
Owner	**IT Committee**/IT Department
Implementation	The AGM-IT of BSCB will be the owner of the Policy.
Monitoring & Supervision	The GM-IT of BSCB will monitor the implementation of the procedures detailed herein.

4.3.2 Need for Policy

Disaster is an unfavourable event and its aftermath, which adversely affects the normal functioning of a business location / unit, resulting in adverse financial and other impacts. Disasters may strike at the infrastructure that supports the business and related processes or a wider geographical area. Disasters have the potential of affecting normal functions over extended period of time.

To recover from the adverse effects of a disaster, BSCB should plan for an orderly recovery route by having Business Continuity Plan (BCP) in place.

A BCP should take an overall business perspective encompassing recovery activity spanning the entire business activities. A business continuity plan (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire or any other case where business is not able to occur under normal conditions.

When developing a BCP all threats that could cease regular business should be determined. The next step is to determine the most significant tasks required to continue operations. Who are the necessary people and what are the tools and information needed to continue operation?

A business continuity plan involves the following:

a. Analysis of organizational threats
b. A list of the primary tasks required to keep the organization operations flowing
c. Easily located management contact information
d. Explanation of where personnel should go if there is a disastrous event

e. Information on data backups and organization site backup

f. Collaboration among all facets of the organization

g. Buy-in from everyone in the organization

The approach to BCP should be from the business perspective.

4.3.3 Requirements for Business Continuity Plan

4.3.3.1 Business Impact Analysis (BIA)

A Business Impact Analysis must be performed in order to identify critical processing platforms and applications on the basis of their sensitivity and availability to assess the impact of a disruption on a business process or systems. BSCB will perform BIA annually in order to ensure an effective and timely recovery.

Every business is susceptible to risks associated with disasters. In the Business Impact Analysis phase, the management should identify the disasters that can potentially affect BSCB and assess the impact of the resulting down time. By the end of this phase, management should be in a position to decide which processes need to be protected and to what extent.

The stages involved to perform the Business Impact Analysis should include the following:

a. Perform Risk Assessment

In this stage, BSCB should identify all the possible risks that it can be subjected to. It can vary from natural to manmade and from infrastructure related to sabotage. The impact of the disaster should be calculated in terms of potential loss of revenue and repute, also considering the probability of the adverse event occurring.

Actions to mitigate the risks identified in Risk Assessment Stage must be taken. The objective of risk mitigation should be to identify action steps and procedures that can be taken before a disaster strike. This will help to minimize the effects of an interruption which might occur.

b. Identify Critical Business Process

A critical business process is a business activity, which if interrupted or unavailable for a period, would significantly jeopardize the operation of the organization. If the critical business processes have already been determined, any additional business processes not included that are critical should be added and irrelevant ones should be eliminated. The business processes identified as critical will receive priority attention following a disruption.

While identifying the critical business processes, the financial and non-financial impact of the business processes should be considered in the event of failure.

c. Identify Interdependencies

For a critical business process to be properly recovered after a business interruption, it is necessary to understand what other business processes and/or functions the critical business process relies upon. In order to successfully recover a particular business process, any functions the critical business process relies upon may have to be recovered simultaneously. For example, if BSCB depends on WAN and MPLS provided by a service provider for its critical business activities, hence the WAN and MPLS should be identified as critical external interdependencies.

d. Determining Recovery Priorities and Time Frames

After all business processes and interdependencies have been identified, attention must be focused on those time-critical business processes requiring recovery as soon as possible, placing non-time-critical business processes at a lower priority for recovery. A recovery hierarchy of all critical business processes, illustrating the recovery order and recovery time frames, needs to be developed.

e. Inventory Resource Requirement

The minimum number of resources (personnel, equipment, etc.) needed during the recovery process must be defined in order to recover the critical business processes in the time frames identified in the earlier stage. Resources as detailed as number of telephones, internet and stationery should be identified for present and future needs.

Once all of the Business Impact Analysis information is gathered, it needs to be entered into the Business Continuity Planning database. This database holds both Business Impact Analysis information and business continuity plan information.

4.3.3.2 Design recovery strategy

a. Recovery Strategy Selection

A recovery strategy is the approach that would be taken on occurrence of business interruption. Various recovery strategies should be identified and assessed, and an appropriate strategy should be selected. Time to initiate recovery, start-up cost, monthly cost, interruption cost, testing cost, resources cost etc. of each recovery strategy are identified for comparison and the strategy that costs the least in the least time taken for recovery is considered.

b. Implement Selected Strategy

Once the strategy has been chosen, it must be implemented. This includes signing any necessary contracts, making provisions for space, supplies, storage, or making any other necessary preparations to ensure that the recovery strategy can be utilized when it is necessary due to a disaster.

The implementation phase consists of two main stages: Business Continuity Plan Development and Testing and Maintenance.

4.3.3.3 Business Continuity Plan (BCP) Development

The purpose of developing a Business Continuity Plan is to document all the information needed to recover critical business processes following a disruption. When completed, the plan will contain recovery teams, recovery procedures, inventory information, and other pertinent information to be used following a business disruption. Through the use of the business continuity planning database, all plans and general business continuity planning information will be organized and readily accessible. During the test plan development stage, the recovery team structure and recovery procedure should be developed; the reference information should be documented. The BCP should also be documented and the BCP database should be updated.

Components of the Plan Development stage are explained below.

a. Team structure

In a Business Continuity Plan, recovery teams consist of individuals who are responsible for the execution of the plan. Team members are assigned specific responsibilities to perform in the event of a business disruption. Recovery teams are generally composed of individuals who perform critical business processes, as well as those from management and support areas. The recovery team structure must be flexible enough to allow alternates to replace primary team members if necessary.

Typically, the structure comprises

- Disaster Declaration Team
- Recovery Coordination Team
- Information Systems Team
- Human Resources Team
- Logistics/Transportation Team
- Accounting Team
- Public Affairs Team,
- Facilities Team.

Operations teams should form part of all teams and leaders should be identified for all teams.

b. Develop recovery procedures

After establishing the structure, specific recovery procedures must be written. Recovery procedures are detailed action steps to be taken when a business interruption occurs. Each recovery team will have its own customized set of recovery procedures. The more specific the written procedures are, the less room there is for error during a recovery from an interruption.

c. Document business continuity plan

The previous steps have been leading up to the development and documentation of a Business Continuity Plan. By combining the information that has been gathered, a BCP can be written. This step will focus on putting all the components together and writing a complete plan.

d. Input information into BCP database

A business continuity planning database should be used to store business continuity plans. It includes a section into which all BCP information can be input. It is important to capture the information into the database as soon as possible to avoid the loss of information.

Roles and responsibilities for contingency planning will be identified in the BCP. Reports concerning the status of BSCB's recovery plans are to be discussed in the IT Steering Committee and presented to the Governing Board on an annual basis.

Management of each business unit has primary responsibility for plan development, maintenance, and testing for that unit. The recovery plan must address both manual and automated processes used by the business unit, and document the resources and actions required to resume critical functions/applications in an appropriate period of time. Facilities, communication and information systems, and critical applications must have adequate backup and recovery procedures in place. Recovery documentation and backup media must be stored offsite.

Written acknowledgment must be provided to the respective authority periodically regarding each business unit's compliance with Policy.

4.3.3.4 Business Continuity Plan Testing

Once a BCP has been developed, BSCB must develop testing procedures to facilitate execution, assessment, and documentation of the BCP to ensure that it is workable and realistic.

a. Develop testing program

A program for frequent testing of the plan is necessary. The types and frequency of the tests must

be determined. The overall purpose of testing is to determine whether the plan procedures are effective in the recovery of critical business processes. Testing also can assist in determining plan efficiency and in training staff in required actions after a business interruption. An effective test program will consist of a long-term testing strategy that progressively tests all critical processes. The three major tests that should be considered in the testing program are table-top, functional, and full-scale. In the long term, all three types of tests must be conducted in order to satisfactorily show that the plan is effective.

Exercise	Description
Table-top Exercise	A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. These exercises are used to assess plans, guidelines, and procedures.
Functional Exercise	Used to validate the capability of the organization to respond to a simulated emergency, in order to test one or more functions of the plan
Full-scale Exercise	Simulates an actual emergency, intended to evaluate operational BCM procedures and capabilities under simulated stressful conditions

Lead points in a developing an effective testing program are as below.

b. Determine which business processes will be tested

It may not be possible to test all critical business processes in each test. It is important that all critical business processes are eventually tested. Include all business processes as part of the ongoing testing program.

c. Prepare regular testing schedule

Determine how often each test is to be conducted. At a minimum, the plan should be tested annually. Prepare a testing schedule of the approximate dates on which the plan can be tested. It is also important to test anything that is likely to change and is crucial to the success of the recovery process, on a regular and ongoing basis.

d. Develop test plan

Each time a test is arranged, a test plan must be created. This test plan is written in preparation for the specific test being performed. Whichever test is being conducted, management approval must be obtained for the test and test date, and all those involved in the test should be required to be available to participate in the test. In preparing a test plan, the scope objective should be defined and the scenario should be defined (table-top, functional, full-scale). The test plan and procedures should be documented and the criteria for evaluation of the tests should also be set.

The evaluation criteria should reflect the number of critical business processes recovered against the targeted numbers and time frames.

e. Testing

Once the test plan has been documented, the test can be conducted. One or more associates should be appointed as "observers." These associates do not take part in the actual test; their role is to record all problems, recommendations, deviations from the documented plan, and changes which need to be made to the plan.

For each test to be conducted, notify both the participants and the observers of the time, place and expected length of the test. Also notify all other associates of the test. For the initial test, it may also be appropriate to inform the participants of the nature of the testing and the objectives of the test. The test should be tested as per the test plan document.

Compare the test results with the test objectives and criteria. This comparison will highlight problem areas and efficiency of procedures. It is likely that during the initial testing a number of criteria will not be met. For example, a call tree test may have shown that insufficient people could be contacted to recover critical business processes. As a result, the plan maintenance may have to encompass more frequent updates of telephone numbers. In addition, other personnel may have to be included to ensure that at least 75% of those required are available.

In evaluating the test results, the participants should be involved in a group discussion session. This can provide feedback on the practicality of the business continuity plan procedures. Written evaluations may also be required from some participants regarding specific tasks or their impression of the recovery procedures in general.

Participants should be comfortable with their role in the test and should be able to document the procedures they are to perform. Observers should be familiar with the test plan. Throughout the test, both participants and observers should be documenting any deviations from the test plan, changes which need to be made to the recovery plan, and any other recommendations or observations.

Now that all recommendations, plan deviations, and observations have been documented and discussed, any necessary changes to the plan should be made immediately. All documentation from the test should be kept and filed in a central location for reference.

4.3.3.5 Business Continuity Plan Maintenance

Once a BCP has been developed and tested, it is vital that BSCB implement plan maintenance

procedures to ensure that the plan remains a living document. Plans must be updated on a regular schedule to reflect personnel changes, phone number changes, hardware/ software changes, and organizational changes that may have occurred since the last update. Regular testing and maintenance of the business continuity plan(s) and strategy help ensure that continuity strategy stays viable, plan documentation is current and accurate team leaders are trained in the execution of continuity plan procedures.

a. Maintenance

The objective of plan maintenance is to keep the business continuity plan accurate and current. During maintenance the plan is updated based on results of test and procedures for maintenance of the test are developed.

To keep the information in the business recovery plan current, it will be necessary to continually incorporate alterations into the plan. Maintenance of the entire plan must also be performed on a scheduled basis - at least biannually.

4.4 Program Change Management Policy

4.4.1 Roles & Responsibilities

ROLE	RESPONSIBILITIES
Owner	IT Department
Supervision& Monitoring	The GM-IT Division or the respective business unit (user department) of the application is the owner of the respective application/s.
Implementer	The Designated Vendor SPOC along with AGM of respective IT division would be responsible to execute, implement and rollout the changes performed on application programs.

4.4.2 Procedures

4.4.2.1 Initial user request

In case of amendments required to an application program, the user shall submit the requirements to the Functional Department. The respective Application team of the IT Division must populate the 'Change Requirement' form. The requirements could relate to bugs in the existing functionality, frequent error messages indicating that some parts of the programs are incorrect, additional features required to be built in the system or report customization and changes forced from the regulatory body. The proof of the user request must be attached to this form.

a. Assessing Priority of Change Request

A suggestion as to how to define different levels of priority is given below:

Priority	Definition
1	Vital – the final software will not work without this. This may be as the result of something external to the software, such as changes in rules, regulations or guidelines governing the functioning of the software.
2	High - it would be very inconvenient to operate the product / software without this. Any work round can only be operated for a limited time. E.g. it might be acceptable to do this by hand during the month, but at year-end the volume of transactions will be too great to cope with.
3	Medium - a work round can operate. E.g. the operator might have to return to the menu to select the next option rather than go straight there
4	Low - nice-to-have but can live without the change. Things like changing the order of fields on the screen.
5	Cosmetic change – in practice these are very often implemented before higher priority ones, e.g. a minor screen change will be done while the code is open for some other reason. But if these changes are never done, they will not impact the benefits or usability from developing /using the product.

4.4.2.2 Approval of request

The Functional Department shall approve the 'Change Requirement' (CR) form taking into account the validity of the requirement in terms of module functionality as well as MIS requirement. This CR form shall then be sent to the DGM / AGM / Chief Officer/Manager of IT Division where the Head along with the respective Functional Department Head, shall conduct a feasibility analysis. Subject to the outcome of the feasibility study, the request shall be forwarded to the development team, which could be an in-house team or an outsourced party appointed for software

maintenance. The roles and responsibilities of the outsourced third party or the vendor as a part of the development activity should be charted out in the agreement entered into with the third party/vendor.

A standard naming convention for each application change requests must be adopted by the respective application teams. This naming convention must clearly bring out the respective application's name, module name and should have a distinct numbering scheme

The development team and functional Head shall analyze the change request in terms of the following:

- Criticality and need for program change
- Exploring new ways of getting the same functionality in existing set up
- Building workarounds
- Effect on other modules/ menu options/ business process - Impact Analysis
- Any possible effect on existing control procedures.

The analyzing team's hall formally provide its recommendations to the Chief Officer, IT Division and the Functional Head of the concerned department.

4.4.2.3 Change Classification and Prioritization

The IT Team shall analyze the program change request and classify it as desirable, essential or critical requirement. They shall document the analysis and provide instructions to the development team for implementation. It is the responsibility of the Functional Head of the concerned department to control the source programs of all centrally supported application systems. Making changes and testing new programs changes made to the application shall comply with the Policy. If the development activity is inhouse the responsibility of controlling the versions of the software and configuration management would rest on IT Team. The outsourced party would be responsible to maintain the same if the development activity is outsourced. Refer, to Version Control procedures for a detail on the procedures to be followed.

All development and changes to applications shall be carried out in the development environment. The development environment shall be a separate location from the live environment. Once the new programs are developed, it shall undergo various tests, which are carried out by the development team and functional users for evaluation of functionality of program by preparing proper test cases. These tests shall be conducted on the Test Server/Backup Server. No testing shall be conducted in the live environment. The Functional User Team shall confirm the test plans and results.

The entire process of testing shall be backed by detailed documentation of test plan, test procedures and results. The test documentation and results shall be reviewed and signed off by the DGM / AGM / Chief Officer / Manager of IT.

4.4.2.4 Change Implementation

a. On successful testing, new programs shall be copied in live environment. Only compiled versions of programs shall be made available in the live environment.

b. Back up of the database shall be taken before copying the new programs to production or live environment. The sign-off from IT Division Personnel and the Functional Users should be obtained for successful completion of program change procedures.

c. All Changes in the Production environment shall be announced to the intended audience before and after the implementation.

d. For upgrades, patches and other items provided by 3rd party suppliers, the installation instructions must be followed to implement the change.

e. The roll back plan for unsuccessful changes/implementations should be prepared before implementation.

f. Only System, Network or Database Administrator can implement the change. Changes can only be made after an approval from the Head – IT Division.

g. Change requests that may have a potentially negative impact on system availability, stability or performance shall be performed outside normal business hours. Changes that do not impact system availability, stability or performance can be implemented during work hours.

h. Suitable version control shall be maintained for all changes as per the 'Version Control Policy of BSCB.

4.4.2.5 Roll out the new programs to other sites

The new programs shall first be implemented on a pilot site. Upon successful implementation of the program pilot site, the IT Division shall rollout the new programs to other units or to the various end user locations depending on the nature and purpose of the application. Here, the programs shall be copied to live environment by Systems Administrator or other designated IT team/outsourced party.

4.4.2.6 Documenting the changes

The Concerned Departments Hall maintain the system documentation of modifications to programs. Application teams should be assisted by a technical documenter for in-house applications. The outsourced party should provide the technical documentation for outsourced applications. It must be sure that the **user operating manual** as well as **system documentation** is updated on a timely basis. The responsibility of maintaining the above documents rests with the Functional head of the concerned department.

Configuration Management: The last stage in the program change management Policy should be configuration management. After the completion of the change management process, all related documents, Hardware/, Patch/system software changes and versions shall be updated in the configuration management document.

4.4.2.7 Emergency Program change control procedures

For all program changes requiring emergency actions and response process, which bypass the suggested Policies and procedures above, the following procedures shall be adopted:

a. Verbal approvals shall be obtained by the Application Team from the respective Functional Head. This shall be immediately followed by an email confirming the same. A verbal approval for the same should be confirmed over the telephone to the IT in charge.

b. Functional User department representatives and the IT support personnel, in conjunction with the subject matter experts (Vendors, third parties) shall co-ordinate the process of the emergency program changes with adequate supervision.

c. Once the emergency change request has been resolved, the Functional Head of the concerned department shall ensure that all activities performed for the emergency program changes are documented. This documentation would include the names of program files changed, reasons for change, effect on other functionality of the application, test conducted to verify accuracy of the changes, along with the user sign-off.

d. Any sub-normal procedures followed during the emergency program change (e.g., giving super-user or root password to the support personnel performing Troubleshooting etc.) should be identified and restored to the original settings and configurations.

e. Even in the situation of an emergency, the 'need-to-do' principle shall be followed, with appropriate restrictions on the support personnel executing program changes.

f. The testing should be carried out in such a manner to ensure the accuracy and integrity of live data and systems.

g. The documentation recommended in documenting the Changes above for normal program change procedures shall also be completed after implementing emergency program changes.

4.4.3 Annexure

4.4.3.1 Change Requirement Form

Change Requirement Form	
Project:<insert project name or identifier>	**Reference:**<state any reference to previous change request forms, risks or issues this form is resolving>
Raised by:<insert name of person requesting change>	**Date raised:**
Position / title:<job title / position>	**Priority:**<see notes above >
Part 1: Describe the change that is being requested	
Part 2: Reason for the change requested	
Part 3: Impact and cost of not doing change	
Part 4: Supporting Documentation / Attachments	

Name: _____

Signature: _____

Date: dd/mm/yyyy

For office use:

Change made by:	
Signature:	
Change checked & confirmed by:	

Signature:	

4.4.4 Impact of Program Change Management Policy

a. The Policy helps in recording and classifying any required change with regard to its importance and how likely each element will impact the project including complex factors that need to be part of the change.

b. The delegated authority assesses the change and makes a risk analysis to study the impact of the change on the project in terms of costs / timelines.

c. All effected stakeholders due the change is kept informed so that they're aware of any updates or modifications happening to the system.

4.5 Logical Access & Review of Access Rights Policy

4.5.1 Roles and Responsibilities

ROLE	RESPONSIBILITIES
Owner	IT Division
Custodian & Supervision	GM-IT Division
Monitoring	System Administrator [AGM(SM)]
Implementation	Users / employees are supposed to follow the Policy stipulated in this document.

4.5.2 Scope

This policy covers logical access to data networks, servers. and personal computers (stand- alone or network -enabled) located at different locations, where these Systems are under the jurisdiction and/or ownership of The BSCB Ltd., and any personal computers and/or servers authorized to access The BSCB Ltd.'s data networks.
This policy applies but is not limited. to the following:

- Applications
- Databases
- Operating systems
- Source Code
- Personal Computers/ Workstations
- Networks
- Interfaces
- Middleware
- Domain Email

This document focuses on The BSCB Ltd.'s corporate for logical access control. Specific procedures and guidelines to facilitate the implementation of this standard shall be established within various

Departments. Regional Offices, Branches, Data Centers, Disaster Recovery centers, training Centers, etc.

4.5.3 Purpose

The purpose of this policy is to ensure that logical access to information resources is controlled and managed based on business requirements.

The BSCB Ltd. aims to protect information resources and effectively manage risks in the environments in which it operates. This policy shall ensure the implementation of appropriate logical access control measures to manage the risk of:

- Breach of confidentiality
- Breach of integrity
- Lack of system availability
- Reputational risk and
- Financial loss through loss of confidential information.

4.5.4 Applicability

This policy applies to The BSCB Ltd., its departments, regional offices, branches, data centers, DR centers, training centers, and their employees, including temporary staff, contractors, consultants, third parties and service providers making use of The BSCB Ltd.'s information resources.

4.5.5 Standard-Request logical Access

4.7.5.1 General

- The official Access Request forms applicable to the office or department shall be completed whenever access to any information resources within The BSCB Ltd. is granted.
- The Access Request form shall, as a minimum, gather the following information as per Annexure Access Request from the user:
- The business requirements for the authorization of logical access to information resources shall be defined and documented prior to logical access being granted.
- The Access Request form shall be signed by the following parties to authorize the access requested:
    - User's manager or head of the department or in-charge of the section — to ensure that the requested access is indeed needed and that all other details supplied are correct.
    - Appropriate Business Unit Manager or delegated manager.
- The authorizing parties shall indicate on the Access Request Form the duration which the access may be granted to the applicant.
- The user shall submit the signed access request form to the applicable logical access administrator in order to him/her to grant the necessary access.

- The IT service provider shall maintain access requests by keeping record of users with access, level of access and which applications and systems the user has access to.

4.7.5.2 Supporting Documentation

A System Authorization list shall be created and kept up to date. This list shall, as a minimum, contain the following information:

- Name of the system
- Persons who may authorize access to the system
- Level of access rights the person may authorize access for.

Each Department shall create and maintain an access control matrix, ensuring that proper segregation of duties is established, to simplify the granting of logical access to systems. The matrix shall include the following:

- Type of work performed
- Systems needed for the work performed
- Classification of information that is needed to perform work
- Type of access that must be granted for the user to perform the work
- Segregation of duties requirements; and
- Duration the access may be granted for.

4.5.6 Grant Logical Access

Granting access to a user is one of the most important activities performed on a daily basis within the organization as this enables the user to perform his/her role in the organization. Having access to a specific information system is. however, also a privilege that should not be misused. To prevent the misuse of access to systems, it is therefore imperative that access is granted in an orderly manner after a number of basic verifications have been performed. As a basic rule only least privileges shall be provided when granting access.

The following lists the basic verification points:

- Access shall only be granted upon receipt of an official request via registered email and the original authorized access request form.
- Access shall only be granted upon positive identification and authentication of the user requesting the access.
- Access shall only be granted with the authorization of the relevant information system owner and the user's manager.
- Access shall be granted according to the principle of least privileges needed to perform the user's specific role in the organization.

4.5.7 User ID Management

There are 4 different levels at which user IDs can be created.

a. **OS Level -** OS level user ID is used for carrying out any activity in operating system.
b. **Application Level** - Application-level user ID is used for any activity to be carried out in Application.
c. **Database Level -** Database level user ID is used for any activity to be carried out at Database level e.g. creating table/objects, updation of records, deletion of records, retrieval of records etc.
d. **Network and Domain user level –** Network and domain user ID is used for carrying out activities related to network security and domain controller purposes.
e. All logical access administrators shall consistently observe the user ID naming standards, except where the AGM(IT) has given explicit permission to use a different naming convention.
f. The use of a shared user ID for a group of users or a specific task shall not be allowed.
g. No duplicate user IDs shall be allowed.
h. After resignation or contract expiry the user ID shall be immediately suspended from the system.
i. Users shall not be allowed to have multiple sessions on the same system, unless appropriately authorized.
j. Anonymous and/or guest user IDs shall be disabled on all systems, except where the system explicitly requires the anonymous and/or guest ID to effectively perform its expected function.
    - Access to anonymous and/or guest user IDs shall only be allowed with written approval.
    - The access rights for the anonymous and/or guest user ID's shall be limited to the specific task that needs to be performed and none other.
    - Monthly checks shall be performed to ensure that the anonymous and/or guest user ID's are used, and if not used. they shall be disabled.
    - Monthly checks shall be performed to verify any attempts to access unauthorized information with anonymous and/or guest user IDs.
k. Every user ID established for a non-employee shall have a specified expiration date, with a default expiration of 30 days where the actual expiration is unknown.
l. During the log-on process information messages shall not convey information such as incorrect password or username. This will minimize the potential for access breaches, conveying information to potential intruders.

m. The last successful log-on time of the user shall be recorded and conveyed to the user on the next log-on session. If the recorded log-on time is incorrect the user shall report an incident.

4.5.8 User Responsibility

a) Users shall be held responsible for all activities performed with their personal user IDs.
b) User IDs shall not be utilized by anyone but the individual to whom the specific ID has been assigned.
c) The end user shall not share or divulge his or her user identification and authentication mechanisms to any other individual.
d) The user shall only access systems for which he/she has received valid user IDs.
e) The user shall not use hacking and/or probing programs designed to gain unauthorized access or compromise user accounts, to any system or application.
f) The user shall ensure the safe storage of passwords, tokens and other devices used for access.
g) Users shall not store passwords in electronic format on their PC's nor shall a paper record of passwords be retained.
h) User shall not include passwords in an automated log-on process.
    a. Whenever there is an indication of possible password compromise, the User shall:
        i. Change the password.
        ii. Report the incident through the Incident Management System.

4.5.9 Access Rights to User IDs

For any activity to be carried out in system, access rights and privileges have to be given to the users. The access rights and privileges should be provided to user as per their designation and on need basis. The access rights control the login of users to system and network resources by granting access only to the specific resources, which they require to complete their job-related duties. Third party/ outsourced / Vendor cannot access BSCB's domain email unless authorized by GM(IT) /DGM (IT) in writing.

a) The number of privileged user IDs shall be strictly limited to those individuals who require such privileges for authorized business purposes. A screening process shall be performed by The BSCB Ltd. to identify any risks that may be inherent to the users before approval of power user's access rights.

b) The use of user IDs such as Root, Sys and Administrator shall be avoided if possible.
c) For accountability, user IDs linked to an individual shall be created with the privileges for Root, Sys or
Administrator.
d) Privileged user IDs shall not be used to perform normal day-to-day work.
e) The use of privileged user IDs shall be recorded and logged.
f) A copy of the privileged user IDs and encrypted passwords shall be stored Disaster Recovery purposes.

4.5.10 Review of access rights

The access rights and privileges should be granted to a user based on the request received or approval from the competent authority.

The creation, deletion and changes of user accounts and privileges must be carried out by trained and authorised staff only (preferably by System Administrator).

The access rights and privileges of the user ids at OS, Domain user id, database and application levels etc. must be carried out periodically at least once in a quarter.

Monitoring Areas:

a) The following areas shall be monitored depending on criticality as decided

- Authorised access
- User ID
- Date and time of key events
- Type of events
- Files accessed
- Programs/utilities used.
- Privileged operations:
- Use of supervisor account
- System start-up and stop
- I/O device attachment / detachment.
- Unauthorised access attempts:
- Failed attempts
- Access policy violations and notifications for network gateways and firewalls
- Alerts from proprietary intrusion detection systems.
- System alerts or failures such as Console alerts or messages
- System log exceptions

- Network management alarms.

b) Logical access rights shall be reviewed to match:

- The actual access rights and the authorized access rights
- The actual access rights and the needed access rights (even though actual access rights have been authorized).

c) Logical access rights shall be changed based on the review of the access rights.

4.5.11 Frequency

a) Logical access rights shall be reviewed on a quarterly and ad hoc basis or on receipt of an official request to ensure the validity of user IDs.

b) Privileged users shall have their access rights reviewed at least monthly by the Information Owner to ensure access to BSCB's information is appropriate and still required.

4.5.12 Deviations

a) The logical access administrators shall ensure that all access rights are in line with business needs. Any deviations shall be investigated and reported to the Division Information Manager.

b) All unauthorized access rights shall immediately be revoked.

4.5.13 Operational Policies

a. The access rights /privileges of all Super user/Data base User/Super DB User/ Administrator user etc. should be reviewed by respective application/project owner periodically at least once in a quarter.

b. The users should not give their IDs to others. Another person's user ID shall not be used.

c. Wherever possible, the system / application shall display logon banners and warning notices to convey the following:

   - the system is for authorized users only
   - usage is monitored (if applicable)
   - evidence of misuse may be presented in legal proceedings

d. The access rights /privileges of all Branch office etc. should be reviewed by respective Branch office heads periodically at least once in a quarter.

e. Requests for users' accounts and access privileges must be formally documented and appropriately approved.

f. Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the system owner.

g. Privileged User Ids like system Administration accounts shall not be shared by more than two users (if more than 1 system administrator employed) who require this level of access to perform their job duties.

h. Third party access request shall clearly mention the purpose of access and period of access requirement. Third party user's access shall be granted for defined time frame only. After the end of defined time frame the access to systems shall be revoked either automatically or manually, as applicable.

i. In case third party access requires to be continued, a request for access renewal shall be initiated and shall follow the original approval procedure.

j. Third Party users shall sign a non-Disclosure agreement for the usage of the IT systems at BSCB.

k. Unnecessary user ids should be disabled.

l. Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access BSCB's systems

m. Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges

n. The access rights /privileges, which are not required should be withdrawn from the users (in case of transfer / resignation / termination of employment). User account has been inactive for more than 60 days, the system shall automatically unauthorize the user from any applications the user had access to.

o. In case of violation of the usage of the application, the System Administrator should revoke access of such user upon notification to the DGM /Chief Information Officer.

p. The IT DGM / AGM / Chief Information Officer reserves the right to temporarily revoke any access granted to any user on identification of any suspicious activity that may be detrimental to the interest of the organization.

q. The reviewer should check and ensure that the access rights/privileges are as per the designation of the user and as per the need basis.

r. All generic user ids should be disabled.

s. In case any generic id is required to be retained for any special purpose, e.g. database purpose tuning, Application management, Reports, Day End/Day begin/Troubleshooting operations,

the same has to be considered as an exception and should be recorded in Exception / Risk Register. It should also be brought to the notice of the competent authority/ Project/ Application owner for approval.

t. The system/application shall display the time and date of the last login to the user, for reference, to enable the user to identify and report any unauthorized activity, being attempted.

u. Maintaining Logical Access:

i) Dormant Logical Access

- Accounts not used for an extended period of time demonstrate that no access to information on that system is needed.
- Logical access administrators shall generate reports on accounts dormant [Or 30 days.
- These reports shall be sent to the Chief Information Manager to determine the validity of the dormant accounts.
- The Logical access administrator shall inform the user and his/her line manager about the dormant account via an e-mail message.
- The Chief Information Manager or Regional Manager / Branch Manager shall inform the logical access administrators whether the accounts need to be removed, disabled or left as is.
- The logical access administrator shall enter a reason in the description field if an account is disabled.

ii) Updating Logical Access Information

- Human Resources Department shall inform the Information Technology Department of organizational changes, e.g. structural changes, appointments, moves and resignations impacting access lists.
- The Information Technology Department shall ensure that the relevant logical access administrators are informed of the changes in order for him/her to update the users' account or details.

iii) Removing Logical Access

Information Security — Access Control Procedure details the removal of logical access.
a) User IDs and biometric identifications shall be removed from the systems when:
- The user leaves the employment of The BSCB Ltd.
- User access rights are changed.
- The users' contract has been terminated.

b) All smart cards or e-tokens shall be handed over to The BSCB Ltd, Information Security Manager when:
- The user leaves the employment of The BSCB Ltd.

- The users' contract has been terminated
- Users' access rights are changed.

c) Logical access rights that are no longer required shall be removed as soon as they have been identified.

d) After an employee leaves The BSCB Ltd., or on contract expiry in the case of contractors' user access shall be removed. There shall be no re-use of any of the user's user IDs. This serves to minimize the risk of dormant access permissions being inherited by a new user.

iv) Security Controls

a). Automatic Lockout

- After three (3) consecutive authentication failures, the users' account shall be locked and require a manual reset. The number of failed attempts may depend on the specific system.

b) Automatic Time-outs

- The users should not leave the system without log out from the system or locking the application or specific resource. Wherever possible inactive system sessions shall be automatically terminated after certain period of time as per the specific system
- Users shall not attempt to circumvent automatic time-out controls, by implementing measures such as pinging the server to maintain connection.

v) Critical Systems

a) A list of The BSCB Ltd. Critical Systems list shall be created and maintained with the following information:

- Name of system
- Description of system
- Date of last risk analysis
- Name of system owner; Contact details of system owner

b) An audit trail shall be activated for all critical systems as listed in The BSCB Ltd. Critical Systems list. These audit trails shall, as a minimum, include the following information:

- User IDs that logged in or attempted to login
- Dates and times for log on and log off
- Activities performed (especially privileges activities)

- Terminal identity or location
- Successful and unsuccessful access attempts to system
- Successful and unsuccessful and rejected data and other resource access attempts.

c) Critical system audit logs shall be securely archived to prevent modification for at least three (3) months or as decided by the higher authority of The BSCB Ltd..

d) Audit logs shall be secure and only authorized persons shall gain access to the logs.

e) All The BSCB Ltd. Critical System Logs shall be protected in a secure way and log entry sequence numbers and shall also be automatically monitored for sudden decreases in size, and gaps in log entry sequence.

f) All audit logs for critical systems shall be reviewed and monitored on a quarterly basis to identify potential misuse of systems or information

g) Audit logs shall also be reviewed on an exception basis.

h) Audit logs shall be reviewed by a system administrator who is responsible for the critical system. Independent review of logs with appropriate tools by The BSCB's Security Officers shall be performed at random.

i) Logging facilities and log information should be protected against tampering and unauthorized access.

j) Any irregularities (any recorded activities that do not follow the norm of data collected in the audit log) in the audit logs shall be reported to the Division Information Manager and an incident logged.

k) Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes

4.5.14 Annexures

4.5.14.1 Access Request Form

User Details

Reference No.	
First Name	
Last Name	
Employee ID	
Designation	
Department/Location	
Email ID	
Telephone Number	

Nature of Access Request

List the specific platform(s) or application(s) for which privileged access is required or indicate all –
Access is required for what time period – <dd-mm-yyyy> to <dd-mm-yyyy>
Why is privileged access required?

For use by system administrator –

Reference No.:	
Access Authorized by:	
Signature:	

Date:	

4.6 Technology Refresh Policy

4.6.1 Roles and Responsibilities

Role	Responsibilities
Owner	IT Steering Committee
Monitoring Supervision	The GM-IT is responsible for monitoring and ensuring the technology refresh.
Implementation	The DGM(IT) of BSCB will monitor the implementation

4.6.2 Purpose:

This policy defines what is required to implement/manage a comprehensive technology refresh approach for maintaining existing technology to support BSCB. It is required that a consistent maintenance and upkeep of these tools be in place to deliver the Bank's services. This policy defines a standard cyclical investment of resources for technology to ensure the Bank can provide its services and maintain its operations.

4.6.3 Policy Statement:

- Information Technology (IT) is a critical tool for conducting Bank's business.
- BSCB will setup an annual update process for technology and allocate the appropriate staff and funding/budget support to effectively manage the implementation of the Refresh Policy.
- Refresh program should stay current with technology in the market and mitigate risks of service delivery for the Bank, which includes, preventing the technology infrastructure from reaching its End of Life or End of Support.
- Refresh program should follow industry standards and best practices in terms of type of asset, age of inventory, timeframe for replacement, etc.

- Refresh program should be affordable to the Bank and should minimize support costs and maximize savings through standardization and bulk pricing opportunities and contracts.
- BSCB's Refresh policy addresses three broad categories of technologies:

  (1) "Front-end" devices
  (2) "Back-end" infrastructure/devices
  (3) "Standard Productivity" software

4.6.4 Definitions:

- **"Refresh"** means renewing all technology devices and standard productivity software already procured and used at the BSCB. Refresh does not include the following:
  - the original purchase of any technology,
  - enterprise software.
- **"Current"** does not mean "Bleeding Edge"; it means keeping technology working so that:
  - the work of the BSCB is not hampered/diminished,
  - the support of the environment is not overbearing/unmanageable,
  - security and compliance issues do not pose a risk to the bank.
- **Front-end devices** include PCs, Laptops, Monitors, Printers, scanners, A/V Equipment. At this time, tablets, mobile devices are not included.
- **Back-end devices** include data center equipment, network equipment, servers, routers, switches, telephony, to support the operations of the BSCB.

4.6.5 Standardization of Technology

At any point in time, the BSCB gains benefits from maintaining, the practice of purchasing equipment according to agreed-upon standards. Agreement by a purchaser to accept standard configurations benefits the BSCB in multiples ways, including:

- Better pricing of components and supplies.
- Reduced administrative overhead.
- More expeditious processing of purchase requests.
- Greater technology support.

- A reduction in maintenance costs; and
- A better ability to train on the new equipment.

Notwithstanding the above, the purchase of non-standard technology components is not prohibited by this policy. However, such purchases should be minimized as much as reasonably possible. The purchase of non-standard technology components must be justified by the existence of special circumstances that require it. Also, the purchaser of a non-standard technology component must document the source of support for the component before purchase will be approved.

4.6.6 Staggered Refresh

To ensure equitable balance between all areas of the Bank, allocation of technology resources is a representative and participatory process linked to the BSCB's planning and budgeting process. Each year, the Manager - IT s will submit a request to annually allocate a fixed cost to refresh computers and other technology. This request will be based on the BSCB's available budget.
In order to control costs and minimize disruption to the BSCB's operations, only a portion (say, approximately 25%) of the computer inventory will be refreshed every year. Equipment will be replaced based on age and program needs. As a result, there is no need to request new computer equipment unless there are programmatic or personnel changes.

a. Age of the Equipment. The first criteria that will be considered is the age of the equipment. Under this criterion, replacement equipment is determined as a result of the annual inventory that identifies the oldest equipment in the Bank.

b. Programmatic Needs. With regard to this criterion, technology resources, including technology refresh resources, are allocated based on priority needs. Needs are determined through the Bank planning processes, and shall be transformed into programs, projects or initiatives and classified as high, medium, or low priority.

   - High Priority. High priority initiatives are typically mission critical, required by code or law, essential to ensure privacy, security and safety, or are driven by economic factors.
   - Medium or Low Priority. Medium or low priority initiatives and programs are prompted by the need to stay competitive, improve efficiency, add value, create opportunities, improve services, and respond to the demand for more services.

4.7 Backup & Recovery Policy

4.7.1 Roles and Responsibilities

ROLE	RESPONSIBILITIES
Owner	IT Division
Implementer	As per the existing ASP Model for CBS, the concerned SPOC for CBS Vendor is responsible for necessary backup and retrieval of the current database.
Supervision & Monitoring	The execution of the procedures will be monitored by AGM(CBS).

4.7.2 Back-up of Data at Data Centre

BSCB is having several types of Back-up which includes

c. Database Backup

d. BSCB - integrated solution backup

e. Application and system state Backup

All the Monthly/Quarterly/Half-Yearly and Yearly Backup are permanent in nature.

Every Backup is having different type of back-up time, periodicity and retention period. Following is the recommended timeline and is subject to change as per the decision by the management of BSCB. The details are given below:

Frequency Type of Back-up	Back-up Time	Periodicity	Retention period	DC	DRC

Database Backup (Production)	After EOD	Daily	5 years	Onsite	Offsite
BSCB Integrated solution Back-up	Before EOD	Daily	365Days	Onsite/Offsite	Onsite
Weekly Backup of above-mentioned databases	On Sunday	Weekend	5Weeks	Onsite/Offsite	Onsite
Monthly Backup of above-mentioned databases	On Month End	On Month End	Permanent	Onsite/Offsite	Onsite
Quarterly Backup of above-mentioned databases	On Every Quarter End	On Every Quarter End	Permanent	Onsite/Offsite	Onsite
Year End Backup	After Year End	After Year End	Permanent		

4.7.3 Operational Policies

4.7.3.1 Information to be backed up

a. Business applications (data and program files) and operating systems residing on the servers as decided by IT Committee (documented in the detailed procedures).

b. Applications (data and programs) managed by Concerned IT official.

c. Critical Data on Workstations, desktops and laptop computers.

d. Data on BSCB specific third-party desktops, laptops and mobile devices.

4.7.3.2 Responsibility

a. Concerned IT Official (designated for Backup & Recovery function) is responsible for taking and maintaining backup of all data and applications as well as operating systems. In absence of the concerned Official an alternate Backup official must be designated by Heads of the department and should perform the backup activity. The designated official should be given required privileges and access to the systems for the purpose of taking backups. These privileges are to be removed immediately after the actual concerned Official resumes duty.

b. It is the responsibility of Steering Committee to decide on the criticality of the data, backup and frequency of backup of the information with respect to the application systems in BSCB.

c. IT Division should preserve the full back-up on discontinuance of an application system.

d. The users are responsible for taking and maintaining the backup of all critical data residing on their individual workstations, desktops and laptop computers.

4.7.3.3 Frequency of data backup

Data to be backed up	Frequency
Data, applications and operating systems.	As per the Policies issued by Steering Committee and decision by Division Heads
Data on Workstations/Laptops	As decided by the respective users. (AtleastonceinQuarter)

4.7.3.4 Procedure for data backup

a. Instruction Guidelines/procedures for taking backup of data would be performed as per the Backup Policies adopted by the organization.

b. The number of backup sets to be maintained is decided by the Steering committee based on the criticality of information residing on the servers & in conformance of backup Policies.

c. A list of all the data files for critical applications is maintained by the IT Division along with a brief description of the contents of those files.

d. In addition to the scheduled backups, backups to be taken in case any of the following event occurs

- Configuration change (Pre Configuration and Post Configuration backup should be taken)
- Upgrade of an operational system
- Peripheral Management

e. In case of any OS upgrade, backup procedures should be developed in consultation with Application/hardware outsourced parties and vendors.

f. If the backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the IT Division so that exceptions or alternative arrangements can be made.

g. If, for some reason, the backup cannot be completed, is missed, or crashes, then it must be completed by 6 a.m. the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails more than one day in a row, end users in the organization must be notified.

4.7.3.5 Backup Media

a. Instruction Policies for backup media are issued by Steering committee detailing type of media, frequency of change in backup media and rules for rotation as advised by the IT Steering Committee.

b. It is to be ensured that the media is regularly examined for readability of the data. The backup media is replaced immediately after encountering the error or at predefined time intervals whichever is earlier. The backup media must be appropriately labeled and numbered automatically by the backup system or manually by the Backup Operator taking the backup. e.g. '<App>-Friday-1- 'On/Off' (where 'App' means the relevant 'application system' , the number of backup media used for the backup and 'On' or 'Off' denotes the sites of storage of the backups).

c. The respective users should back up the data on workstations and laptops on to external storage device.

d. The IT Operations Team tracks the usage of backup media, and the media is replaced after a stipulated number of usages.

e. At least 3 backups must be taken every time a backup activity is initiated for critical applications, as decided by Steering Committee.

4.7.3.6 Storage of backup

On-site

On-site data backup should be maintained in safe custody, preferably in a fire-proof room. The access should be available only with designated IT Team. A log should be maintained for all accesses.

Off-site

Off-sitedatabackupshouldbemaintainedatalocationidentifiedasan'off-site'. The backup media will be stored in 'fire-proof cabinet/safe'. The key to the cabinet/safe is available only with IT Team and the duplicate is kept with DGM/AGM/Chief Officer, IT Divisionforemergencyuse.Thescheduleofoff-sitebackupwillbedecided concerned steering committee.

Real-time off-site backup

ThesteeringCommitteeshoulddecidetherequirementofareal-timeoff-site backup facility. Based upon the criticality of the business function supported by the respective system, this facility will be crucial to provide continuity of services when disaster strikes. (Refer to Disaster Recovery Procedures)

4.7.3.7 Backup logs

The backup logs maintained by the IT concerned official should either be manual registers, or the reports generated by the system (operating systems or the applications), which is to be printed and hardcopies maintained.

The Backup Operator should maintain the backup movement logs for the backups at off-site location.

4.7.3.8 Recovery of Backup Data

a. Backup documentation must be maintained, reviewed, and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:
    - Identification of critical data and programs; and
    - Documentation and support items necessary to perform essential tasks during a recovery process.
b. Documentation of the restoration process must include:
    - Procedures for the recovery
    - Provision for key management should the data be encrypted.
c. Recovery procedures must be tested monthly.
d. Recovery tests must be documented and reviewed by the DGM / AGM.

4.7.3.9 IT Disaster Recovery Plan

An IT DRP must be formally documented and contain the following details:

a. Step-by-step procedures to recover critical IT systems and applications and restore data after a major disruption, including:
    - Emergency response to a major disruption
    - Initial recovery of the most critical IT systems
    - Full recovery of most critical systems, applications, and data
b. Clear roles and responsibilities.

c. List of critical systems and applications that are aligned with the BCP.

d. Detailed minimum requirements and specifications for the critical IT system components, including mapping of critical applications and data hosted on servers.

e. The IT DRP plan must be reviewed and tested at least annually to ensure documented information is up to date and that all team members are aware of their responsibilities, roles and tasks to roll-out the plan effectively.

f. Contact information of key resources, including phone numbers (daytime and non-working hours), email and physical address where possible, for:

- The IT emergency response team.
- Other IT contacts (IT staff, 3rd party IT supplier, application vendors, etc.).
- Other business contacts (applications and system owners and administrators, key suppliers, customers and stakeholders, communication team, etc.).

4.7.3.10 Restoration testing

a. To verify the readability of backup media, mock restoration tests must be carried out, at least once in a month on the test/backup servers.

b. The entire process is to be documented detailing the test plan, the activities carried out and the test results.

c. It is to be ensured that the restored data is deleted from the test servers after successful completion of testing.

Use of off Sites for restoration testing:

a. Steering committee should issue Policies for the backup restoration testing, including system privileges, and overall responsibility of the designated IT Team. The outsourced party and vendors should be contacted at the time of framing procedures for the restoration of data.

b. The test plan is prepared in advance and essentially includes 'mock test' with the restored data. The backup media kept as 'Off-site backup' should be used for such restoration.

c. Upon restoring the data on the test server, the results should be documented. DGM / AGM / Chief Officer / Manager - IT at end of the restoration exercise must verify these test results. The data restored is deleted from the test server after successful completion of the exercise.

d. Any exceptions in the process mentioned above must be reported to the concerned Functional head of the department.

Backup solutions

Backup and Recovery solution must be selected based on the criticality of the application server and dependencies of business. Solutions to be considered are:

a. Redundancies on site – Duplicate hardware or data maintained at site to prevent service outages or any data loss in case of any emergency.

b. Mirrored Backup site - Creation and maintenance of redundant copies of a database. The purpose is to ensure continuous data availability and minimize or avoid downtime that might otherwise result from data corruption or loss, or from a situation when the operation of a network is partially compromised.

c. A fully functional data center with hardware and software, personnel and customer data, typically staffed around the clock, operationally ready in the event of a disaster

4.8 Disaster Recovery Policy

4.8.1 Roles and Responsibilities

ROLE	RESPONSIBILITIES
Owner	IT Division
Implementer	The Chief Information Security Officer (CISO) holds the primary responsibility to direct the implementation of the procedures; he is also the owner of the Policy. The Group Leaders along with their respective teams will be responsible for the implementation of these procedures
Supervision & Monitoring	AGM-IT / GM-IT will supervise and monitor the implementation of procedures

4.8.2 Strategic Objectives of DRP

The DRP developed should address the following strategic objectives

- Establish alternative strategies to recover critical information processing systems.
- Ensure that necessary data can be recovered and processed so that critical business functions

can be re-established.

- Protect and preserve BSCB's Data whereby it reduces overall risk of company.
- Ensure that plans are developed, tested, and maintained to minimize any inconvenience or interruption in the ability to continue operations and services.
- Provide a means for assessment of DR situation
- Establish a methodology to ensure notification to the appropriate management and support areas in the event of an interruption to operations.
- Establish a methodology for communicating emergency situations to affected employees, clients, customers, and agencies etc.

4.8.3 Relationship between Business Continuity and Disaster Recovery Plans

Business Continuity is an all-encompassing term covering both disaster recovery planning and business resumption planning. Disaster recovery (DR) refers to having the ability to restore the data and applications that run business and how quickly data and applications can be recovered and restored. While Business continuity (BC) planning refers to a strategy that lets a business operate with minimal or no downtime or service outage.

A disaster could be defined as:

- Complete loss of each single physical site including IT production.
- Complete failure of any single internal and/or external IT infrastructure service provider (including outsourced IT infrastructure functions and/or services.
- Power outages and/or disruptions of internal and/or external network connections (e.g. LAN/WAN) for each single physical site with IT production.
- Any single point of technology failure with significant impact as identified in the risk assessment and/or disruptions and outages covering IT infrastructure.
- Non accessibility of any critical location.

4.8.4 Disaster Recovery Plan: Key Components

The Disaster Recovery Plan should address the following:

- Identification of critical applications and processes.
- Checking of data backups and updates
- Identification of minimum recovery hardware configuration.
- Identification of required software and platforms.

- Prioritizing restoration of applications and verification steps to be performed prior to bringing up further applications.
- Target recovery times for each mission critical function as well as normal service functions.
- Actions to be taken during the phases of business resumption:
  - Response (initial action following a disastrous event).
  - Resumption (establishing the alternative processing site and begin processing time sensitive business functions).
  - Recovery (resume processing for less time-sensitive business functions).
  - Restoration (returning to the original processing site).
- Identification of critical personnel and event notification information.
- Description of how to acquire necessary resources, such as vendor information, and temporary employees.
- The affordable critical loss of business data should be below 30 Minutes and the recovery time for business to start operations from Disaster Recovery site after calling for disaster is 120 Minutes.
- Access requirements concerning who is authorized for declaring a disaster, entering the off-site storage facility, gathering recovery resources, or accessing the primary location after police/fire/detectives have isolated the area.
- Identify the critical checkpoints to declare a disaster.
- Persons authorized to purchase, what they can purchase and authorized spending limits.
- Security issues such as guards and premises protection at the Disaster recovery site.
- Communication needs, such as who will address the media in a disaster situation and what employees should NOT say to any outside person at this time.
- Additionally, the plan should include the following information:
  - Notification procedures for employees, vendors and customers.
  - Groups, group leaders and their contact numbers.
  - Action plans for each group (concise step-by step descriptions of actions required).
  - Detailed instructions for Disaster Recovery Procedures and Contingency Procedures.
  - Network documentation including HLD and LLD of cabling and specifications
  - Up-to-date equipment and software inventory.
  - Building plans such as air, water and electrical system mappings.
  - Evacuation procedures including safe meeting areas.
  - Vendor agreements.

- Contingency plan.
- Vendor contact list.
- OEM Contact list
- Customer contact list.
- Maintenance schedule.
- Test/exercise schedule.

4.8.5 Backup/Data Recovery

The frequency of backup information should be determined based on the criticality of the data, the system, location and departmental needs.

A routine schedule for off-site rotation of backup information must be established. Depending on the threat of a regional disaster, the off-site location should be outside of the regional area to avoid total loss of information.

The following backup information should always be available in current status:

- Historical and current system processed information required by BSCB law and regulators.
- Copies of current versions of the operating system and other significant software used within the organization. This software must be stored off-site unless compatible versions are easily available and customizing/reconfiguring is a minor task.
- The availability of production data should be as per the Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) defined.
- Analyze the business and rank the business needs in terms of priorities.
- What from the regular operations can be down for 24 hours and more?
- Priority listings concerning the restoration of applications in a logical order based on sequences dictated by the system or by management decision. These decisions are made jointly by IT operations, applications managers and business users and should be reviewed annually.
- All critical systems in BSCB's IT environment should have mirror copy of OS maintained which needs to be synchronized monthly, to avoid any inconsistency.
- Maximum expected time, which would be required to complete the installation of replacement hardware and software should be clearly stated (recovery lead times).
- Equipment and network layouts (network and software configuration diagrams) and any other information vital to restoration of the current system or necessary for setting up a new system(s).
- All the critical links should be under automated observation continuously to ensure availability in cases of Disaster.

- All the networking and security components should be replicated and updated for any changes made in the DC with reference to software version, signature update and configuration changes.

Non-system related backup information that is very important, and should be held at off-site locations, includes, but is not limited to:

- Hardware and software inventory, including serial numbers and detailed information that would be useful for identifying needed items such as makes, model numbers, engineering release levels and types of equipment used to process transactions. This listing should also include alternatives to equipment in case of unavailability.
- Copies of current operational manuals and procedures or access to the same (i.e., from other site, vendor or offsite data storage).
- Important legal duplicates/originals of critical documents.
- Unique critical supplies.
- Vendor listings that could be used to expedite the replacement of hardware, software or important supplies that needs to be purchased quickly.
- Important business forms and documentation such as purchase orders that may be required in a disaster situation.
- Information particular to the functionality of a department that would be vital for the continuation of critical business processes.

Backup requirements and recovery strategies for transmitted and received data (electronic media) must be considered.

Review and updation of all data and items maintained in an off-site storage area should take place periodically.

4.8.6 Maintenance and Testing

The objective of testing is to demonstrate that DR Plans and solutions developed and implemented are in line with the DR plans and deliver the capabilities specified. The success of DR is highly dependent on being able to demonstrate that the IT technology and services that are required by the business in support of its Business Continuity Plans are available. BSCB can test the DR Plans by using following test methodologies:

- Structured Walk through - A desk check test of each application belonging to the business products including the interfaces to the business. This should include Call Tree verification
- Scenario Test - An extended desk check based on simulated scenarios and the implied reaction of all involved parties. Some of the scenarios have to be defined in the DR Plans and have to be tested. This should include Call Tree verification

- Alternate Site Test - A test of all Alternate Site facilities connected to the businesses' production site. This should include: a test of the unit's ability to relocate staff to the Alternate Site and Cell Tree verification
- End-to-End Test in conjunction with the business units - A Production Test of the Alternate Site facilities of the supplier - internal or external -connected to the businesses' production site. The test has to be performed in conjunction with the business units

To summarize: Initially, DR drill may be carried out in a test environment for all critical applications, in course of time, DR drill to be carried out the production system. Finally going ahead DRP 100% testing by way of drills.

The aim of the first full-core disaster recovery test is to familiarize the team with the experience of a sudden and unexpected data center move while supporting critical applications. The test would expose many problems and unforeseen situations are likely to arise. BSCB should not expect a successful disaster recovery test the first time. In fact, the full restoration of a complete production environment within pre-established time constraints will require a number of trials.

Ongoing procedures must be established and implemented to provide regular updates to the information contained in the business continuity plan (BCP). The DRP and the BCP should be tested periodically. It should be ensured that there is a gap of not more than 12 months between the two test dates. It is up to the organization's management to identify business units or key operating areas that may require more frequent test, i.e., quarterly or semi-annually.

4.8.6.1 Notification Procedures

Information is valid and current, including:

a. Current names
b. Current business, home and mobile telephone numbers
c. Current home addresses
d. Availability of alternate and vital records when the primary record is not available
e. Mail forwarding procedures
f. Notification procedures should work both during and after business hours

4.8.6.2 Testing

a. The Periodic testing plan should contain the following information:
    - Detail of the areas to be tested
    - Specific dates for each test

b. The periodic test plan should include scheduled tests for the following areas:
   - Integrated Solution)
   - Network (LAN, WAN and SAN)
   - Distribution channels if applicable

c. Periodicity of testing to be defined; gap between two test dates not to exceed twelve months.

d. The DR drill should be carried out ideally on the production system switched to the DR site to ensure that the setup is ready to take over in contingency and should extend over a minimum period of 4-6 hours on a working day.

e. Testing should pertain to the critical components of the plan at frequent intervals

f. When the Plan matures 100% testing shall also to be practiced by way of drills

g. The testing should be reviewed by the internal audit

h. Detail testing documentation should be prepared, and test results documented.

i. BSCB should incorporate disaster recovery plan improvements into its day-to- day procedures.

j. BSCB should have a disaster recovery coordinator who should be responsible for managing tests and observing failures.

k. The regular testing of established plans should provide the basis for which plan maintenance standards are followed.

4.8.6.3 Test Documentation

a. A test plan document should be prepared for every test.

b. The testing documentation should always contain, at a minimum:
   - Test location
   - Test purpose and objectives
   - Measurement criteria
   - Test schedule
   - Test time frame
   - Participants
   - Test script
   - Test result

c. A member of the internal/external audit staff should be scheduled to be in attendance as an observer at each test.

d. As part of test follow-up, the testing team should formalize an evaluation document.

e. The evaluation document should address, at a minimum, the following questions:
   - Were the test objectives met?
   - Was the test accomplished in the planned time frame?
   - Did the test participants perform as intended?
   - Was the testing approach deemed appropriate for this area?
   - Would the recovery personnel in this area be able to use this plan in an effective manner and to recover operations?
   - Were recommended next test/step activities outlined?
   - The follow-up evaluation document, once completed, should be distributed to all interested parties (i.e., senior management, internal audit, etc.).

4.8.7 Recovery Strategy

Disaster Recovery (DR) is the ability to respond to an interruption in services by implementing a plan to restore an organization's critical business functions. Both are differentiated from Loss Prevention Planning, which comprises regularly scheduled activities such as system back-ups, system authentication and authorization (security), Incident scanning, and system usage monitoring (primarily for capacity indications).

A Disaster Recovery Plan (DRP) covers both the hardware and the software required to run critical business applications and the associated processes required to transition smoothly in the event of a natural or technical or human-caused disaster. The DRP detailing what needs to be done in the event of a disaster should be documented. IT should focus on the protection and recovery of application software, information assets, technical infrastructure and facilities.

Generally, DRP comprises those procedures, guidelines and products that allow for the timely resumption of the computer-based activities in the business processes of an enterprise following a significant large-scale interruption in service. The fundamental assumption behind a DRP is that the building where the computers reside is neither usable nor accessible. In this respect, disaster recovery is a separate discipline within the general category of remote site recovery. This has several implications. Disaster recovery presupposes that the data center is not accessible and must be recreated at some other location. Remote backup copies are necessary for successful disaster recovery.

The implementation of a business process approach to DRP ensures that the enterprise's critical business processes of BSCB should continue despite unforeseen events. The team drawing up the business resumption plan begins by defining the specific internal and external constituencies that interact with the business and their expectation/requirement of the products, information or services. Each enterprise has at least three constituencies: current and prospective customers, employees and

investors. Additional constituencies may include vendors, partners, distributors, the public at large, and the board of directors and the press.

Objectives

The objective of the Disaster Recovery Plan in the event of a disaster or a system breakdown is:

- To provide BSCB's operations and business teams a plan, which would ensure an efficient and timely resumption of the interrupted business processes.
- To ensure that the critical operations continue in the event of a crisis
- To minimize the inconvenience and potential disruptions to customers and other stakeholders.
- To provide a sense of security
- To minimize risk of delays
- To guarantee the reliability of standby systems
- To provide a standard for testing the plan
- To minimize the scope for decision-making at the time of a disaster

Management Commitment

Top management (Directors) must support and be involved in the development of the disaster recovery planning process. Management should be responsible for coordinating the disaster recovery plan and ensuring its effectiveness within the organization.

Adequate time and resources must be committed to the development of an effective plan. Resources could include both financial considerations and the effort of all personnel involved.

A planning committee should be appointed to oversee the development and implementation of the Plan. The planning committee should include representatives from all functional areas of the organization. Key committee members should include the operations manager and the data processing manager. The committee also should define the scope of the plan.

Risk Assessment and business impact analysis

Risk assessment should be carried out to identify the critical IT production elements within the IT production environment (such as server, networks, middleware, data networking systems, e-mail). This should cover each of the business and operations units of the organization. Assessment should be made of risks associated with confidentiality, integrity, availability, and accountability issues relative to the operational environment associated with all the sites where BSCB renders customer services and conducts data processing. Specifically, the risk assessment must be conducted relative to

all business units/branches, technology systems, telecommunication systems, and operational internal controls that the BSCB relies on. This ensures that a thorough threat and risk analysis is conducted, and the associated threats and single points-of-failures are identified.

There are potentially three primary threats that need to be addressed:

- Natural threats (e.g., fires, floods, earthquakes, Building Disaster, Campus disaster, act of God)
- Technical threats (e.g., hardware/software failure, power disruption, communication interference, telecommunication failures; rack failure;)
- Human threats (e.g., riots, strikes, disgruntled employees, sabotage etc.)

The risk assessment process should also evaluate the safety of critical documents and vital records.

The plan should provide for the 'worst case' situation: destruction of the data center. It is important to assess the impacts and consequences resulting from loss of information and services. The costs related to minimizing the potential exposures should also be considered.

Disaster Avoidance Measures

Disaster avoidance measures are implemented to address items identified during the risk assessment phase and are intended to reduce the probability of an outage occurring. The availability of existing disaster prevention measures for major risks such as fire, flood, security, sabotage, power failure, housekeeping, fraud or theft, and hardware or software failure should be evaluated. These findings should be noted and recommendations made. The DR should address the following major aspects at the minimum:

Technical areas

The DRP should address the three main technical areas

- Hardware
- Networking
- Software

This covers operating systems, user written applications and third-party software.

An inventory of the software currently used in BSCB's various departments, the current version, license information and support contact information should be kept handy and be available to the concerned employees in case of a disaster scenario.

For customized applications, it is desirable to have the source code and library.

Defining and identifying critical systems

Based on the Business Impact Analysis (BIA) carried out, applications can be categorized into three main categories:

- Critical (essential): Network or application outage or destruction that would cause an extreme disruption to the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore, or the restoration process is disruptive to the business or other systems. Thus, critical system could be defined as an application, the failure of which would have a direct impact on customer service or on regulatory compliance.
- Important (delayed): Network or application outage or destruction that would cause a moderate disruption to the business, would cause minor legal or financial ramifications, or provide problems with access to other systems. The targeted system or data requires a moderate effort to get restored, or the restoration process is disruptive to the system.
- Minor: Network or application outage or destruction that would cause a minor disruption to the business. The targeted systems or network can be easily restored.
- The critical systems list should contain at least the following systems:
  - Stand-alone non-core application systems
  - Internet /mobile based transactions (if applicable)

For each critical application an appropriate, comprehensive and verifiable DRP must be developed, implemented, tested and maintained.

4.8.7.1 Recovery Point Objectives & Recovery Time Objectives

A proper business impact analysis should be done to identify the actual losses i.e., what would be the loss in terms of money which the organization may suffer in case of a complete outage of critical systems or if the data of transactions done in half an hour goes missing in the worst-case scenario. The RTO and RPO should be accordingly defined based on Business Impact Analysis.

At present, as per Service level agreements with different Service Providers, RTO of 120 minutes & RPO of 30 minutes is allowed for recovery, which will be reviewed periodically at regular intervals as and when required after conducting Business Impact Analysis.

Recovery Time Objectives (RTOs)

Scenarios of IT disruption that are anticipated, must consider the length of disruption for each scenario and their respective recovery times, by defining clear parameters to invoke DR Plans within the respective business and operation units.

- The groups are required to define their RTOs on the demand side (business and operation teams) and the supply side (technology teams). They should then carry out a GAP analysis. Based on the analysis it should be decided whether the gap could be bridged using technology or whether manual workarounds need to be built.
- In order to bridge the gap, so assessed, either redundancies should be built up or agreements should be entered into to hire servers on a temporary basis in case of an outage beyond a certain time.
- The limits for RTOs under various circumstances need to be specified
- The RTO for the core systems solution should not exceed 120 minutes from the declaration of disaster
- The RTO for other critical systems identified should not exceed 8 hours from the declaration of disaster, subject to the availability of electricity/telecom facilities.

Recovery Point Objectives (RPOs)

Recovery point objectives (PROs) should also be considered while preparing the plan.

For 'simple' Core application Solution which could be defined as a setup where updates are based only on vouchers and are keyed in by the organization's staff at branches, a RPO of several hours of data loss could be acceptable, as the missing transactions could be re-constituted from the vouchers at the branches.

For 'complex' Core application solutions, where transactions are also triggered from alternative channels - Lost transactions from such channels are more difficult to rebuild. It is desirable to stipulate a RPO of around half an hour.

It should be noted that for most of the other applications there would no instantaneous replication, but log shipping every 30-60 minutes.

Prioritization

Depending on the business requirement and the criticality of the systems, prioritization should be done among various applications e.g., CBS, LOS, AML, EMS, GST, etc.

4.8.7.2 Disaster Recovery Site selection

a. The Disaster Recovery Site (DRS) should ideally be situated in a seismic zone different from the zone where the primary Data Centre is located. This is expected to help avert disaster in case of an earthquake.

b. Additionally, the Disaster Recovery site should have equipped and skilled staff. For improving the

productivity of staff, cross functional training to be considered at the alternate site Redundancies could also be built in.

c. Any remote recovery implies some form of preparedness at the alternate location. This alternate location could also be by way of any of the following:
   - Fully Functional Data Center
   - Equipped Data Center
   - Cold site
   - Parallel running of alternate sites/data centers
   - Outsourced Service center
   - Reciprocal/bilateral arrangement between similar organizations
   - Consortium arrangement among organizations
   - Stand-by equipment supply arrangement with vendors
   - Combinations of the above

d. A fully functional data center with hardware and software, personnel and customer data, typically staffed around the clock, operationally ready in the event of a disaster.

e. An equipped data center that does not have customer data; an organization can install additional equipment and introduce customer data following a disaster. (Hot sites are significantly more expensive to staff. A cold site will require a very rapid process of acquisition and installation of hardware to become useful.)

f. The DRS should ideally be a manned warm/hot site in order to be ready to commence business with minimal disruption

g. The DRS and the data centers should ideally be serviced by multiple service providers i.e. multiple vendors for electricity, telecom, network connectivity etc., to reduce dependency on single vendor in case of a disaster.

Option for arrangements to hire servers for any gap in capacity in case of an outage beyond a certain time could be considered.

Applications Interface: DR should be developed for application interface between the core application software and other software used in various businesses.

While creating Back-up applications at DR Site, it is highly pertinent to take special care of replicating the interfaces among different systems as exist in production environment. This is especially applicable for interfaces of Core application software with various applications of business areas. Interfaces can be on-line or off-line connectivity to core application solution for operations like accounting entry, balance inquiry, validations etc. all such interfaces at the DR site should be in-sync with the Production environment to ensure integrity of Process and Data.

Configuration of the application

The software applications should be configured suitably depending upon the business requirement for the identified application. The entire set up including requirement of hardware and software along with the scope for scalability should be properly documented. Configuration of servers should ideally be standardized.

Based on the risk assessment and the Business Impact Analysis, configuration requirement of the critical systems should be standardized based on the business inputs and requirements. For example, BSCB may take a view that they would size the application on the DR set up at say 100% or 50% of the capacity of the primary setup.

Documentation required

As the capability of the personnel at the DRS may not be similar to that of the production site, all processes should be documented in detail and be made accessible to the personnel at the DRS. Ideally, both soft and hard copies of the manuals should be available to the relevant authorized personnel at the DRS. Periodic disaster recovery drills should also be undertaken to make the staff at the DRS conversant with the processes.

It will depend on several factors and while defining the recovery strategy the following factors have to be considered.

- Criticality of the operation
- The maximum outage time
- Criticality of disaster
- Availability of resources
- Cost involved in the adaptation of a particular strategy

Based on above the separate disaster recovery strategy has to be developed for each of the critical operations.

The process for drawing up the recovery strategy will begin with classifying the operation as per criticality. The operation can be clubbed in four or five categories from most critical operations to the operation where the RPO can be for one day. The recovery strategy can be classified as under.

- Recovery from the previous day back up at another server on the same or near site
- Recovery at the cold site with max. 8 hrs. back up
- Recovery at DR site with RPO and RTO of 6 hrs. backup
- Synchronization of data and system with RPO of 3 hrs. delay

- Online synchronization at DR site Recovery

There can be more strategies for DR, based as per the requirement of recovery. For this, every possible failure has to be identified and divided into various subsets of failures and the strategies have to be based on these subsets of the failures.

4.8.8 Transition / Migration Back to the normal IT production environment

The primary purpose of the transition activities is to ensure that BSCB does not experience any significant difficulties in its move from the alternate recovery site to the restored primary facility. These activities generally being during the site restoration phase of the recovery plan and technically are part of the site restoration. The restored environment must support the pre-event configuration and should have sufficient facilities, hardware, and communications to support the re-established operation.

A major component of transition planning is the development of a migration plan. The migration plan is intended to provide procedures for the actual transition of operations (hardware, telecommunications, and processing) from the alternate recovery site to the restored primary facility. It should be similar to the plans used by the recovery teams to move operations to the alternate recovery site. The location of the site should depend on the severity of the event and the estimated time to restore the primary facility), this component of the transition activities needs to be flexible enough to accommodate any one of several recovery scenarios and sites.

If the transition does not move smoothly, there is the potential for significant delay in the availability of the premises and systems. Therefore, it is critical that this portion of the transition planning activities receive the same attention to details as the procedures used to recover operations at the alternate recovery site.

4.8.8.1 Steps involved in transition

a. Site Readiness

The purpose of this activity is to endure that the restored site is ready to accommodate the normal operations of BSCB's data center. Site readiness comprises facilities, hardware, telecommunications, and staff.

b. Facilities Transition

The facilities transition is composed of five sections covering electrical, HVAC (Heating, Ventilation and Air Conditioning), physical security, fire protection, and furnishings. Site management personnel (as designated by the Support Team (Facilities Management Group Personnel) should be responsible for completing facilities transition, Operations, telecommunications, and vendor

personnel should be working closely with site management personnel to ensure that all of the electrical and HVAC systems meet the specifications of the computer hardware and telecommunications equipment.

c. Hardware Transition

The purpose of the hardware transition is to ensure that proper hardware is installed and tested to provide BSCB branch/office with a configuration equivalent to what existed prior to the disruption. There are two basic components to the hardware transition: an installation plan and an operations check. The installation plan includes all pertinent information needed to install the repaired and replacement equipment at the data center.

d. Telecommunications Transition

The telecommunications transition activities are similar to the hardware transition activities. The primary purpose is to provide for restoration of the telecommunications network to the pre-event configuration. There are two components to the transition, viz., an installation plan, and an operations check of the repaired and replacement equipment. The installation plan should include all of the pertinent information needed to install the repaired and replacement equipment at the concerned branch/office. Once the equipment is installed, a complete operations check should take place. The areas to be addressed by the migration plan are as follows:

e. Off-Site Data Transfer

Once a transfer date is set, the technology team should prepare to move the weekly backups and any incremental backup files created at the alternate recovery site, back to the storage facility. Once the files are moved to the storage site, they must be checked to verify that all the files have arrived. On completion of the migration, the normal process of moving files to an off-site facility must resume as quickly as possible.

f. Operations Restoration

The restoration process should be similar to the one used to recover operations at the alternate site facility. The Technology Team should complete their normal system verification procedures prior to beginning the restoration operations. Restoration of operations can begin after the systems have been restored and tested.

g. Telecommunications Restoration

The Technology Team should begin the process of restoring the telecommunications network concurrently with the systems restoration.

h. Operation Validation

As the systems are restored, telecommunications start functioning, and the processing gets re-established, the testing/validation process should begin. The purpose of the operation validation

phase is to ensure that the systems software and telecommunications features are functioning properly. Telecommunications should be validated first. After successfully testing the circuits, telecommunications operations control should be transferred to the recovery site. While validations of telecommunications and systems software facilities are the key considerations, the Business Resumption team must validate application data. Testing may vary according to the application system. Specifics of data validation are beyond the scope of this recovery plan, but business unit managers must prepare the same.

4.8.9 Vendor BCP

Vendor support should be available also at the DR site for hardware, software & networking. Proper service level agreement for both the site should be entered into. Proper SLA for facilities management to be available at DRS.

Outsourced IT Production Environment functions and/or services must include (as a minimum):

- Reference to the affected contract.
- Precise description of the outsourced functions and/or services.
- Plan for an extended failure of the service provider.
- Overview of all affected IT production elements.

4.8.9.1 Vendor Support Services

Having support services from your major vendors in place adds a strong value to disaster recovery planning. For example, specifically managed hot standby sites or on-site services with rapid response times can significantly ease disaster recovery. Key questions regarding vendor support include:

- Are support contracts in place?
- Has the disaster recovery plan been reviewed by the vendors, and are the vendors included in the escalation processes?
- Does the vendor have sufficient resources to support the disaster recovery?

Most vendors have experience handling disaster situations and can offer additional support and assist with limiting downtime in the case of an unexpected outage.

If the data center itself is outsourced, all associated disaster recovery services should be clearly specified in the outsourcing agreement.

4.8.10 Operational Policies

4.8.10.1 Backup Site Preparation

BSCB needs to equip the DR site with critical equipment's, data files and supplies: Power generators, equivalent IT systems, equipment and parts to replenish any critical assets, digital cameras, basic first aid etc.

4.8.10.2 Testing and maintaining the plan

It is essential that Disaster Recovery Plans be tested periodically. If an arrangement exists for alternative sites, it is desirable that testing takes place utilizing the actual recovery facility. After an exercise, all recovery personnel are responsible for submitting a written report indicating problems encountered and plans for resolution. The plan should be updated to reflect those recommendations.

A management review of the plan should take place at least annually or more frequently when significant changes are made to the applications, hardware or software at a location.

4.8.10.3 Communication/ Awareness/ Distribution

Each IT employee should be aware of his/her role and responsibilities in a recovery effort and should participate in Disaster Recovery tests when possible. All primary and alternate key personnel responsible for participation in the business recovery should maintain a copy of the plan, both at work and at home. (Depending on their assigned roles, it may not be necessary to distribute the entire plan to all individuals.)

BSCB's internal Audit will also maintain a current copy of all Disaster Recovery Plans. The SLA signed with the vendors should contain vendor's commitment in case of a disaster.

4.8.10.4 Alternative sites/ Contingency planning

In the event that a facility is damaged and inaccessible, or a business interruption occurs that requires relocation of the business, then alternative locations would be required. The capacity of an alternate location/recovery site should meet the minimum needs required to address critical processing functions. These needs would be based on the alternative processing strategy, the time required to recover the critical business functions and options for alternate/recovery sites.

4.8.10.5 Risk Analysis

A risk analysis is the process of identifying risks, assessing the critical functions necessary to continue

operations, defining the controls that are in place to reduce exposure, and evaluating the cost for such controls. The risk analysis often involves an evaluation of the likelihood of an occurrence. The risk analysis will be performed on computer/network environments to identify and evaluate risks and determine any disaster mitigation requirements. The risk analysis is generally a collaborative effort of various functions including IT, Facilities Management, Infrastructure Management, General Management, Internal Audit, along with any public utilities and services which support the organization.

4.8.10.6 Existing systems

The existing systems should be evaluated for the extent of compliance with the DR Policy by the DGM / AGM / Chief Officer-IT. If not in compliance, the recovery strategies should be determined and a recovery plan should be documented, which should be tested and maintained annually.

4.8.10.7 New systems

Recovery considerations must be provided within the project charter for all new/upgraded IT systems intended for critical business functions. BSCB's security function, along with business units and IT development areas, should ensure that any system/application being considered for purchase is evaluated for compliance with this Policy.

4.8.10.8 Business Impact Analysis

In addition to the risk analysis, a Business Impact Analysis (BIA) should be performed periodically. The BIA is the process of determining the impact on an organization should a potential loss identified by the risk analysis occurs. BIA includes identifying critical business functions, system dependencies, interfaces, and maximum duration of outage, the consequences and impact if a disruptive event occurs. The BIA should quantify, when possible, the impact of an interruption from a financial standpoint.

The DRP Team, consisting of Business Analysts and technical experts in each of the systems should perform the BIA upon completion of the risk analysis.

4.8.10.9 Near DR Site Selection

BSCB shall consider setting up of a near DR site close to the proximity of primary Data site to ensure minimum data loss during disaster at DC.

4.8.10.10 Maintenance and Testing

a. Arrangements should be made for vendor support at the DR site for hardware, software & networking. Proper service level agreement for the site should be entered into.
b. Periodicity of testing should be at least annually and should be carried out for the critical systems.
c. The DR drill should be carried out ideally on the production system switched to the DR site to ensure that the setup is ready to take over in a contingency
d. Testing should pertain to the critical components of the plan at frequent intervals
e. Testing shall be carried out by conducting two-way drills when the plan matures.
f. The testing should be reviewed by the internal audit.

4.8.10.11 Applications Interface

DR should be developed for application interface between the core software and other software used in various businesses.

While creating Back-up applications at DR Site, it is highly pertinent to take special care of replicating the interfaces among different systems as existing in production environment. This is especially applicable for interfaces of Core software with various applications of business areas like Cheque Management, Mobile app solution. Interfaces can be through on-line or off-line connectivity to core solution for operations like accounting entry, balance inquiry, validations etc. all such interfaces at the DR site should be in-sync with the Production environment to ensure integrity of Process and Data.

4.8.10.12 Configuration of the application

The software applications should be configured suitably depending upon the business requirement for the identified application. The entire set up including requirement of hardware and software along with the scope for scalability should be properly documented. Configuration of servers should ideally be standardized.

4.8.10.13 Documentation required

As the capability of the personnel at the DRS may not be similar to that of the production site, all processes should be documented in detail and be made accessible to the personnel at the DRS. Ideally, both soft and hard copies of the manuals should be available to the relevant authorized personnel at the DRS. Periodic disaster recovery drills should also be undertaken to make the staff at the DRS conversant with the processes.

4.8.10.14 Version control

All DR documents should be dated and there should be proper version control on the DR document. The latest version incorporating all the changes should be available at both the sites. Additionally, personnel at the DRS should be trained on the changes in the application, wherever required.

4.8.10.15 Resiliency and Backup Services

Resiliency and backup services form a key part of the disaster recovery process and be reviewed at regular intervals to ensure that these services continue to meet the criteria set for the disaster recovery plan. Network resilience is the ability to recover from any network failure irrespective of whether the same is related to a disaster, hardware, and design or network services. A high-availability network design may be sufficient to handle some minor or local disasters.

As per recommendation, backup data for both critical and non-critical applications should be present and updated at both DC and DR site and one set should be outside the premises (offsite).

4.8.10.16 Back up of vital records

BSCB must make an inventory of its critical records and the systems that access the same. The critical records should not only include the data sets and databases, but also the applications that access them. BSCB should include application development and production load libraries as part of the suite of critical records that require backup.

4.8.10.17 Backup Storage

The following aspects should be addressed while deciding on the back-up storage facilities:

- Appropriateness of security
- Physical security and controlled access are adequate
- There is enough protection against probable disasters (for example, fire, flood etc.).
- Appropriate assignment of accountability and documentation of the same.
- Documentation of processes and procedures and making the same available and known to the relevant officials
- Labeling is adequate for identification and easy retrieval

4.8.10.18 Risk Mitigation procedures

Physical Security of the IT assets and accessibility

The DR site should be adequately guarded and all access to the same should be strictly monitored preferably through electronic surveillance. Care should be taken to ensure that the same does not prolong the time required to access the DRS location of Diesel Generator set, etc. The DG set should ideally not be located in the basement of a building to avoid the risk of inundation in case of a flood. As the load bearing capacity of higher floors may constraint the movement of DG sets, steps should be taken to ensure that the DG sets are at least installed on a higher platform when they are located in the basement.

4.8.10.19 Personnel Requirement

a. The Disaster Recovery site should be adequately manned with skilled staff
b. As DRS is normally manned with lesser people, they should be conversant with multiple functions and procedures. In order to retain the productivity at the time of disaster, all relevant officials should mandatorily undergo cross-functional training at regular intervals.
c. Employees located close to the DRS may be identified and trained in advance to ensure early commencement of services even when transportation of officials is difficult due to a disaster.
d. Adequate redundancies should also be built in to ensure availability of manpower in case of a disaster.
e. Frequent drills should be carried out at the DR site to keep the staff acquainted and updated with the procedures.

4.8.10.20 Disaster Recovery Emergency Procedures

Disaster Declaration and Notification Disaster Assessment Team (Would also carry out Damage assessment)

This team's prime responsibility is to ascertain whether the situation is grave enough to declare a disaster and to act accordingly. It is suggested that adequate training and authority be given to certain officials at each production/user end to make suitable recommendation to the central/zonal/regional/system team recommending declaration of disaster.

Disaster Declaration Team

The disaster declaration team shall prepare a call tree (contact list) incorporating the organizational hierarchy for invocation of the disaster recovery plan and the escalation procedures. The contact list should contain the name and the contact number of the relevant officials in BSCB and their alternates in case the person having primary responsibility is inaccessible.

Disaster Management Team (Including recovery)

The primary role of this team is to bring up the DR site as production site and to carry out the relevant

changes at DR site for the same. This involves: -

- System setup
- Application setup
- Recovery of database to the latest possible point of time.

If required, the disaster management team should contact the relevant officials in BSCB as well as the vendors/service providers and their alternates in case the person having primary responsibility is inaccessible.

Change Management Team

The primary responsibility of this team is to ensure that any changes being carried out on the production are changed in parallel at the DR site.

Communication to outside agencies/vendors

The public-relations / similar team in BSCB should prepare standard communication steps to be used in case of disasters. The communication to the press/public at large should be released by the authorized officials only in order to avoid any confusion and misunderstanding.

Arrangements should be made for availability of system vendor's officials at the DR site in case of a disaster. The officials in the disaster management team may be authorized to communicate with the vendors. This communication may be through any of the acceptable channels like telephone, mobile phone, electronic mails, facsimiles etc.

4.8.10.21 Switch over/Migration to the DR site

At the time of switch over to the DR site applications, the following are few critical points to be ensured:

- Complete routing of telecom network to the DR location before releasing the DR applications to the users.
- Data integrity check for all DR applications (Including restoration of recent data)
- Interface checking of various applications before release of applications

Application set-up creation, database integration, telecom network redirecting, User- level client application changes are some of the critical steps during switch-over. The switch-over process should be automated to the extent possible, so that elaborate and time-consuming migration procedures are not required at this point.

4.8.10.22 Maintenance and update

BSCB works in an operational environment that could be subject to change. Every DR plan must not stand in isolation from the dynamics of the operational environment. DR Plan and Solution maintenance must be carried out on a cyclic basis, and at times when the technique, process chain, organization or regulatory requirement demand changes, People at the DR site to be communicated of the changes in the systems within 30 calendar days.

4.8.10.23 Plan Maintenance

BSCB's plan maintenance procedures may be divided into two general categories: Scheduled and unscheduled. Scheduled maintenance is time-driven, whereas unscheduled maintenance is event-driven.

4.8.10.24 Scheduled Maintenance

Scheduled maintenance should consist of quarterly reviews and updates as well as annual structured walk-through.

Scheduled maintenance occurs as a result of a time-driven review of the DRP. Reviews are predictable and are scheduled at quarterly intervals. The purpose of the plan review is to determine whether changes are required to strategies, tasks and procedures.

Scheduled maintenance of BSCB's DRP- should be performed as follows: -

- Each DR team leader is to be considered the "Owner" of his team's plan and should be responsible for seeing that it is regularly maintained.
- Each individual team should be responsible for maintaining its own DRP. Each team should meet regularly to discuss changes needed to its plan and implement those changes. Changes include personnel information (e.g., new hire, termination, change of address or phone number), changes to vendor information, changes to minimum operating requirements for systems, applications, and technology.
- Each team leader should appoint an individual from the team who should input necessary changes into the DRP. Each issued plan and subsequent revision should maintain a control number. All older versions of each plan should be returned to the recovery teams for destruction.
- Senior management should meet with the recovery team at a regular frequency to discuss testing issues, plan revisions and recovery plan modification. The evaluation process must address the growth capacity requirements associates with the increase of transaction processing volumes of application systems as well as the addition of new systems to the operation environment.

4.8.10.25 Unscheduled Maintenance

Certain maintenance requirements are unpredictable and cannot be scheduled. The majority of these unscheduled plan changes occur as a result of major changes to hardware configurations, application software, networks, transaction-processing, addition of new FI products, organizational structure, etc. The following are examples of items that may trigger the need for unscheduled maintenance:

- Changes in data processing architectures, hardware, or environmental changes
- Major changes in operating system (s) or utility software programs
- Major Changes in the design of a production system database
- Major changes in communication, systems network design, adapters, etc. (i.e., addition of a communication circuit, etc.)
- Changes in off-site storage facilities and methods of cycling items, etc.
- New application systems development or purchase/Implementation
- Significant modification of basic processes, data flow requirements, and accounting requirements within an application system.

Unscheduled maintenance of DRP may be performed as follows:

- The DR Head must be made aware of all changes to the respective plans resulting from unscheduled maintenance and shall then notify and advise all recovery team leaders and alternates to review their plans and procedures for changes that may be required as a result of the item that has triggered the review.
- The Business Resumption leaders are required to attend unscheduled reviews. BSCB's other staff members may be invited to satisfy the needs of a specific review session. The review shall address events that have occurred within team's area of responsibility that may affect the recovery capability of their DRP.
- Recovery teams should then update their plans with any changes in the manner prescribed above in "Scheduled Maintenance."

The results of regular plan tests must be used to update the recovery planning media (hard copy, software), To ensure that formalized business continuity plans and DRP are being maintained, the following should be created or updated:

- A permanent file for storage of relevant documentation between DRP testing evaluations
- Enterprise -wide DRP testing schedule
- Listing of tests completed since the last DRP test evaluation
- Recovery plan test summaries for tests completed since the last DRP test evaluation
- Audit comments made on the status of testing since the last review

- DRP test related correspondence since the last DRP test evaluation

4.8.10.26 Connectivity to other critical systems

The enterprise must ensure that the disaster recovery plan accounts for all required equipment. Certain applications may have unique processing requirements, such as special telecommunications links, the availability of certain kinds of servers or special finishing equipment.

4.8.10.27 Distribution of DR plan

The DR team is responsible for the distribution of the DR plan. This is accomplished by developing a master distribution list that is based on the need to know and is approved by the senior management/DR sponsors. Careful consideration should be given to identifying recipients. The recovery plan reveals, in great detail, the specifics of the recovery strategy, critical files, names, places, etc. Because of the classified nature of this information, it should not be used for general publication. The DR plan is considered proprietary and confidential. The master distribution list should be maintained in a confidential file.

The distribution and control procedures for the DR plan are outlined below:

- For ease of maintenance, the DR plan should be maintained in an automated form.
- The DR plan hard copy, and the selected automated media should be stored off- site.
- Each recipient should acknowledge receipt of the original plan and updates.
- Each recipient of the DR plan is required to maintain it in a secure location.
- Each recipient of a DR plan is responsible for inserting updates when received.
- Each team leader and alternate team leader should maintain his/her copy of the plan off-site (such as, at home) for immediate use in the event of a disaster.
- Three (3) copies of the DRP should be available. One each in the Data center and DR site and one copy in off-site storage.
- The DRP review with stakeholders should ensure that all issued copies are updated to agree with the master copy maintained.
- It is suggested that the DRP should have various flow diagram and chart indicating activity, timeslots, decision makers and people responsible for each type of DR situation.
- Extending the above, the DRP should also have checklist for the action suggested in the DR situations based on the flow diagram. There will be separate checklist for different operations.

4.9 Hardware Acquisition, Maintenance & Upgradation Policy

4.9.1 Roles and Responsibilities

ROLE	RESPONSIBILITIES
Owner	IT Cell
Implementer & Monitoring	The AGM(SM) as per the Policies and instructions of IT division is responsible for implementation of procedures for hardware acquisition, maintenance and upgradation. All IT Users have secondary responsibility. Monitoring the h/w performance.

4.9.2 Hardware Categorization

- DC/DR Hardware: Server, Storage, router, switch etc.
- HO/Branches Hardware: endpoints (PC, laptop), scanner, printer, external hard drive, LCD monitors, mobile tabs etc.

4.9.3 Capacity Planning

Major IT Asset acquisition should be guided by Capacity Planning.

BSCB runs mission critical applications, hence Systematic Capacity monitoring procedures should be developed. The data collected while conducting such an exercise can be later used for Capacity Planning. The System Administrator of the mission critical application should monitor the systems and capture the technical information.

The data collected must be in conjunction with the following:

- The IT division may be consulted to understand any complaints from users regarding the degradation of performance of their respective applications.
- The IT Chief Officer/AGM must be consulted to gather information regarding the performance of the servers under their purview.
- The operations team must provide a record of the identified performance indicators on their respective servers.

The need for acquisition of new systems for capacity increase should be identified by the concerned Head of the Department supported by the existing system capacity. The projections of future business requirements should be evaluated while planning a system capacity.

Capacity Planning exercise should be carried out by the Functional Team/user department in consultation with the DGM / AGM / Chief Officer / Manager - IT , taking into consideration the technical data regarding the usage of machine capacity for respective systems.

Capacity Planning would address the risk related to poor performance translated into response time degradation of the mission critical systems and would help the IT to justify to the management for the expenditure to be incurred during the financial year.

Approach to conduct capacity planning-

This activity can be broken down into: -

- Data Gathering
- Model Construction
- Documentation of alternatives

4.9.3.1 Data Gathering

Types of measurement that are required, per major application area are Hardware Usage, Workload and Program Measurement. It is at the discretion of the Functional Head/departmental Head to decide the extent and content of data (as listed below) that needs to be captured depending on the criticality of the server.

The Hardware usage can be computed by collecting data related to CPU, Channels, Control units, and storage devices, number of read/write operations, data set contention and bus contention.

The Workload of the servers can be monitored based on the following parameters

- Number of jobs running concurrently
- Turnaround time
- Transactions per time period
- Total number of transactions
- Transaction types (batch, real-time, database)

The response time would also depend upon the following parameters, which would enable monitor the program measurement

- Location of instructions being executed

- Percentage of time spent executing instructions
- Percentage of time spent waiting for completion of input/output
- Paging activity

4.9.3.2 Model Construction

Future capacity demands should be computed by mapping the expected growth in business and considering the current and projected trends of information processing, new business, and system requirements to ensure adequate processing power and storage. The forecasted capacity utilization should consider the desired service levels (e.g., response times, turnaround times etc.).

Appropriate software and hardware tools should be used to gather the data required, e.g., Platform Migration tool.

4.9.3.3 Documentation of Alternatives

The information collected on identification of trends of usage related to business application should be presented to the IT- DGM / AGM / Chief Officer / Manager enabling him to identify and avoid potential bottlenecks that might present a threat to system security or user services and plan appropriate remedial action.

4.9.4 Environmental checks

a. Dust-free/ smoke-free and temperature-controlled environment for network equipment such as Firewalls/routers/modems/switches etc. should be maintained.

b. Humidity controls and optimum humidity levels need to be maintained as a part of the environment in which the hardware, systems are stored.

c. CO2 type fire extinguishers should be strategically placed in computer area, refilled in time, and maintained properly.

d. Computer area should be free from water leakage, dampness etc.

e. UPS should be maintained properly, and the water level of batteries checked and maintained regularly.

f. UPS should be kept out of reach of public to avoid accidental switching off.

g. Digital Generator should be maintained periodically. E.g. servicing, Refueling etc.

h. Pest Prevention/Rodent Prevention measures should be taken-.

i. The Electrical/Electronic Items such as AC, fan etc. should be under maintenance/Annual Maintenance Cost (AMC).

j. Computer and its peripheral should be covered to protect from dust.

4.9.5 Acquisition of Hardware

Acquisition of hardware system should support capacity planning. Where necessary, hardware is checked to ensure that they are compatible with other system components. The routine hardware purchases would be as per the budgetary sanctions and procurement rules of BSCB.

4.9.5.1 System Acceptance Criteria

An acceptance criterion for new critical information systems, upgrades and new versions should be established by HO-IT and suitable tests of the system should be carried out prior to acceptance. The User Department and IT team ensures that the requirements and criteria for acceptances of new systems are clearly defined, agreed, documented and tested. The following controls may be considered:

- Validation of Hardware Specifications in conjunction with the Bill of material
- Power On tests should be conducted before installing / accepting hardware into the BSCB environment.
- Restart procedures, and contingency plans.
- Agreed set of security controls in place. (e.g.:
- Business continuity arrangements.
- Evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times (e.g., in the daytime).
- Evidence that consideration has been given to the effect the new system has on the overall security of the organization.
- User training on operating of new systems
- Appropriate tests are carried out to confirm that all acceptance criteria are fully satisfied.

4.9.5.2 Asset Tracking

Branch/regional office and department using computer systems should also maintain their own inventory as per the Policies of BSCB. This should necessarily involve the following procedures:

- Maintain updated asset records
- Labeling and numbering of assets, such that each asset has a unique ID, which displays the location of the asset.
- Updating inventory details of hardware.
- Periodic physical verification of assets deployed across BSCB.

4.9.5.3 Process of Asset Updation (Addition, Deletion or Modification)

a. For creating any server, IT Server support team seek for an approval from functional head/departmental head along with Head IT Infra & Operation's approval.
b. After getting the approval, Server support team creates a server and hand it over to respective Application team (Bank/vendor). The details of the server been added in Asset Inventory.
c. For any infrastructure related support, the respective application team (Vendor/bank) reaches out to server support team for any kind of assistance.
d. For deleting or modifying any server details, the server team seek the same approval from Functional Head/Dept Head and Head IT Infra & Operation.
e. For any IT Asset updation like addition, deletion or modification, approval required from Head – IT Infra & Operations, and the team shall log a ticket for tracking of the changes made.
f. For any asset update (addition, deletion, modification) if the update is within the banking unit, then the team updates the required field as per the instructions of the banking unit head only. If the update/change is between the two banking units, then after approval from Head – IT Operations, the changes are incorporated by the IT support team.
g. A proper naming convention should be followed for all the IT Assets like DC Server, DR Server, End Points, Workstation, Application, Biometric Device, CCTV, Monitor, Laptop (Branch & HO), Desktop (Branch & HO), Network Devices etc.

4.9.5.4 IT Asset Update & Review

All the IT Assets should be tracked and updated by dedicated IT asset management team every day whenever there is any update in IT asset to record. A dedicated IT asset

management team member will review the IT asset items on quarterly basis and the same will be reported to the lead IT Infrastructure.

4.9.6 Disposal of IT Assets

4.9.6.1 Disposal Methods

Acceptable methods for the disposal of IT assets are as follows:

- Reassigned to a less-critical business operation function.
- Used as a trade-in against cost of replacement item.
- Sold to existing / retired employees.
- Auctioned through Tendering process by issuing a public notice through either of the following: BSCB's Website/Newspaper/Notice Board of branch / office
- Donated to schools, charities, old age homes, and home for orphans, libraries and other similar organizations.
- Recycled and/or refurbished to leverage further use (within limits of reasonable repair).
- Sold as scrap to a dealer.

4.9.6.2 Obsolete Assets

As prescribed above, "obsolete" refers to any and all computer or computer-related equipment with approximate lifespan (as decided by BSCB concerned authority / department) as mentioned below and/or equipment that no longer meets requisite functionality:

a)	UPS batteries:	3 years
b)	Inkjet printer / Scanners:	5 years
c)	Laptop / iPAD etc. allotted to Individuals:	5 years
d)	Desktop / Thin Client / UPS / network equipment/CCTV/others:	5 years
e)	Servers:	5 years

However, ordinarily no IT asset will be declared obsolete if it has been upgraded within last three months.

4.9.6.3 Surplus IT Assets

It refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

4.9.6.4 IT Assets Beyond reasonable repair

It refers to all equipment whose condition requires fixing or refurbishing that will entail cost equal to or more than total replacement. It requires certification by vendor or IT official.

4.9.6.5 Returning of the hired PCs / storage

The hired PCs or storage hired in the Tech Park shall be returned only after formatting the hard disk. All the media accompanying the hired PCs shall be formatted before returning.

4.9.6.6 Process of Disposal

a. **Reassignment of Retired Assets:** Reassignment of computer hardware to a less-critical role is made at the sole discretion of the competent authority.

b. **Trade-Ins**: Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable action must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement.

c. **Auction**: The IT assets identified for disposal should be serially numbered. The list along with the public notice prepared for a particular auction may be published through either of the following: BSCB's Website/Newspapers/Notice Board of branch/office or by invitation.

d. The auction notice should contain last date, time, place of submission bids and contact person. Items to be disposed should be auctioned "on as is where is and what is there is" basis. Bids should be opened at predetermined time in presence of a committee of two or more officials of the office/branch in which the Bidder may also participate and the Items should be awarded to the highest bidder.

e. However, preference may be given to the existing/retired employees of the organization by conducting an in-house auction for employees only by publishing on notice board before initiating public auction.

f. **Donations:** The working condition but obsolete IT assets identified for disposal may be donated to schools/ colleges, charities, old age homes, home for orphans, libraries, and other similar organizations to earn goodwill in return.

g. **Sale to scrap dealer:** Where it is not possible to reuse, sell or donate the IT assets, the same may be sold as scrap-to-scrap dealer/s by invitation.

h. **Decommissioning of Assets:** All hardware slated for disposal by any means must be fully wiped clean of all the organization's data.

- Hard disk of critical servers should not be disposed. It should be broken down into smaller parts and to be disposed off separately.
- Server disposal to be handled by Head Office only.
- Assets such as laptops, iPADs etc. after 5 years to be deleted from Asset register and to be transferred in the name of the individual to whom it is allotted after charging a nominal value after depreciation **and subsequently new device to be issued. Further, individuals attaining superannuation on or before 5 years may retain Laptop/IPAD allotted by paying written down value.**

i. **Income Derived from Disposal:** Whenever possible, it is desirable to achieve some residual value from retired or surplus IT assets. However, this desirability is not intended to become a deterrent against donations or quick disposal. The decision of the competent authority will be final.

j. **Record Keeping:** The IT assets so disposed must be deleted from the Asset Register with proper noting. A separate Register should be maintained by the disposing authority incorporating the following information:

- Item description (Desktop PC, printer, scanner, etc.)
- Purchase** value
- Date purchased**
- Date discarded
- Method of disposal (sold/donated/recycled)
- Amount of proceeds (if sold)
- Details of documents, if any, such as certificate of destruction, bill of sale, receipt etc.
- Receiver's particulars & acknowledgement
- Signature of the Head of the Branch/Office/Corporate division at HO

**As some IT items identified for disposal may be quite old and were purchased long back, the exact date of purchase and purchase value may not be readily available / traceable. In such a situation, the tentative/approximate year of purchase and value are to be certified by steering committee.

4.9.7 Management and Operation of IT Assets

4.9.7.1 Operational procedures and responsibilities

Responsibilities and procedures for the management and operation of all IT hardware assets should be established. These include the development of appropriate operating instructions and incident response procedures. Segregation of duties is ensured, where appropriate, to reduce the risk of negligent or deliberate system misuse.

4.9.7.2 Documentation & Maintenance of operational procedures

The operating procedures for each critical IT asset should be documented and maintained by the respective Department/Branch. Operating procedures will be treated as formal documents. The Operational procedures for the maintenance of the applications are the responsibility of the respective Project Leaders/Functional Head. The procedures should specify the instructions for the detailed execution of each job and should include following:

- System startup and close-down procedures
- Back-up of information, equipment maintenance
- Processing and handling of information.
- Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities
- Support contacts in the event of unexpected operational or technical difficulties
- System restart and recovery procedures for use in the event of system failure
- Computer room security.

4.9.7.3 Operations Change Management Process

It should be ensured that changes to information processing facilities and systems are controlled. Inadequate control of changes to information processing facilities and systems is a common cause of

system or security failures. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. In particular, the following controls should be considered:

- Identification and recording of significant changes.
- Assessment of the potential impact of such changes.
- Formal approval procedure for proposed changes.
- Communication of change details to all relevant persons.
- Procedures identifying responsibilities for aborting and recovering from unsuccessful changes.
- Allocation of specific responsibilities and procedures to effectively monitor all relevant security activities
- Responsibilities and procedures for reporting and handling security incidents.

4.9.7.4 Maintenance of Hardware

Hardware maintenance refers to all activities involved in the upkeep, repair, and review of hardware resources after the installation to ensure proper functioning, correction of faults, improvement in the performance and adaptation of the hardware in the IT environment.

During the purchase of equipment's, the contract contains the clause of AMC, because of which the vendor promises to maintain the functionality of the facility for a given duration of time. During that period, if any component is rendered useless, or becomes defective, the vendor replaces it with a functional unit without any extra purchasing cost paid by the bank. Once an AMC expires, generally it is renewed with the same vendor. In case the previous vendor is unwilling to extend the coverage, then a new vendor is sought for to cover the equipment's. When the assets are replaced by the vendor, IT team ensures that the data present in the IT assets are being hard formatted.

4.9.7.5 Repairs and Maintenance

a. Maintenance of all equipment should be governed by the Warranty / Maintenance Contract entered with the respective Suppliers/ Agents. The third party shall sign a Non-Disclosure Agreement with BSCB to the effect that they shall not disclose any confidential information that they encounter in the course of their work.

b. The Authorized Department should settle bills only after the user department/branch certifies that the repairs/services have been carried out satisfactorily. For this purpose, concerned department/Branch shall maintain a Register indicating all particulars of routine maintenance and repairs carried out on such equipment at BSCB. It should necessarily document the maximum

turnaround time for a maintenance call and the desired service level as agreed with the hardware vendor.

c. It should also be noted that, to prevent unauthorized disclosure of data when computers are sent out for repair or used by others within or outside the BSCB and data cannot be deleted; all data stored on hard disks must be encrypted via user-transparent processes.

4.9.7.6 Items Not In AMC

Whenever IT assets are not under AMC then permission from competent authority to be obtained for procurement of spares on need basis for maintenance purpose.

4.9.7.7 Movement of Hardware outside BSCB for maintenance

a. In case of computer hardware being sent out of BSCB for repairs or other maintenance work, Departmental/Branch Head should approve it.

b. A complete analysis of data residing on the computer hardware (if any) should be carried out.

c. The concerned data owner(s) should analyze the data and depending upon the classification of the data, appropriate security procedures should be followed before sending the hardware out. This may include removing the data from the hardware going out for repairs and backing it up in other systems at BSCB and dispatching the hardware without any live data.

d. An approval from the OEM to move the computer hardware outside the BSCB facility should be obtained. Any methodological, special provisions through which the Hardware is required to be moved maybe specified by the OEM. The same needs to be complied with by BSCB.

4.9.7.8 Asset Surrender

Whenever the asset owner of an IT network device changes, the device is sent back to the Head Office by the branch manager. The device is inspected, and the data deletion is performed by the IT Support Team. The logs are maintained of the data formatting activity by the team, as and when required it is assigned to a new employee. Once the employee logs into the system, the IT Support Team should update the identifiers of that device to the new user. In the hyphen period between the surrender of the asset, and the re-allocating of the same to a new employee, the asset ownership lies with the IT End User Support Team. If in case a device is used by multiple users, the department head will be the asset owner. All these processes must have trackers with the respective departments which will be tracked and reviewed on a regular basis.

4.9.7.9 Loss & Retrieval of IT Assets

BSCB shall ensure that any loss of End User device shall be reported to Local Helpdesk to be tracked and logged with Legal, ITAM (Information Technology Asset Management), Security and remote wipe actions taken. BSCB shall include the return of issued physical and electronic assets belonging to Corporate in employee and third-party termination and separation processes. There shall be a process in place for the return of BSCB's assets in their possession on termination of their employment, as per contractual agreements and the Human Resource Security Policy and related standards.
In cases where an employee or a third-party user purchases an asset for BSCB use or uses their own personal asset for official use, appropriate procedures shall be followed so that sensitive BSCB information is securely stored in the asset. Following usage, the sensitive data shall be erased from the asset.

BSCB shall terminate access to sensitive BSCB information by employees, third parties and contractors post separation.

Any computing or communications equipment shall be examined by the IT Department and internal information shall be retrieved or destroyed from the device prior to reuse of the device or issuance to another employee.

4.9.7.10 Transportation of IT Assets

BSCB shall ensure that all media being transferred shall be correctly labelled and measures such as media encryption implemented before transportation takes place.

All transfers, replacement, or other physical movement of hardware will be reported according to established procedures and logged in central inventory tracking tool.

BSCB shall enable a process to track and protect media containing nonpublic data, putting in place appropriate security safeguards such as encryption of data on the media and lockable physical containers for transportation.

A BSCB media inventory for offsite transfers of media containing nonpublic data shall be maintained to keep a record of any transfers; and shall record the contents, date and time, name of the custodian and recipient of the asset(s) being transferred.

4.9.7.11 Acceptable Use of Technology Assets

Employees and third-party users having access to the BSCB's assets shall be made aware of the information security requirements of BSCB's assets. Employees and third-party users shall be made accountable for their use of any information processing resources and/or any such use carried out under their responsibility.

- In the event BSCB's IT assets are assigned to contractors, procedures for assigning and monitoring the use of the technology asset shall be included in the contract.

- If BSCB-owned IT assets are assigned to volunteer workers, there shall be a written agreement specifying how and when the property will be inventoried and how it shall be returned upon completion of the volunteer assignment.

Individuals shall be assigned only the assets they need to perform BSCB business as part of their role. Documented approval by the Line Manager is required for each additional computing systems/devices assigned to a user. All requests for IT assets or upgrades to these devices (e.g., faster processor, additional memory, or larger hard drive) require documented Enterprise Architecture Lead approval. BSCB need to have an authorization process for new technology assets that includes the following:

- IT assets (internal to BSCB or via a service provided by a third party) shall have appropriate user management authorization of their purpose and use.
- Authorization shall also be obtained from the manager responsible for maintaining the local information system security environment such that relevant security policies and standards are met.
- A technology asset shall employ appropriate security measures, such as cryptographic controls, commensurate with the type of information the technology asset will collect, store, process, or transmit.
- The technology asset shall operate in compliance with applicable laws, regulations, policies, and standards.
- Hardware and software shall be checked for compatibility with other system components.
- Establishing policies, standards, and procedures that include the security organization in procurement considerations for new IT assets.
- All BSCB assets that process nonpublic BSCB information shall be reviewed on an annual basis for their continued suitability to process this information. All BSCB nonpublic information that is available on BSCB assets shall be reviewed annually to ensure their continuing suitability, adequacy, and accuracy.

4.9.7.12 Standard Practices for Maintenance of IT Assets

Equipment needs to be appropriately maintained to ensure its continued availability and integrity.

The following controls should be implemented to achieve that objective:

a. Systems Administrators/Chief Officer-IT/Branch Heads are responsible for ensuring proper maintenance of the IT assets allotted to them.

b. Department/controlling Offices/Branch Office should maintain list of all the IT assets.

c. Equipment is maintained in accordance with the OEM's recommended service intervals and specifications.

d. Only authorized maintenance personnel are allowed to carry out repairs and servicing of equipment.

e. Records are maintained for all faults and all preventive and corrective maintenance.

f. The maintenance personnel from AMC vendors are adequately monitored during maintenance operations. In case the IT asset needs to be sent out for maintenance, then documentation is prepared to ensure traceability and accountability.

g. Appropriate care is taken while sending equipment off premises for maintenance.

h. Requirements of insurance Policies related to IT assets, if any, are complied with

4.9.8 Annexure

4.9.8.1 System Capacity Monitoring

S. No.	Existing Server Specification	Date of Procurement	End of Life	Problems Detected	Data Backup	New Hardware Installation	Platform Migration	Data Migration / Restoration	Data Check

Note: The above format can be used or there are several server monitoring tools available online that can be used to carry out the system capacity planning activity more accurately.

4.10 Incident Management Policy

4.10.1 Roles & Responsibilities

ROLE	RESPONSIBILITIES
Implementation	Users are expected to know whom to report the incident. Chief Information Security Officer (CISO) is expected to constitute CSIRT
Monitoring & Supervision	AGM–IT/System and Networks team
Escalation	GM-IT

4.10.2 Risk Assessment

THREAT	LIKELIHOOD	IMPACT
Incident not detected	High	High
Incident detected but not handled.	Medium	High
Incident detected, handled but not escalated	High	High

4.10.3 Punitive Action for Violation

Sr. No.	Description of Violation	HIGH	MEDIUM	LOW
1	Failure to report an incident	ü		
2	Failure to constitute CSIRT	ü		
3	Non-Adherence to the Escalation Procedure		ü	
4	Improper management of incident, due to negligence or gross incompetence (such as failure to take corrective action within the necessary time)		ü	
5	Failure by third parties to give sufficient notice to BSCB before initiating any change that could be described or could lead to an incident.		ü	

The action to be taken against the individual/group in violation of the Policy shall be decided by the IT Steering Committee depending on the severity and circumstances.

4.10.4 Operational Policies

4.10.4.1 Establishment of CSIRT

BSCB should establish a Computer Security Incident Response Team (CSIRT)to handle reported incidents. The team should consist of Security Manager, Head, IT division, an external expert on Security Incidents and 3 end users.

Charter of CSIRT

The CSIRT must have a charter which specifies what it should do, and the authority under which it will do it. The charter should include at least the following items:

- Mission statement
- Constituency
- Sponsorship / affiliation
- Authority

Functions of CSIRT

CSIRT will assist system administrators in handling the technical and organizational aspects of incidents. It will provide assistance or advice with respect to the following aspects of incident management

a. Incident Triage

- Investigating whether an incident occurred.
- Determining the extent of the incident.

b. Incident Coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other similar sites who have reported the incident (if applicable).
- Facilitating contact with appropriate law enforcement officials (i.e. the Government Cyber Security), if necessary.
- Sharing reports to other CSIRTs.
- Send out notifications to users, if applicable.

c. Incident Resolution

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of

evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.

- Collecting evidence where criminal prosecution, or
- Disciplinary action, if contemplated.

d. Data Collection & Analysis

In addition, CSIRT will collect statistics concerning incidents which occur within or involve BSCB information resources and will notify the relevant parties proactively as necessary to assist it in protecting against known attacks.

e. Incident Classification, Categorization and Prioritization

- The incident should be classified by the Incident Response Team (IRT) into the following categories:
  - Hardware
  - Software
  - Network
  - Services
  - Others
  - People
- Further sub-classification to the next level of granularity should be performed by the Incident Response Team (IRT)
- The incident must be categorized into security incident, major incident by the Incident Response Team (IRT)

f. Policies for Major Incident

The following criteria can be considered while determining if an incident is a major incident:

Functional Area	Criteria
Financial	Incidents that could potentially lead to a loss.
Service	1. If there is down time in service. 2. If branch is down for more than one day.
Site	Incident has affected more than one branch/site.
Service Level	Incident has affected critical service level targets that could result in financial penalty.
Reputation	Incident may malign the brand image or popularity.

Security	Incident has resulted or has highlighted a major security flaw or compromise.
Health and Safety	Incident has resulted in the deterioration of the health and safety of personnel, systems and/or infrastructure.

- Configuration Items (CIs) affected by the incident should be identified by the Incident Response Team (IRT). An impact analysis on the CIs affected by the incident should be performed by the Incident Response Team (IRT). This should identify the service(s) affected by the incident.
- Urgency of resolution of incident should be determined on the basis of user input provided as part of the incident details or determined by the nature of incident and affected CIs. In case of difference between the two, the urgency should be determined by the nature of incident.
- Depending upon the nature of the incident, the incident should be assigned to the respective support groups by the Incident Response Team (IRT).

g. Incident Investigation & Diagnosis

- The Support Team (which may comprise of System Integrator's team and few members of IT division) should provide the initial support to resolve the incident to the satisfaction of the Incident notifier based on results obtained by matching the reported incident to a Known Error / Solution History / Knowledge Repository. Wherever possible, the Incident Notifier should be provided with means to continue the work interrupted by the incident, even if only with a degraded service.
- Each of the Support Team involved with incident handling should investigate and diagnose what has gone wrong. All investigation and diagnosis should be fully documented in the incident record so as to maintain the complete historical record of all incidents.

h. Incident Recovery

- Once the potential resolution/workaround has been identified, the same should be tested by the Support Team. Wherever possible /applicable testing of the resolution / workaround should be performed in the test environment. The test environment should mirror the live environment as closely as possible. Even when the resolution has been found, sufficient testing should be performed to ensure that the recovery actions are complete.
- In case the incident is categorized as Major Incident, the categorization of the incident should be initially approved by the Subject Matter Expert and subsequently by the Incident Manager

i. Incident Closure

- It should be checked that the incident is fully resolved, and the Incident Notifier is satisfied and willing to agree that the incident should be closed.

- While closing the incident record the following should be performed by the Incident Response Team (IRT):
  - Checking and confirming that the initial incident categorization / classification was correct. In case of incorrect categorization/classification, updating the record store reflect the correct data.
  - Obtaining a feedback from the Incident Notifier on the satisfaction of incident resolution
  - Checking the completeness of the documentation associated with incident record.
  - Deciding whether it is likely that the incident could reoccur and determining any preventive action to avoid this.
  - Changing the status of incident to 'Resolved'.
- Once the Incident Notifier confirms the closure of incident, the incident status should be changed to 'Resolved' (or 'Technically closed'). Subsequently, after 48 hours the incident should be closed automatically, or the incident status changed to 'Closed'. The Incident Notifier has an option to force close or reopen the incident within these 48 hours.
- The Knowledge Repository should be updated by the incident response team with any additional knowledge /know – how / learning / resolution / workaround / checklist / initial support actions encountered during incident lifecycle.
- The incident record should be periodically reviewed to ensure timely closure of incidents. Based on the review findings, escalations or corrective actions should be taken as required.

4.10.4.2 Information Services

List of departmental security contacts, administrative and technical should be made available to all the users in BSCB and general public, via commonly available channels such as the Intranet/World Wide Web and/or the Domain Name Service.

4.10.4.3 Auditing Services

Central file integrity checking service to be done for various servers.

4.10.4.4 Archiving Services

Records of previous security incidents handled should be stored. While the records would remain confidential, periodic statistical reports would be made available to BSCB's users.

4.10.4.5 Detection and initial reporting

An incident may be detected by anybody in BSCB. The concerned personnel should immediately bring it to the notice of the person designated by CSIRT. The person so designated should escalate the issue as per escalation Policies.

4.10.4.6 Documentation and formal reporting by CSIRT

A person designated by CSIRT should maintain the central database of all such incidents. The person so designated, after analyzing the extent of exception and facts of the incident, should appraise the CSIRT. A detailed risk and impact analysis for the incident should be carried out by the CSIRT. It should be the responsibility of the CSIRT to ensure that all incidents are categorized based on the nature of each incident and are held in a database created for the purpose. The database should be able to provide information on demand and have the capability to perform analysis on the data contained within. BSCB employees encountering incidents would thus be able to access the incident database and possibly find solutions if the incident had occurred before. Frequently asked questions should also be incorporated into the database to assist the user in finding solutions to incidents encountered.

4.10.4.7 Monitoring

All the major incidents should be reviewed and monitored by DGM / AGM / Chief Officer / Manager every month and discussed in the Information Technology Steering Committee meeting. The magnitude and criticality of the incidents may prompt the designated ISM to discuss and take action on the incidents immediately instead of at fixed intervals.

4.10.4.8 Development of corrective action plan

The CSIRT, in consultation with effected System administrator or any other person it deems fit should prepare the corrective action plan for the incident. The action plan, though specific to each case, should typically cover the following:

a. Facts and explanation / reasons for the incident
b. Corrective action to be taken
c. Estimated cost of implementing the corrective action
d. Estimated time frame, start date and end date
e. Personnel responsible for taking the action

4.10.4.9 Confidential Information sharing Policies

The following information will not be released by CSIRT for general public:

a. Private user information about particular users, or in some cases, particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons. However, if the identity of the user is disguised, then the information can be released freely (for example to show a sample .cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).
b. Private site information of the technical nature except with explicit permission of the site in question.
c. Vulnerability information without informing the relevant vendor a week in advance. However, if the

vendor fails to respond within a week, BSCB will be at its discretion to release the information at any forum it deems fit.

d. Any information that has been classified as confidential or restricted.

4.10.4.10 Escalation Procedures

The central principles of the escalation process:

a. All incidents for which this process is invoked will always be resolved at the lowest possible level of escalation.

b. Contact between provider organizations will always be between organizational peers. That is, the point of contact for a lower level of criticality will not directly contact the point of contact for a higher level of criticality within another provider's organization.

c. Exceptions to the latter may be made only by explicit mutual agreement on a per-incident basis.

Levels of Escalation

- **Level One -** Escalation Level One is the initial level for all incidents. The contact must be available 24 x 365. The contacts at this level must have the ability to call IT official to take action and escalate to management as required, to resolve all categories and severity of incidents. This level consists of Helpdesk management executives or System Administrators.
- **Level Two -** Escalation Level Two represents the next level of management. Escalation to this level is appropriate only when Level One interaction has failed to result in resolution and further action transcends the authority of Level - One staff. This level consists of the AGM-IT/GM-IT.
- **Level Three -** Escalation Level Three represents senior management with authority to take actions that fall outside the standard operating Policies of the concerned organizations. Escalation to Level Three is appropriate in cases where Level - One and Level-Two interactions have been unsuccessful in resolving an operational issue. This level consists of the Chief Information Security Officer (CISO).

4.10.4.11 Points of Contact

Point-of-contact information is required for each escalation level defined above. Telephone numbers and email addresses are required for each level.

4.10.5 Annexures

4.10.5.1 Annexure 1 - Incident Reporting Form

Department:	**Date:**
Name of the Employee:	**Division:**
Facts of the incident:	
Signature:	

4.10.5.2 Annexure 2 - Reporting of the Incident to Manager, IT Division

Department:	**Date:**
Incident Reported by:	**Incident Occurred on:**
Facts of the incident:	
Analysis of the incident by Head of Department/Division and impact:	
Signature: Systems Administrator/ Operator in-charge of the branch	**Signature:** **AGM**

4.10.5.3 Annexure 3 - Incident management –Manager, IT Division

Incident Number:			**Incident Date:**		
Branch:			**Date of reporting from the branch:**		
Facts of the incident:					
Risk and impact analysis:					
Discussed with IT Committee on:					
Corrective Action plan for incident management:					
Sr. No.	**Corrective Action**	**Responsibility**	**Start Date**	**Expected Date of Completion**	**Estimated Cost**
Signature: DGM, IT Division Date:					

4.11 License Management Policy

4.11.1 Roles and Responsibilities

ROLE	RESPONSIBILITY
Owner	IT Department
Implementer	The AGM-IT and the IT team as well as all users are responsible for implementing and executing the procedures.
Supervision &Monitoring	GM – IT should monitor the execution of the procedures.
Employees	Employees shall follow this Policy and all software usage Policies and procedures. Users should report any misuse or policy violations to their AGM-IT.

4.11.2 Operational Policies

4.11.2.1 Software inventory

a. **Category** A – Approved software – which can be installed for all types of users

b. **Category** B – Prohibited software – which should not be installed on BSCB hardware for any user

c. **Category** C – Restricted software – which require permission from Functional Head/System Administrator prior to installation

The inventory is to be updated on a **quarterly basis.**

4.11.2.2 Software Licenses

At every inventory update, the System Administrator needs to ensure that all software falling in Category A and C have a valid license for the next quarter, except for software that may not require license for usage.

Acquisition of new software or additional licenses for current software must be planned on an annual basis to ensure that it is carried out in a controlled manner. Such requests need to be sent to the System Administrator by the Functional Heads.

The procurement of new software / additional licenses must be based on evaluation of current usage and formally established need for additional licenses across BSCB.

a. Conflicts between law and Policy

Where a Conflict arises between national and/or local laws and BSCB's Policy, the law should be complied and the Manager - IT Division must be notified of this situation by the concerned OEM representative / Auditor / Procurement Officer of BSCB.

b. Compliance with law

The Functional Heads/User department In-charges/ Branch Heads should ensure full compliance of the laws and regulations relating to their information and the IT applications that process that information. The laws and regulations may include, among others:

- Prohibition of the use of illegally acquired software
- Prohibition of the use of illegally acquired data

c. Control of Software Licenses

Software Licenses within the IT shall be controlled and maintained to ensure protection against default or contractual and/or other limitations and liabilities.

d. Software License terms and conditions

Software License terms and conditions, including those applying to limited use, shall be always observed.

e. Illegally acquired software

Illegally acquired software shall not be loaded on to computer systems used by BSCB.

f. Authorization Required to Copy Licensed Products

Products licensed to run on a specific server shall not be copied onto another server or another site without written authorization from the vendor. Sharing of license with other agency or organization shall be prohibited.

4.11.2.3 Procedures for Hiring of PCs

a. Hiring of PCs

Hiring of PCs should not be allowed. In exceptional circumstances, special permission should be taken from the Manager– IT Division.

b. Licensing of hired PCs

It should be ensured that there is no illegal data in the hired PCs. It should be loaded only with licensed software and the vendor should provide the copy of an original paper License. This copy

shall be retained by the concerned team/department/branch and returned to the vendor on returning the PC. The concerned team/department/branch must inform the vendor that the hired PC's will be returned only after complete formatting of the hard disk and other media accompanying the PC.

c. Checking for genuine anti-virus license

The concerned team / department / branch with the help of the anti-virus software / helpdesk (if separate department is present) shall check the hired PCs for the existence of genuine anti-virus license.

d. Monitoring of the Licenses for software installed on the hired PCs

The concerned team/department/branch should separately monitor the software installed on the hired PCs

e. Returning of the hired PCs / storage

The hired PCs or storage hired in the Tech Park shall be returned only after formatting the hard disk. All the media accompanying the hired PCs shall be formatted before returning.

The IT assets for disposal shall be cleansed of any specific licensed / proprietary software and data, by the IT department.

4.11.2.4 Demo Copies of Software

a. Installation of Demo Copies

The IT department employees must necessarily inform their respective heads (Manager– IT Division) in case they want to install any demo software on their respective machines.

b. Tracking of demo copies

The IT department shall keep a record of the demo copies installed on the machines.

c. Uninstallation of demo copies

The IT department shall monitor the demo copies to ensure that once the purpose of the demo copy or the time frame is over, the demo software has been uninstalled.

d. Freeware

Freeware is a software distributed / downloaded at no cost to the user. There must be a formal process to monitor the installation and timeframe of evaluation software. The IT team must review

the security risks associated with installing freeware and must subsequently authorize requests to install the same.

e. Tracking of freeware

Freeware should be installed only after taking permission of the Manager - IT. The IT team shall keep a record of the freeware installed on the machines of the IT.

f. Un-installation of Freeware

The IT team in charge of the respective systems shall uninstall the freeware once the purpose of the freeware or the time frame is over, whichever is earlier.

4.11.2.5 Periodic Audit of Licenses

a. Audit

An audit should be conducted by random sampling and checking of paper Licenses every six months in the IT. In addition, surprise audits should be conducted from time to time in order to ensure that Policies laid down are adhered to. A full audit of all Software licenses held by IT shall be carried out annually.

4.11.2.6 License Management Responsibility

a. Operating System Licenses

The IT Team shall maintain the operating system licenses and master list of all operating systems running in BSCB should be recorded.

b. PC Productivity Software Licenses

The Manager- IT shall monitor the PC Productivity software (MSOffice etc.) licenses. The concerned IT Officials shall maintain the master list of licenses running in BSCB.

c. License Renewal

Licenses (or integrated licenses) for software such as Loan Origination Systems, Finance & Accounting systems, Mobile Applications, RDBMS Systems, Anti-Virus software, Front-end (GUI) software, e-mail etc. and hardware shall be maintained by the IT Division. Within 90 days prior to expiry of existing Maintenance, renewal quotations need to be requested from the service provider. Renewal quotes are valid until the expiration date indicated on the quote.

4.11.3 Annexure

4.11.3.1 Master Table for Maintenance of License

S. no.	Name of the product / application	License Issued by	License Issue Date	Validity

4.12 Procurement Policy

4.12.1 Methodology

Procurement of new hardware & software and upgradation of existing systems would be made from/by OEM or 'Original Software Developer (OSD)' or 'Authorized Channel Partner (ACP)' or Authorized Dealer (AD) or 'Public Sector Enterprise™ (PSE). Such procurement and/or upgradation of existing systems will be done under any one of the 4 Procurement Processes (i.e., Open Tendering, Limited Tendering, Emergency Purchases & Sundry Purchases).

4.12.1.1 Open Tendering

Head Office would do all large-scale procurements or specific projects involving financial outlay of more than INR.500,000 and less than INR 10,000,000 through open tendering process. For each procurement under 'Open Tendering' process, an advertisement inviting proposals for supplying IT equipment required by BSCB and inviting attention of prospective bidders to the website of the organization should be published in selected national newspaper/newspapers. BSCB may explore the possibility of uploading the tender notices in web site of BSCB. E-Mail addresses of the organization will be indicated in the tender notice as per requirement of BSCB.

The newspaper insertion should clearly mention that only those bidders who are eligible as per eligibility criteria of the RFP should send proposals as per the terms of the tender document (RFP). The website display should include all documents relating to the tender like RFP, 'Application Form' etc. If BSCB wishes to charge for the 'Application Form' downloaded from the website, the bidder may be asked to pay the amount by Demand Draft / Banker's Cheque / Mobile payment/Internet Banking/Pay Order at the time of

submission of the application form and bid documents. Tender notices would be sent by one or more quick means of services like email, fax, speed post, courier etc. The competitive bids shall be in three parts viz. Eligibility Bid, Technical Bid and Price Bid. All these Bids shall be submitted in separate sealed envelopes with appropriate superscription. All pages and documents in individual bids should be numbered as page no–. (Current page no.) Of page no-- (Total page no.) And should contain tender reference no. and organization's name. For open tender, BSCB can also have rate contract clause in RFP for a particular period so that during that period any such requirement can directly be procured from L1 bidder without going for fresh tender process. This will save total time of implementation of the project.

4.12.1.2 Procedure for Open Tendering

It is proposed to form IT Purchase Approval Committee (ITPAC) and Tender Planning and Evaluation Team (TPET). The constitution and the activities of these committees is mentioned below.

Sr. No.	Steps to be taken	Action to be taken	To be approved by	Estimated time schedule / Remarks
1	Decision to purchase to be taken by Admin Division after assessment of the requirement in terms of items, quantity and approximate cost	An Office Note is to be initiated by the concerned Departmental In charge seeking permission for publication of advertisement Inviting proposal.	/DGM	Should be in keeping with the Budgetary approval
2	Preparation of Tender Documents (RFP)	The Tender Documents should be prepared by the Tender planning and evaluation team	CEO/DGM	Planning and evaluation team will select the mode of advertisement vis-à-vis the name/s of newspaper/s, website etc.
3	Publication of advertisement inviting proposal	Necessary arrangements for paper insertion and website display have to be made by the Department as per the recommendation Of Planning and Evaluation team	CEO/DGM	The website display should be made available from the date of paper insertion till the last date of submission of tender
4	PBTD	Concerned Planning and	Manager-	The date of PBTD should

Sr. No.	Steps to be taken	Action to be taken	To be approved by	Estimated time schedule / Remarks
		Evaluation team will arrange & conduct this discussion in presence of vendors.	IT/AGM	be any day after seven (7) days from date of paper Insertion.
5	Clarifications of Pre-Bid Technical Discussion	Planning and Evaluation team will prepare clarifications	DGM / AGM / Chief Officer/AGM	Clarifications should be hosted on web site as a part of revised RFP and will be communicated to all bidders.
6	Submission of Tender	A suitable arrangement for receipt of tenders at the scheduled date and time through conspicuously located tender boxes needs to be adopted by Planning and Evaluation Team	X	Last date of submission of tender should be after three (3) weeks from the date of PBTD or the date mentioned in letter incorporating any suggested changes in RFP whichever is later.
7	Opening of Eligibility BID: Evaluation team of the TPET should open the eligibility bids in presence of the bidders.	TPET should prepare an evaluation sheet of these eligibility BID	Opening committee's Chairman	Within 5 business days after closure of tender submission time
8	Evaluation of Technical BID	TPET should prepare a technical evaluation sheet of these technical BID. The technical BID of those parties shall only be opened who have passed the eligibility evaluation	Evaluation committee's Chairman	After completion and closure of technical evaluation
8	Price Bid Opening	TPET should open the Price bids in presence of the bidders. PET should select L1 bidder as per terms of RFP by making a	X	After the completion of technical bid evaluation.

Sr. No.	Steps to be taken	Action to be taken	To be approved by	Estimated time schedule / Remarks
		chart. The Prices bids of only technically qualified bidders will be opened.		
	Bidder Negotiation and Finalization			
9	Negotiation with L2, L3 etc. in case L1 is not capable of supplying and maintaining BSCB's full requirement within a fixed time frame.	It may be done if found necessary by TPET after giving sufficient justification, TPET may recommend cancellation of tender process and move forward to negotiating process with L2 and so on.	Negotiation Team as advised by Awarding Committee	X
10	Financial Approval	Financial approval of the purchase from appropriate authority is to be taken by the Awarding Committee	Awarding Committee followed by CEO; sometimes may be placed before BoD	X
11	Issuance of Purchase Order / Work Order	Administration Division may issue Purchase Order / Work Order to the selected bidder.	CEO/DGM	X
12	Uploading of result of tender on BSCB's Website	TPET should ensure uploading of result of tender on BSCB's website	DGM / AGM / Chief Officer/AGM	Seven (7) Days from the date of Financial Approval.

Any document being placed to Manager - IT or IT Purchase Approval Committee (ITPAC) should be submitted by Tender Planning and Evaluation Team.

4.12.1.3 Limited Tendering

Procurement of hardware & software and upgradation of existing systems involving financial outlay of

less than Rs 5 Lacs would be done through limited tendering process among empanelled firms. Information Technology Department, Head Office, would prepare BSCB's panel. However Regional Offices can procure and upgrade computer-related items by exercising their Discretionary Power (after obtaining budgetary approval) from among BSCB's empanelled firms at a rate fixed by tendering process and in accordance with the terms & condition of the tender documents.

a. Empanelment of firms for Limited Tendering

Empanelment of firms should be done by an advertisement inviting ,Expression of Interest and inviting attention of prospective bidders to the website of BSCB would be published in selected national newspaper/newspapers. The newspaper insertion and the website display should include Eligibility Criteria in detail. All correspondence should be sent by quicker means of services like email, fax, speed post, courier etc. Such panel of firms should be valid for a period of three years only. Since limited tenders are issued to the approved firms dealing in a specific item/job on the basis of their capacity and performance it is imperative to update the list of approved firms at least once in a year weeding out the non-performers and including fresh entrants in the field. If the performance of any existing / empanelled firm is found unsatisfactory during any of the previous three years the firm may not be considered for future empanelment. The necessary procedure to be followed for empanelment is as below:

Sr. No.	Steps to be taken	Action to be taken	To be approved by	Estimated Time Schedule / Remarks
1	Decision for empanelment of firms for Limited Tendering	An Office Note is to be initiated by the concerned Departmental In charge seeking permission for publication of advertisement inviting EoI.	DGM / AGM / Chief Officer / Manager - IT	X
2	Preparation of EoI	Eligibility Criteria (EC) for EoI have to be prepared by the TPET.	Awarding Committee of TPET	TPET will select the mode of advertisement and the names of newspaper/s, website etc.
3	Publication of advertisement inviting	EoI Necessary arrangements for paper insertion and website display to be made by	CEO/DGM	The website display should be made on or before

Sr. No.	Steps to be taken	Action to be taken	To be approved by	Estimated Time Schedule / Remarks
		the TPET		paper insertion.
4	Submission of EoI by vendors	Arrangements as regards who will receive and forward the EoIs to whom to be made by TPET.	TPET	Last date of submission of EoI should be seven (7) days from date of paper insertion.
5	Evaluation of EoI	TPET will make arrangement for preparation of evaluation sheet & select eligible vendors as per Eligibility Criteria for empanelment	DGM / AGM / Chief Officer / Manager - IT	X
6	Forming of Panel	The Department should inform the selected vendors of their selection.	DGM / AGM / Chief Officer/AGM	X
7	Uploading of result of tender on BSCB Website	TPET should ensure uploading of result of tender on BSCB's website	DGM / AGM / Chief Officer / Manager - IT	Seven (7) Days from the date of approval by Administration Division

b. Procurement through Limited Tendering

The necessary procedure to be followed is as below:

Sr. No.	Steps to be	Action to be taken	Approved by	Estimated Time Schedule/Remarks
1	Decision to purchase after assessment of the requirement in terms of items, quantity and approximate cost	An Office Note is to be initiated by the concerned Department seeking permission for issuing letters to empanelled firms inviting participation in tendering process.	DGM / AGM / Chief Officer / Manager - IT	Should be in keeping with the Budgetary Approval
2	Hosting of Tender	Notice by TPET informing	DGM / AGM /	Sale should start at

Sr. No.	Steps to be	Action to be taken	Approved by	Estimated Time Schedule/Remarks
	Document / Preparation of RFP	availability of RFP served to all empanelled vendors will include the - i) Start date with time of RFP sale ii) Last date with time of RFP sale iii) Date & time of Pre-bid Technical discussion iv) Last date with time of tender submission v) Date & time of Technical bid opening and vi) Date & time of Price bid opening	Chief Officer / Manager - IT	least 1 day after issuing of notice and should continue for one week. Any modification in RFP including time schedule and other terms & conditions is to be made by Tender Committee and is to be approved by Manager-IT
3	PBTD	Concerned Planning and Evaluation team will arrange & conduct this discussion in presence of vendors.	DGM/AGM/Chief Officer / Manager IT	The date of PBTD should be any day after seven (7) days from date of sale / publishing of RFP.
4	Submission of Tender	A suitable arrangement for receipt of tenders at the scheduled date and time through conspicuously located tender boxes needs to be adopted by TPET	X	Last date of submission of tender should be one week from the date of PBTD or the date informing any suggested changes in RFP whichever is later.
5	Technical Bid Opening & its Evaluation	TPET should do the opening of Technical bids in presence of the bidders and submit minutes of opening to Evaluation Team. TPET should select eligible vendors as per terms of RFP	Evaluation committee's Chairman	Evaluation sheet should not be prepared in presence of the bidders.

Sr. No.	Steps to be	Action to be taken	Approved by	Estimated Time Schedule/Remarks
		by making an evaluation sheet of the technical bids.		
6	Price Bid Opening	TPET should do opening of Price bids in presence of the bidders. TPET should select L1 bidder as per terms of RFP by making a comparison chart	X	One week from opening of Technical bid
7	Negotiation with L2, L3 etc. in case L1 is not capable of supplying and maintaining full requirement.	It may be done if found necessary by TPET after giving sufficient justification, TPET may recommend cancellation of tender process and move forward to negotiating process with L2 and so on.	Negotiation Team as advised by Awarding Committee	X
8	Financial Approval	Financial approval of the purchase from appropriate authority is to be taken by the Department.	Awarding Committee followed by CEO; sometimes may be placed before BoD	X
9	Issuance of Purchase Order / Work Order	Administration Division may issue Purchase Order / Work Order to the selected bidder.	CEO/DGM	X

c. Issuance of Purchase Order and Entering into Annual Maintenance Contract

Manager-IT have been delegated discretionary powers to purchase computer and peripherals and to enter into AMC with vendors. In view of the above Head of the Head Office of BSCB may accord financial approval and issue Purchase Orders to the selected vendors at a prescribed rate arrived through tender process and such orders should be issued in terms of tender documents.

d. Emergency Purchases

BSCB may procure certain hardware and/or software on urgent basis to meet requirements in the context of Information Technology projects floated/advised as per the government's guidelines, for business requirements or for disaster handling even when such requirements have not been provided for in the Information Technology Plan of the organization. Information Technology division, Head

Office would make such procurement inviting quotation(s) from existing supplier(s) after obtaining necessary sanction from appropriate authority as per' Discretionary Power'. Wherever required, the division should seek the services of technical consultant. The quotation of purchasing should not exceed limit of Rs. 2 Lacs for a single purchase / per occasion.

4.12.2 Sundry Purchases

Sundry Purchases' should be made only for operational convenience by Departmental Heads of Head Office (for the department). Such purchases should be made after inviting at least three quotations, by using 'Discretionary Power' of the sanctioning officer and as per the 'Technical Specification' provided by Admin Dept. Head Office. Such expenses to be made by the Regional Heads/ Branch Heads should be with in the 'Budgetary Allocation' of Regional office, which will have to be provided for in the centralized budget of Head Office. However, it should be restricted to maximum of Rs. 2 Lacs (subject to approval from Head–IT).

4.12.3 Procurement Procedure

4.12.3.1 Appointment of Technical Consultants

The appointment of Technical Consultants should be absolutely need based and for specialized jobs only. The scope of work and role of consultants should be clearly defined, and the contract should incorporate clauses having adequate provisions for penalizing the consultants in case of defaults by them at any stage of the projects including delays attributable to the consultants, As far as possible a Project Implementation Schedule indicating maximum permissible time for each activity should be prepared with a view to arrest time over-runs of the projects. The role of the consultants should be advisory and recommendatory and final authority and responsibility should be with the departmental officers only.

4.12.3.2 BSCB Level IT. Purchase Approval Committee (ITPAC)

BSCB level IT Purchase approval committee would be formed as decided from time to time to be approved by CEO. Constitution of Committee may comprise of the concerned departmental head / chief, procurement officer and CEO.

The committee will approve the purchase and upgradation of Computers (including peripherals, software packages and other software) in respect of capital expenditure.

4.12.3.3 Tender Planning & Evaluation Team (TPET)

Tender Evaluation and Planning Team would be formed before each tender through Internal Office Order by Management with minimum the combination of BSCB's Opening Committee, Evaluation Committee and the Awarding Committee which will each by headed by their respective chairman.

a. Functions of Tender Planning & Evaluation Team (TPET)

To identify and suggest procurement of hardware and/or software or upgradation of any computer system including the total quantum for various Information Technology projects and decide the configuration of the requirement. Any decision taken by the committee should generally be within the budget approval. TPET are responsible for the following activities -

- To design the format for paper insertion inviting proposal in case of 'Open Tendering' and to design the format for paper insertion inviting 'Expression of Interest (EoI)' in case of 'Limited Tendering', nonstandard purchase and appointment of consultant.
- To prepare tender document RFP.
- To fix the charges for downloading of the application form in case of 'Open Tendering'.
- To fix the price at which the tender document (RFP) should be sold to the empanelled vendors in case of 'Limited Tendering'.
- To evaluate the EoI and arrange for distribution of RFP to eligible vendors.
- To arrange and conduct 'Pre-bid technical discussion'.
- To arrange for tenders receiving and opening of tender bids.
- To prepare a detailed comparative chart of the offers received from bidders along with their observations on the technical competence of the bidders and the technical and commercial aspects of the hardware and software.
- To finalize the name/s of the prospective vendor/s (L1 or other along with L1) to whom the purchase order may be placed.
- To place proposal to the Tender Awarding Committee of the TPET, for onward forwarding to the competent authority (if necessary), for approval of procurement/upgradation of computer system or implementation of the concerned project.
- To place purchase orders to the selected vendor/s and to keep regular follow up for completion of the project.
- To bind all the papers and documents from tender initiation to acceptance of purchase orders and to keep it in safe custody.
- To do any other function/activity that appropriate authority of BSCB may deem fit for the team to perform.

4.12.3.4 Undertaking by Groups/ Committees

The members of the Groups/ Committee should give an undertaking (Conflict of Interest declaration form) at the appropriate time, that none of them has any personal interest in the Companies/Agencies participating in the tender process. Any Member having interest in any Company should refrain from

participating in the Tender Committee.

4.12.4 Tendering Process

4.12.4.1 Single Bid Situation

The single bid situation is normally resorted to when the specifications are adequately defined and the items being procured are standard equipment, designed and manufactured as per general industry standards or the monopoly products. In such situation it is advisable to go in for re-tender. If even after this more than one bidder is not available contract can be awarded to said bidder. However, there may be certain deviations in tender specifications vis-à-vis bidders' offers. In order to compensate for such deviations, loading criteria, to be adopted, for evaluation purpose should invariably be indicated in the bid documents.

4.12.4.2 Two Bid Situation

In case of the two-bid situation, techno-commercial negotiations may be conducted with all the bidders to clarify, if any, the deviations vis-à-vis tender specifications/requirements. After bringing the acceptable offers on a common platform, all the commercial terms/conditions and technical specifications should be frozen. In case some changes are made in terms/ conditions or technical specifications, the bidders may be given a fair chance to revise their price bids accordingly. The distribution of work if considered necessary should be done in a fair transparent manner.

4.12.4.3 Notice Inviting Tender

For any procurement under 'Open Tendering' process, advertisement should be published in selected national newspaper/newspapers inviting proposals for supplying IT equipment required by BSCB. For making panel of prospective vendors under 'Limited Tendering' advertisement should be published in selected national newspaper / newspapers inviting 'Expression of Interest' for empanelment. The paper insertion should attract the attention of prospective bidders to the website of the organization. The newspaper insertion should clearly mention that only those bidders who are eligible as per eligibility criteria of the RFP should send proposals as per the terms of the tender document (RFP). The website display should include all documents relating to the tender like RFP, 'Application Form' etc. The 'Application Form' should mention the charges for downloading of the application form known as the tender fees. The bidder may be asked to pay the charges by Demand Draft / Banker's Cheque / Pay Order / Mobile payment / Internet Banking at the time of submission of the application form and bid documents. Tender notices would be sent by one or more quickly means of services like email, fax, speed post, courier etc. The panel for 'Limited Tender' should be updated annually (with grace period of six months) weeding out the non-performers and including fresh entrants in the field.

In order to generate fair and adequate competition, it is important that sufficient time, depending upon the magnitude and complexity of the project should be given to the bidders to submit their bids. Any

corrigenda issued in support of extension of dates, or any other information should be individually intimated to the bidders by quicker means of services like email, fax, speed post, courier etc.

4.12.4.4 Eligibility Criteria (EC)

The following points should be taken into account while fixing the EC for open tender:

- Bidder's experience and past performance on similar contracts for last 3 years
- Bidder's financial standing through latest Income Tax Clearance Certificate (I.T.C.C.), Annual reports (Balance sheets and Profit & Loss Account) for the last three years.
- Bidder's capabilities with respect to Sales during last three years, Installation base, number of Service Centers, support personnel and manufacturing facilities
- Presence of service centers

In view of the above, BSCB would invite proposal from reputed vendors with proven capabilities. Some of the guidelines for setting up of the eligibility criteria are given below:

- The bidder should be an 'Original Equipment Manufacturer (OEM)' or 'Original Software Developer (OSD)' or Authorized Channel Partner (ACP) of the solution or eligible Public Sector Enterprises (PSE).
- The bidder should be financially sound and should have average Annual Sales based on the procured item. BSCB always recommend bidder to submit EMD and PBG for high value contract.
- For tendering process BSCB always looks for vendors who have completed similar work during the last 3 years.
- The bidder should be able to provide immediate support service through direct presence of its support personnel in our offices where the system to be procured would be installed. This condition will however be waived if there is a specific requirement of BSCB and only one company is capable of delivering it.
- The bidder should submit a profile statement, which will comprise of information on:
  - The company's corporate structure
  - Client information including the certificate of satisfaction on installation and maintenance, completion certificate
  - Client wise present installed base of the computer system to be procured
  - Sales (number of installation and value) in the previous three years
  - List of support Service Centers
  - Audited Balance Sheet of last three years

4.12.4.5 Tender/Bid Documents

The tender documents should not contain obsolete, irrelevant, Conflicting, vague and incomplete clauses.

All the important clauses pertaining to earnest money deposit, completion schedule, factory testing of equipment, performance guarantee, payment terms, penalty for delayed completion, vendor's liability, safety arrangements, arbitration etc. are to be incorporated in the bid documents, in proper and explicit manner so as to fully safeguard the interest of BSCB. The bidders are required to be made aware of what is expected to be done by them after award of the contract so that they may consider all factors while submitting the bids.

The detailed generic technical specifications along with a list of preferred makes of major equipment should be incorporated in the bid documents. In addition, the performance parameters and the technical evaluation criteria, if any, need to be specified in the bidding documents in unequivocal terms. However, despite all precautions there may be some contradicting and Conflicting specifications/conditions. In order to overcome such crisis, an order of precedence i.e. which part of contract will prevail over the others should also be mentioned in tender documents.

4.12.4.6 Pre-bid Technical Discussion

Pre-bid technical discussion in case of 'Open Tendering' should be conducted approximately after seven (7) days of publication of advertisement in newspaper/newspapers. In case of 'Limited Tendering the PBTD should be conducted with the empanelled bidders after five (5) days from the last date of sale of RFP. The purpose of such discussion is to clarify the requirement of BSCB and to answers the queries that may be raised by probable bidders. Organization may invite their technical consultant to take part in the discussion, wherever necessary.

4.12.4.7 Receipt of Tender

A suitable arrangement for receipt of tenders at the scheduled date and time through conspicuously located tender boxes needs to be adopted. The tender notice should categorically contain the information regarding receipt of bids, viz. designation and address of officer to whom the tender should be addressed, the superscription/reference number to be indicated on the envelopes and most importantly, the due date of opening of tenders to be written on the envelope containing tenders.

4.12.4.8 Postponement of Tender Opening

For 'Limited Tender', at least one week's prior intimation is to be served to all the bidders in case of any change in the terms & conditions of the tender, specifications, and tender opening date, etc. Such changes should be made with the approval of the Management or Awarding Committee of the TPET.

In case of 'Open Tender', such intimation should invariably be through the publication of corrigenda in the selected newspaper and in BSCB's website as also through individual intimation to all those firms who had purchased the tender documents within the original tender sale date. However, if submissions of first bid like pre-qualification documents or date of pre-bid technical discussion is deferred, subsequent dates i.e., the tender sale date or date of submission of bids should also be extended accordingly.

4.12.4.9 Opening of Tender

The opening of tenders in presence of the bidders' representatives needs to be scrupulously followed. While opening the tenders it needs to be ensured that each page of tender, particularly the price and important terms and conditions should be encircled and initialled with the date. Any cutting/overwriting should be encircled and initialled in red ink by the tender opening officer/committee. The tender opening officer/committee should also prepare an 'on the spot statement' giving details of the quotations received and other particulars like the prices, taxes/duties, EMD, any rebates etc. as read out during the opening of tenders. A proper tender opening register in a printed format should be maintained containing information viz. date of opening including extensions, if any, names and signature of all the persons present to witness the tender opening which should include the bidder's representatives also.

In order to make the system fool proof following steps may be taken while opening tender:

- Attendance of all the persons present in bid opening need to be taken in both in 'Tender Opening Register' and 'Attendance Sheet'.
- Representatives of the vendors should be asked to sign all the pages of their respective bids opened and to put date & time.
- 'On the spot statement' giving details of the quotations received and opened along with the minutes should be kept in the 'Tender Opening Register'.
- The tender opening officer/committee should sign on the envelopes containing the price bids and the due date of opening of price bids should be clearly mentioned on the envelopes and should again be placed in the tender box.
- The detailed comparative chart of the offers received from bidders along with the observations on the technical competence of the bidders should not be done on the spot.

4.12.4.10 Basis of selection

Evaluation of all eligible bidders should be done on weightage basis. Total score of 100 should be distributed among the Eligibility, Technical and Commercial Criteria. Bidder who scores the maximum number of marks will be selected as L1, and other bidders will be selected as L2, L3 – depending upon the marks scored. L1 bidder may be selected on basis of combined scoring or solely on basis of commercial bid among technically qualified bidders.

4.12.4.11 Post tender Negotiations

a. There should not be any negotiations. Negotiations if at all shall be an exception and only in the case of proprietary items or in the case of items with limited source of supply. Negotiations shall be held with L-1 only. Counter offers tantamount to negotiations and should be treated at par with negotiation. Negotiations can be recommended in exceptional circumstances only after due application of mind and recording valid, logical reasons justifying negotiations. In case of inability to

obtain the desired results by way of reduction in rates and negotiations prove infructuous, satisfactory explanations are required to be recorded by the TPET who recommended the negotiations.

b. In case of L-1 backing out there should be re-tendering.

c. Counteroffers to L-1, in order to arrive at an acceptable price, shall amount to negotiations.

d. Post tender negotiations may be done with L2, L3 vendors in case L1 is not capable of supplying and maintaining BSCB's full requirement within a fixed time frame. It may be done if found necessary by TPET after giving sufficient justification. TPET may recommend cancellation of tender process or negotiate with L2 for finalization and so on.

4.12.4.12 Cancellation of Tender Processing

BSCB may cancel the tender processing at any point of time prior to the issuance of purchase order without assigning any reason whatsoever for unforeseen and unavoidable circumstances. The organization may also cancel the tender processing for want of any participating bidder or if all the participating bidders fail to qualify eligibility in terms with technical or other reasons. TPET with the approval of the Management can cancel Tender Processing.

4.12.4.13 Post Contract Modifications

After acceptance of the purchase order by the successful bidder/s, any relaxation in the contract terms/specifications should be strictly discouraged. However, in exceptional cases where the modifications/amendments are considered absolutely essential, the same should be allowed only after taking into account the financial implications and Tender Committee should take such decision with the approval of the Management.

4.12.4.14 Sale of Tender Document

Tender Document (RFP) should be sold to the empanelled vendors in case of 'Limited Tendering' at a price to be decided by TPET.

4.12.4.15 Pre-shipment Quality Inspection

For all purchases Pre-shipment Quality Inspection or Post Delivery Quality Inspection of equipment conducted by the vendor/s can be accepted on the basis of inspection certificate to be submitted by supplier/s. However, BSCB may conduct pre-shipment inspection by its own employee or by approved third party either on random basis for a minimum of 10% of the quantity to be purchased or on each & every item on 100% basis. Such approval for services of competent outside agencies for Quality Inspection will have to be obtained from Management.

4.12.4.16 Problem Relating to AMC

To eliminate practices where vendor is evaluated as L1 based on lower AMC rates but subsequently vendor takes no interest in AMC, it is better to have a clause of pre-estimated damages for delays and non-performance since proving of liquidated damages and risk purchase usually poses problem.

4.12.4.17 Intimation to unsuccessful Vendor

TPET with approval of management should ensure intimation of rejection to the vendors whose eligibility/ technical bids have been evaluated but found not to meet the qualification criteria, along with the return of the un-opened price bid.

4.12.5 Identification & Disposal of Obsolete Equipment

As per IT Policy of BSCB, the obsolescence of a technology will be determined by reviewing the IT assets using various parameters including the following:

- Efficiency
- Total Cost of Process
- Support
- Maintenance, enhancement and upgradation

The competent authority of BSCB should follow the procedure for identification & disposal of the obsolete/ unusable computer hardware and its peripherals as detailed herein below.

4.12.5.1 Identification of Obsolete Equipment

While procuring hardware, organizations generally takes 3 years warranty and rates for AMC for another 3 years, as it is presumed that IT Hardware will have a life of 6 years. In this age of fast technology upgradation and introduction of new technologies, it is generally experienced that in most of the cases, availability of spare parts and support service also starts deteriorating with time as the products reaches their end of life. Also, it is felt that due to wear and tear, the efficiency of the system decreases. As the new products are more efficient and cheaper, it is observed some times that the cost of maintaining hardware is higher than the cost of replacement by new Hardware. Therefore, all Hardware older than 6 years may be declared as obsolete and become eligible for disposal depending on requirement.

In addition to above if for some reasons, some products/ equipment reaches end of life even before 6 years and receiving spares and support becomes difficult, it will be prudent for BSCB to replace such equipment's with new one as process becomes more efficient, cheaper and maintenance and support is easily available. Any Hardware equipment not older than 6 years, which is certified by OEM vendor for non-availability of, spares and support may be declared as obsolete with the permission of DGM / AGM / Chief Officer.

4.12.5.2 Hardware Up gradation and Disposal

After identification items are to be disposed as per following clause (Disposal of Obsolete Items)

4.12.5.3 Policies for Disposal of Obsolete Items

a. The IT Division at Head Office of BSCB would keep the inventory of all such items erstwhile using in different divisions of head office. The inventory of all such items of branches and other controlling offices would be kept in concerned Regional Offices.

b. The Manager-IT would be the Competent Authority for disposal of obsolete equipment at Head Office.

c. The head of the Admin Dept., Head Office would be the disposal authority at Head Office.

d. A resolution should be passed in departmental Purchase Committee for disposal of obsolete/ unusable equipment's mentioning each item along with the original purchase cost & present book value. The Competent Authority may approve the proposal and intimate the concerned offices accordingly. BSCB may arrange to display the proposal in its website and/or by News Paper Publication for public notice if necessary.

e. BSCB should explore the possibility of disposing obsolete items under buy-back arrangement while procuring new hardware for getting cost advantage.

f. If BSCB fails to dispose the material through an auction / buy-back, the competent authority would be authorized to dispose the material as they may deem fit including donation of the obsolete items to educational or social organizations after taking necessary approval from competent authority.

4.12.6 Amendment Authority

Whenever there are changes in the manual, the same will be ratified by management and whenever there is a change in any concept, the approval will be taken from Board. However, ITPAC will be authorized to override any explicit provision if it is deemed to be useful considering the dynamic nature of the technology and changes in the form and structure of the technology provider.

4.12.7 Electronic Tender

Whenever BSCB will introduce tendering system, the procedure suggested would be followed by the system and they may not involve manual intervention as has been detailed in the manual.

4.13 Version Control Policy

4.13.1 Roles and Responsibilities

ROLE	RESPONSIBILITY
Owner	IT Department
Implementer	The AGM of the respective department under the IT cell of the organization will be responsible for proper implementation of procedures detailed herein, in coordination with GM-IT.
Supervision &Monitoring	GM-IT shall monitor the implementation of the version control procedures.

4.13.2 Version Management Functionality & Processes

Version Management support should include the following capabilities: -

- **Check-in/check-out** capabilities to trigger and tag versions of content
- **Version Property management** - providing a history of the content state as it is checked in and out of an object store
- **Capability to individually** save and maintain each version of content in the content management system
- **Ability to bind minor versions** to a major version
- **Capability to retain all edits**, not only the most recent backup copy of a document, and incrementally designate new minor versions upon check-in
- **Version Series Management** - Ability to retain all minor versions of a content object until a person deliberately creates an approved, major version
- Ability to distinguish between working versions (minor), approved versions (major), and published versions
- Allows BSCB's teams to promote a minor version to a major version without checking the document in and out (human initiated promotion)
- Allows BSCB's teams to demote a major version to a minor version without checking the document in and out (human initiated demotion)
- Allows BSCB's teams to limit/permission access to minor versions

4.13.3 Operational Policies

4.13.3.1 Version change procedures for Applications developed in-house

a. Decision making

Decision to implement the new versions of add-on modules of the application systems should be taken by Functional Head/Project Leader.

The following are the pre-requisites for implementation of the new version:-

- Detailed analysis of current procedures and system functionality should be carried out
- Detailed study of the limitations of the existing system should be done

Additional functionality and system features should necessarily justify implementation of add-on modules.

b. Maintenance of standard library for software

The Functional Head/Project Leader should ensure that a library of all object, source programs and modules detailing project name listing, old version number, size(lines of code and byte size of program file),last updated date and new version number for all the respective applications is available and regularly maintained.

c. Document Access Control

The access to the document mentioning the version and program changes should only be granted to the Functional Head/Group Leader.

d. Program Check-out request

The check-out request should be initiated by Application team once the program version changes are intended to be made and approved.

e. Software development

The procedures relating to software development, pilot-run testing should be on similar lines as that of program change management procedures.

f. Program Check-in request

The Application team should prepare the program check-in request for recording details of program change. The functional Head/Group leader should then update the version change documents and records accordingly.

g. Roll out of new versions to various locations/departments

It is the responsibility of the IT department for rolling out new versions of applications to multiple locations. Documentation of testing as well as Department/user sign-off should be maintained after successful implementation of new versions.

h. Version control

All programs should have a standard naming convention to identify the version numbers. If the application is running in a decentralized mode then it is the responsibility of the respective Application Team to ensure that uniform and standardized versions of business application systems are running across the user groups of BSCB.

i. MIS for version controls

The following information should be available with the respective Application Team for effective controls on version changes. The reports may be generated from the version control tool or utility or they may be maintained manually.

4.13.3.2 Version change status report

The Functional head/Group Leader is responsible for maintaining the Version Change Status Report. The report should reflect the following information-

- No. of current projects running for version change, respective modules and programs as on a given date
- Total changes made for a given period
- Last change date
- Details of programs undergoing changes, lines of codes (LOC) changed for source code and object code

4.13.3.3 Check-in and Check-out Statistics

This report, maintained by the Application Team, should reflect the following information:

- Date range
- No. of programs checked in
- No. of programs checked out
- No. of bytes added (Object & source code)
- No. of bytes reduced (Object & source code)
- No. of bytes changed (Object& source code)

4.13.3.4 Version change procedures for software developed by Outsourced party

The procedures for approval, check-out and check-in request, testing, implementation and roll-out of new version of the software are on the similar lines to that of the in-house developed application and add-on modules as mentioned above barring the aspect of software development. BSCB should clearly indicate the roles and responsibilities of the outsourced party/ vendor, in the Service Level Agreement entered into for the purpose of Software Maintenance, in the process of version change/ up gradation of the software.

a. Data migration during version change

The entire database should be backed up before migration to a new version.

The data conversion, if any, required for implementation of the new version of the application system should be carried out in a phased manner. Data integrity assumes a greater importance in all the data migration jobs. The database or application features should be used for data uploading. This would ensure that the data undergoes all the program validations while uploading into the new system and takes care of additional database tables or fields in the new version. The tests should be performed to establish the integrity and accuracy of data after uploading to the new version. Detailed documentation of version change procedures, data load error logs and history files, and test results should be maintained by the respective Application Team.

4.13.3.5 Version change procedures for System software

The system software includes PC/ desktop operating system, network operating system, systems tools and utilities, firmware, interfaces and bridge software, messaging system and groupware and any other systems being used in the organization at any given point of time.

a. Decision making for change in the version

Decision to implement the new versions of software is taken by the IT-Manager. Prior to implementation of new version, Functional Team will test and ensure the implications, benefits, effects and risks faced due to the change in version.

b. Implementation

The implementation of the new version of system software should be carried out by the respective vendor.IT clearance for implementing the new version is mandatory. Concerned Functional Team will support the entire process. The System Administrator/ Console Operator responsible for the relevant system should coordinate and supervise the procedures for implementation of new version. Entire file system backup should be taken before implementing the new version of system software. At the end of the installation, the official sign-off from vendor and organization's authorized official should be documented.

c. Version control

A detailed documentation of the different software versions running should be maintained by the concerned user departments. This document should be updated based on the sign-off received from the respective System administrators after successful installation of new software version. Other procedures for check-in, check-out would remain the same as explained above in Program Check-in and Check-out for applications.

d. Patches and upgrades to operating system and other software

Detailed documentation should be maintained for installation of all patches, updates and upgrades received against a version of operating system and other software mentioned above.

4.13.3.6 Periodic Return

All the Functional Team leaders should file a report to DGM / AGM / Chief Officer / Manager Division, detailing the versions of applications, system software and utilities being used. This report should be prepared regularly and updated into the list.

4.14 Virus Protection Policy

4.14.1 Roles & Responsibilities

ROLE	RESPONSIBILITIES
Implementation	**AGM-SM** should ensure the regular update of DAT files in all super agents (Branch Anti-Virus local server) and agents (client's machines)
Monitoring & Supervision	GM-IT

4.14.2 Risk Assessment

THREAT	IMPACT	LIKELIHOOD
Threat to continuity of network operation due to virus, Trojan, worm activity	High	Low
Threat to network operation due to non-updation of virus DAT files	High	Medium

4.14.3 Purpose

This policy document sets out the policy for the protection of the stand-alone and networked environment and for the continued provision of the services that we provide to our customers against the threat of malware. It provides guidance and direction on minimizing the risk of a malware infection(s) and what to do if one is encountered.

4.14.4 Scope

This policy applies to Information Technology resources and to all staff authorized to use/access those computer systems and communications networks whether they are employed directly by the Bank, contractors, bank staffs, or suppliers granted access for support purposes.

4.14.5 Procedures

4.14.5.1 Role of Anti-Virus Helpdesk / System Integrator

BSCB needs to establish an Anti-virus helpdesk / System Integrator (SI) that monitors released virus, supports users on virus related queries, updates virus signature files regularly and takes remedial measures in case a virus is detected. This Helpdesk / SI, which is a part of IT division, should be responsible for overall Virus Protection for BSCB and shall aim to provide the total technical support for prevention, detection, reporting and eradication of computer viruses.

In case the 'Anti-Virus Help desk' is outsourced to a third party (SI), Service Level Agreements should be signed and maintained.

4.14.5.2 Updates of Virus 'DAT files'

These are the files, which contain the data on virus signatures. Anti-Virus Helpdesk / SI should update these 'DAT files'. The Helpdesk should download and deploy or live update the data from the Internet website of OEM whenever a new update is available. The Helpdesk should monitor and maintain the status of anti-virus.

4.14.5.3 Updating of 'DAT files' on client computers/ network nodes

Once the updates of virus DAT files are copied/update on the central host computers (admin console servers), an operating system/admin console should be scheduled in the network server for pushing/deploying these DAT file updates onto client computers/ network nodes connected including branch offices. This job should be scheduled at the earliest during lean business hours.

4.14.5.4 Anti-Virus software upgrades

a. All PC's and Files Servers should be protected by Anti-virus software.

b. A member of IT will load the latest version of the software onto all the units upon installation. Also they are responsible for procuring and providing latest upgrades of anti-virus programs in regular and timely manner.

c. PCs will be updated automatically by the central virus software installation servers where possible, if this is not possible then users will be shown how to update their virus software with the minimum of intervention of their part.

d. Where PCs, laptops or PDAs are not connected to either the Trust LAN (or WAN) then virus protection software must be supplied to them by another means. Users requiring this arrangement must contact the IT division.

e. The concerned team / department / branch with the help of the anti-virus software / helpdesk (if separate department is present) shall check the version and existence of genuine anti-virus software in the hired PCs / storage as well.

4.14.5.5 Virus protection - some specific procedures

a. It should be ensured that the Anti-virus (AV) software is installed and active on every machine. Proper password protection should be there so that the Anti-virus check is not disabled by the users.

b. The Anti-virus software should be run at least once in a week by each user and it should be properly scheduled, preferably during the lunch hours of the office.

c. Virus scanning shall be performed by the users each time any file is copied from any source including network drives and any removable media.

d. Every external storage device should be scanned for virus before use.

e. Systems should be implemented to review the anti-virus software activity/ logs, especially to check whether the users are running the Anti-virus system regularly on their desktop computers. Anti-virus helpdesk to monitor and ensure that the desktops in the branch are not kept un-scanned for more than 15 days.

f. If the anti-virus in a desktop/PC is not getting updated then the user has to inform the same to the Helpdesk immediately, and Helpdesk to ensure that the problem is resolved at the earliest.

g. Upon encountering the virus problem, the AV software should stop the computer operations, delete the related files and clean the affected areas. The other options such as 'continue' and 'move to a directory' in AV check should not be enabled.

h. Messaging and Anti-virus: The AV software for messaging system (e-mail) should be implemented. If the virus is found in mail attachment file, this file should be deleted and the sender should be informed. The recipient would get the remaining message.

i. Checking the software downloaded from Internet: Software/ data downloaded from outside sources such as Internet may contain a virus. Before such software is decompressed, the users should always have virus scan active on such workstation. In order to provide more security, the users should log out of all files servers and terminate all other network connections. Before executing the software, it should be screened with the approved Anti-virus package. If a virus is detected, the Systems Administrator should be notified immediately, and no further work should be carried on the affected machine until the virus has been shown to be eradicated.

4.14.5.6 Virus reporting

Upon encountering the virus attack, the users should immediately stop using the involved computer and report it to Systems Administrator in-charge of the unit and IT's Helpdesk. As the viruses have become very complex, users should not attempt to eradicate them without expert advice.

The virus logs utility in AV check software should always be enabled and the logs should be reviewed by Systems Administrator and Helpdesk. On encountering the virus, the detailed virus log should be printed/stored by the System Administrator and Helpdesk. The log should also capture the virus itself so that the Helpdesk can subsequently update its software to detect new viruses as well as mutated versions of old viruses.

All the virus incidents should be reported by users and Departmental Heads to the Helpdesk/System Administrator immediately on the similar lines of procedures given in the "incident management" domain. The Helpdesk should also be immediately informed about the virus attacks.

4.14.5.7 Virus Patching

All systems that are fully patched are significantly less likely to be affected by malicious software. Malware targets known weaknesses or vulnerabilities in target operating systems or applications and uses these to attack the target system. Software updates/ patches prevent exploitation, it is therefore important to follow up on these newly release patches to ensure any newly identified vulnerability is mitigated as quickly as possible. Regular review, assessment and installation of the latest patches should be completed as close to regular release cycles. BSCB should aim to ensure that relevant official devices are:

a. Routinely patched with security patches (patches which have failed testing may be excluded on a host-by-host basis)

b. Servers: should be no more than 2 months behind available and tested security patches; Central servers should be tested bimonthly to ensure continuous updation of anti-virus software against new malicious content being generated around the world.

c. Desktops and Laptops: should be no more than 1 month behind available and tested security patches.

d. Networks/Other: should be no more than 1 month behind available and tested security patches

4.14.5.8 Restricted Download Rights

BSCB and its Regional Offices (ROs) should make sure that no software programs or executable files are to be downloaded from the Internet and installed on devices without permission from the relevant team. Technical controls should be in place to restrict the ability of the majority of users to download files from the Internet. All users should take appropriate precautions to ensure they limit the possibility of downloading malicious software.



4.14.5.9 Email

Email has become an indispensable medium for communication. Increasing reliance on email service leaves it open to exploitation as a means of transmission of malware and phishing attacks.
Attachments - All email including attachments is to automatically check for viruses before it enters or leaves the email system. Please refer 4.3 Email policy for detail information.

Phishing and Spams - Social engineering techniques often attempt to convince users to open attachments or 'click' on hyperlinks (that will spread malware infections) or even divulge sensitive information such as passwords. The users should be careful about such unsolicited emails.

4.14.5.10 Suspected Malware Outbreak

If a user observes any unusual activity leading them to suspect a malware attack, the user must:

a. Inform the concerned team immediately

b. Shutdown the machine and unplug network cable and ensure no one else uses it

c. Gather any media, USB memory stick, that was used for transporting information in or out of the machine and make available to the concerned team

d. Submit a First Information report to maintain record to Helpdesk or system administrator.

e. Not use the PC (or suspected media) until it has been cleared as being safe to use.

4.14.5.11 Training Requirements

Although many threats can be combated using technology the key to robust protection is empowering each user with the necessary knowledge to help prevent or limit virus outbreaks. End users should be made aware of good practice guidance such as, but not limited to, only opening emails from trusted sources or attempting to download/install software on their PC. Appropriate awareness campaigns/training should be aimed at staff to raise awareness.

4.15 ATM Policy

4.15.1 Policy Statement

BSCB shall install, monitor ATM, for use of account holder(s)/Customers and Staff.

4.15.2 Scope

This document addresses Policies related to ATM deployed/installed by Bank.

This Policy applies to all customer(s), employees of the Bank, Vendors & respective outsourced parties. Additionally, this policy applies to any and all usage of the Bank's ATM.

4.15.3 Introduction:

BSCB introduced ATM in the year 2016. ATMs (Automated Teller Machines) result in extension of branch network, establish superior customer service, reduce cost and improve profitability. Having ATM as one of the key alternate service delivery channels networked through a Switch, which apart from providing the basic functionality of cash withdrawals and account balance enquiries would also seek to augment the fee-based revenue through value added services and by acquiring transactions of other bank card holders. The ATM channel shall also be enhanced to cover other functionalities such as Third Party Fund Transfer (Card to card & card to A/c), PIN Change & Mini Statement, Immediate Payment Service (IMPS) – instant fund transfer to other banks and acquiring transactions over the inter-change network.

In place of ATM. Bank may install Cash Recycler which will work as ATM and Cash Deposit Machine.

4.15.4 Micro ATMs: -

Micro ATMs will allow customers to perform basic financial transactions using their Aadhaar number and their biometric/OTP as identity proof (along with a Bank Identification Number for inter-bank transactions). Unlike an ATM, the cash-in / cash-out functions of the micro-ATM will be performed by an operator (Business Correspondent BC), thus bringing down the cost of the device and the cost of servicing the customer. The micro-ATM will support the following financial transactions:

- ✓ Deposit
- ✓ Withdrawal
- ✓ Funds transfer
- ✓ Balance enquiry

Bank shall follow the micro-ATM standards published by RBI/IBA/NPCI that are broad-based, standards-based, and generic. They are based on a bank-led model for financial inclusion, where the Aadhaar infrastructure is an overlay on the existing banking and payments infrastructure.

4.15.5 Deployment Strategies:

- Bank may deploy front loading as well as rear loading ATM/CDs as per the business requirement. Currently Bank is having only front loading machines,
- Bank will deploy Cash Dispenser/ATMs/Micro ATMs/ Full Function ATM with latest technologies with or without depository module / with & without Biometric and/or EMV functionality, depending on its business requirements or/and as per the guidelines from RBI from time to time.
- Bank will install CDs/ATMs at Offsite locations based upon the Business opportunity and on proper recommendation of field functionaries.
- While deploying the CDs/ATMs at Offsite locations, bank to undertake the feasibility study of that area so that ATM gets maximum hits per day.
- At onsite and offsite locations, bank's products / services related publicity material shall be used to attract noncustomers. Subject to RBI approval, bank may also explore to place / host third party advertisements at onsite / offsite ATMs to generate fee-based income for the bank.
- Bank may also deploy at selected locations to facilitate the customers to perform noncash transactions.
- Depending upon the business requirements of the branches, bank will deploy Single /Bunch Note Cash Deposit acceptors at identified locations.
- Depending upon the business requirements of the branches, bank will deploy at identified locations.
- Micro ATMs shall be deployed as per Department of Finical Services (DFS) guideline.
- Bank may also deploy desktop ATMs/CDs as well as low denomination dispensing ATMs/CDs.

4.15.6 Minimum Configuration

The configuration of the prescribed models for the ATMs/CDs/Cash Recycler/Micro ATMs/ shall be of the latest generation as available with defined product roadmap from the respective OEMs and in vogue in the industry. The machine to be procured should meet the desired functionalities to meet the business requirement of the bank and norms prescribed by RBI/Govt. of India.

The above-mentioned types of machines need to be procured with minimum 1-3 years of onsite product warranty.

4.15.7 Multi-Lingual Screens

The Cash Dispenser/ATMs/Cash Recycler/Desktop ATMs/Micro ATMs will have screens in the Regional language, Hindi and English language.

1. The Banks requirement for Cash Dispenser/ATM/Cash Recycler/Micro ATMs as well as for the ATM Switch must contain this item.

2. Deployment in every new region must be with the regional language in that region.
3. All the previous installations will be upgraded to reflect this policy.

4.15.8 Site Security

Security arrangements at ATM premises to be followed as per the guidelines of Bank's physical "Security policy".

4.15.9 Storage of Journal Print & Electronic Journal (EJ) Log

1. The Branch will store the Journal print as per Data Retention Policy of Bank. Currently it is disabled due to high used of consumables.
2. The EJ will be stored at the Switch center as per Data Retention Policy of Bank.
3. Bank's reconciliation cell to keep the backup of the EJ as per Data Retention Policy of Bank.
4. The time-limit given to customer for disputed transactions must be within the time frame as per RBI norms.

4.15.10 Provision of DVR / CCTV camera and storage of footage / images

Each CD / ATM to be deployed with Digital Video Recorder (DVR) / Full Motion Camera. At risk prone / vulnerable sites bank will deploy Digital Video Surveillance system / CCTV, alarm system besides Digital Video Recorder (DVR) already available in the ATM/CD.

4.15.11 ATM Monitoring

(i) Online ATM monitoring tool to be provided by Bank to all ATM owning branches and Zonal offices through CBS network for ATM monitoring. Respective Branch office & Zonal Office are required to login to ATM Monitoring tool on frequent basis to access the status of ATMs.

4.15.12 ATM Hardware Related Product Enhancements & Upgrades

As per requirement system related to ATM/Cash Recycler/CD/Micro ATM shall be upgraded.

4.15.13 Acquiring Policy

The Bank will acquire both Debit Cards & Credit Card on the ATMs. Bank may become issuer & acquirer of VISA / RuPay / Mastercard / Maestro /Amex/Diner's club/ Discover Financial Services (DFS) transactions/ JCB/ Union Pay & other approved payment systems.

4.15.14 Networking / Connectivity of CDs/ATMs

For CAPEX model ATMs (Onsite and Offsite): Networking with ATM shall be provided through branch LAN Switch & router and connectivity through VSAT/Leased Line / CDMA / WiMax, 3G, 4G, 5G, SDWAN etc.

4.15.15 On-Us ATM Transactions & Services at BSCB ATMs

For first time use of Bank Debit Card at Bank's ATMs will require the customers to mandatorily change PIN of their choice.

a) Cash Withdrawal
b) Fast Cash
c) PIN Change through Green PIN
d) Balance Inquiry
e) PIN Change
f) Mini-Statement
g) New facilities may be introduced or existing may be removed from time to time and as per Bank's discretion.

4.15.16 Remote-On-Us (Issuer transactions) & Not-On-Us (Acquirer transactions)

The Bank will offer Remote-On-Us & Not-On-Us ATM Transactions in case of shared networks:

a) Cash Withdrawal
   1. In case of On-Us transactions The Per-Day withdrawal limit will be fixed as per Bank's/RBI norms or as per Govt of India guidelines.
   2. In case of Not-On-Us transactions The Per-Day withdrawal limit will be as per the card issuing bank.
   3. The maximum allowable single withdrawal will also be fixed as per Bank's/RBI norms or as per Govt of India guidelines at other bank ATMs which may vary as mutually decided amongst the members of the shared network.

b) Balance Inquiry
c) PIN Change
d) Mini Statement
e) Mobile Banking registration (Subject to the certification by other bank for the service on NFS network).

4.15.17 Grouting of ATMs/Cash Recycler and other security norms

- The ATMs/Cash Recycler required to be grouted to a structure (wall, pillar, floor etc.) except for ATMs installed in highly secured premises such as airports etc. which have adequate CCTV coverage and guarded by state/central security personnel.
- Ensure the electric switch/ plugs/ electrical wirings and network cables are properly shielded so that they are not visible / accessible to any external person from the ATM room.
- Ensure that all the network equipment's are kept in a locked or restricted location.
- Ensure that no unwanted / isolated items are lying in the ATM room.
- Regular physical inspection of the ATM should be performed by the ATM custodian/ Branch head to ensure no unauthorized skimming device is attached to the card reader slot / ATM keyboard.
- CCTV camera should be always in working condition.
- Ensure that lighting arrangement and the CCTV camera are fitted in front of the user in the ATM room and the user's face is clearly visible in the CCTV footage.
- Installing anti skimming device
- Changing the default number lock of the ATM cash vault.
- Marking of the cash cassettes with the assigned denomination, so as to avoid swap loading of cash.

4.15.18 Robbery

Robbery of ATM or ATM Cash

To be governed as per Banks insurance policy.

Robbery of Customer at Bank's ATM Site

The Bank will give customer explicit instruction to be careful when using the ATM. The Bank can publish a guideline for the customer. In sensitive areas, bank can install a second 'Perimeter' Camera / CCTV to capture the robber.

4.15.19 Insurance

The Bank shall get comprehensive insurance of all its ATMs / Micro ATMs / Cash Dispensers along with all the accessories available at the ATM sites with all furniture and equipment against Fire, theft, burglary, vandalism, natural disaster and riots amongst other risks. However, for ATMs installed under OPEX, it is responsibility of the vendor to get the complete insurance for cash, site and equipment's.

4.15.20 ATM Maintenance Service

The Bank may engage the services of Service Provider preferably Original Equipment Manufacturer (OEM) for general maintenance of ATMs as part of Annual Maintenance Contract (AMC).

4.15.21 Replacement of Machine / up-gradation with Biometric functionality and Chip card reader

Bank may replace an ATM that is minimum 5 years old and giving frequent trouble in normal operations to the customers or surpassed end of life / end of support.

Bank may up-grade the existing ATMs with biometric functionality, upgrade to 4 or more cassettes for higher denomination dispensations at places wherever such scope exist.

As per direction of RBI, Bank may upgrade the card readers of the ATM to read CHIP cards i.e. EMV compatible.

4.15.22 Cassette Swap System

In terms of the RBI guidelines, bank may introduce cassette swap system particularly at Offsite locations wherever cash replenishment services are through CRA agencies / third party vendor to negate counterfeit / forge currency notes dispensation from the ATMs.

4.15.23 ATM Switch

Switching of Capex, OPEX model ATMs /Cash Recycler will be through Bank's own switch or switching arrangement with third party vendor. However, bank may align ATM switching / driving arrangement keeping in view the directives of the Govt. of India / RBI.

4.15.24 Grievance Redressal:

For assistance in ATM Service, a customer may contact customer care of the Bank. For complaints of any nature, customers may contact the Branch maintaining the Primary account.

4.15.25 Regulatory & Supervisory Issues

a) The services should only include local currency (INR) products.

b) The Bank shall adhere to and comply with the guidelines issued by DFS, MOF, GOI/RBI/NABARD/IBA from time to time applicable to ATM Operations.

4.16 Debit Card Policy

4.16.1 Policy Statement

BSCB shall issue debit card(s), for use of account holder(s)/Customers and Staff.

4.16.2 Scope

This document addresses Policies related to Debit card issued by Bank. This Policy applies to all customer(s), employees of the Bank, Vendors & respective outsourced parties. Additionally, this policy applies to any and all usage of the Bank issued debit card.

4.16.3 Debit Card

A Debit Card is, essentially, an instrument that can be used to

- Avail of banking services such as cash withdrawal, balance enquiry etc., from any ATM and Micro ATM.
- Make payments to merchants against purchase, withdrawal of cash at POS or both within the prescribed limit by RBI at merchant outlets.
- To use over Internet for Online transactions through secure channel.
- Debit Card may be used for e-mandate for recurring transaction

4.16.4 Personal Identification Number (PIN)

PIN is a four-digit secret number/code which is given to the customer at the time of issuing a **debit card** for the purpose of security. This PIN should never be stored. PIN can be generated in physical or paperless (Green PIN) mode.

4.16.5 Types of Debit Cards

The Bank will issue Personalized (with /without photograph & Image Card)&Non-Personalized Contact/Contactless Debit cards approved by Card Payment Processor. These cards shall be allowed to use at ATM, POS & over the internet for online usage.
Bank may introduce any types of cards / Card Schemes to cater to different segment of the customers as per business requirements of the bank.

4.16.6 Eligibility for Issuance of Debit Cards

a) The Bank may issue VISA, Rupay, MasterCard /Maestro & other any Brand of Debit cards (Personalized &Non-Personalized) to be used at ATM, POS & over the internet for online usage. Cards to be issued after getting customer request on prescribed application form duly filled and signed by the customer.
b) Bank will not issue unsolicited cards to customers.
c) Bank to issue Debit Cards to Savings / Current (Individual, Proprietorship) A/c holders, KCC holders.
d) Only RuPay Brand Debit Cards to be issued to the account holders with Government sponsored schemes.
e) Debit Card should not be issued to deceased, inoperative, Dormant, Club, Society, Association etc.
f) Bank to ensure that issuance of Debit cards to be as per the RBI Guidelines.
g) Bank will not dispatch the card to a customer unsolicited, except when the card is a replacement for a card already held by the customer.
h) The relationship between the bank and the card holder will be contractual.
i) With a view to reduce instances of misuse of lost/stolen cards, Bank may issue personalized cards with name of the cardholder on the card.
j) Bank may issue Debit card to illiterate and blind persons on their request. However, the person applying for debit Card should be at least numeric literate and bank employee/s may advise all the related risks to the illiterate accountholder at the time of issuance of debit Card.

k) Customer can apply for Debit Card from any Branch of the Bank based on the following Mode of Operation:

Mode of Operation	Debit Card Access provided to
Either or Survivor	Any one Account Holder

Former or Survivor	Former Account Holder and in case of demise of the Former account Holder, access to survivor.
Anyone or Survivor	Any Account Holder

4.16.7 Responsibility of Bank

a) While issuing debit cards to the customers, branches to ensure that card holder/s submits the requisite application form duly signed at all the pages including terms & conditions given in application form for the purpose. Bank shall make available to the cardholders in writing, a set of contractual terms and conditions governing the issue and use of such a card. These terms shall maintain a fair balance between the interests of the parties concerned. The terms shall be expressed clearly.
   - The terms may be altered by the bank, but sufficient notice of the change shall be given to the cardholder to enable him/her to withdraw if he/she so chooses.
   - A period shall be specified after which time the cardholder would be deemed to have accepted the terms if he/she had not withdrawn during the specified period.

b) Bank will provide the facility of controlling the debit card over different channel of transaction i.e. ATM/POS/e-Commerce at Domestic/International level. The limit updation shall be allowed within the prescribed limit only.

c) The bank will not reveal any information relating to customers obtained at the time of issuing the card to any entity.

d) For online transaction through Bank's debit card OTP will be delivered at registered mobile number

e) All new debit cards will be issued only for domestic usage unless international use is specifically sought by the customer.

f) The entire active international card issued by the banks would have threshold limit for international usage. The threshold will be determined by the bank based on the risk profile of the customer and accepted by the customer.

4.16.8 Responsibility of Cardholder(s)/Customers

a) It is obligation of Cardholder(s) to take all appropriate steps to keep safe the card and the means (such as PIN or code) which enable it to be used.

b) Cardholder(s) shall not to record the PIN or code, in any form that would be intelligible or otherwise accessible to any third party if access is gained to such a record, either honestly or dishonestly.

c) Cardholder(s) shall notify the bank immediately after becoming aware:
   - of the loss or theft or copying of the card or the means which enable it to be used.
   - of the recording on the cardholder's account of any unauthorized transaction.
   - of any error or other irregularity in the maintaining of that account by the bank.

d) Cardholder(s) to change PIN of Debit Card on regular basis (at least once in 180 days) as security precaution.

e) By Default, all debit card International Usage will be disabled for all cards. It is responsibility of card holders to enable international usage of debit card before using internationally.
f) Customer has to use debit card at least once at ATM in India before using it Internationally.
g) By default, all debit card Online/E-Commerce & contactless usage will be disabled for all cards. It is responsibility of card holders to enable Online/E-commerce & contactless usage of debit card before using it for online/E-commerce & contactless transaction.
h) Customer has to use debit card at least once at ATM before using it for Online transactions.
i) Customer can set transaction limit for ATM/POS/E-Commerce both for Domestic/International transactions within the prescribed limit of card.

4.16.9 Transaction Limit & Other Charges

Transaction limit and other charges are as per the discretion of Bank and guidelines of Regulatory Authorities subject to revision from time to time.
The Bank will not be held liable for any loss caused by a technical breakdown of the Card payment processing system if the breakdown of the system was recognizable for the cardholder by a message on the display of the device or otherwise known. The responsibility of the bank for the non-execution or defective execution of the transaction is limited to the principle sum and loss of interest subject to the provisions of the law.

4.16.10 Security and other aspects

a) Bank shall ensure to provide secured session for carrying out transaction through bank's debit card and the losses incurred by any party on account of breach of security or failure of the security mechanism shall be borne by the bank.
b) Banks shall keep for a sufficient period of time, internal records to enable operations to be traced and errors to be rectified as per the policy of Bank for mandatorily keeping of old records for a specific time period.
c) The cardholder shall be provided with a receipt of the transaction or SMS on registered mobile number with Bank after he has completed it, either immediately in the form of receipt or within a reasonable period of time.
d) If any Customer's card is lost or stolen or if PIN is disclosed to a third party, customer has to report the incident immediately by calling Customer Care Service or by informing Bank through predefined SMS, e-mail. If customer is travelling overseas, information to be given to the nearest Visa centre (GCAS) as soon as possible.
e) The cardholder shall bear the loss sustained up to the time of receipt of acknowledgement against the notification to the bank of any loss, theft or copying of the card but only up to a certain limit (of fixed amount or a percentage of the transaction agreed upon in advance between the cardholder

and the bank), except where the cardholder acted fraudulently, knowingly or with extreme negligence.

f) Bank shall provide means whereby his customers may at any time of the day or night notify the loss, theft or copying of their payment devices.

g) On receipt of notification of the loss, theft or copying of the card, the bank shall take all action open to it to stop any further use of the card.

4.16.11 Lost or Stolen Card

a) If any Customer's card is lost or stolen or if PIN or other card details i.e., CVV/Expiry Date/OTP is disclosed to a third party, customer has to report the incident immediately by contacting Customer Service or may hotlist the card through SMS mode through registered Mobile Number,

b) Customer is liable for all amounts debited to account using Debit Card as a result of the unauthorized use of card/PIN until reported loss, theft or disclosure of your card or PIN. If your card/PIN which has been reported lost or stolen is recovered, it must not be used again.
For loss and compensation, policy on compensation cum customer relations and Standard Operating Procedure on Limited liability of Customers in Unauthorized Electronic Banking Transactions to be followed for disposal of Customer's compliant for suspected fraudulent transaction through Debit card.

4.16.12 Issuance of Duplicate Cards on account of lost or Damaged

On receiving a 'lost/damaged card' complaint from the customer over telephone (toll free nos. or email with customer care) or physically in the branches, the card status will be changed to 'Hot' within 30 minutes. In case of non-personalized card, new Card with New PIN will be issued to the customer on next working day by the card issuing branch. But in case of Personalized Card, request shall be processed, and card shall be dispatched to the customer's address directly and PIN at the Branch. Upon receipt of the Card, customer shall visit at branch to receive the PIN Mailer and thereafter Branch shall send the card activation request through Finacle.

4.16.13 Issuance of Cards to Joint Accounts

Card will be issued to the account with mode of operation either or survivor. Primary card will be issued to the primary account holder.

4.16.14 Inventory management of cards

Branches shall maintain the inventory of card once the same is received by respective branch from Head Office.

4.16.15 Prospective

a) Debit Card Insurance: Bank may offer insurance services on debit card to ensure complete security and utmost peace of mind to its customer.
b) Tie up with other Payment Processing systems: In future depending upon business requirement Bank may tie up with other payment processing systems after taking appropriate approval from the concerned Committee/Authority.
c) Co-Branding Arrangement: Bank may issue co-branded debit cards as per the Business requirement after taking appropriate approval from the concerned Committee/Authority, if introduced in Bank, will essentially unify a partnership agreement between the card issuer (bank), the card brand (any of the card payment processing organizations) and the company seeking the co-branded card for promotional activity.
d) Contactless Debit Card: Bank may issue Contact-less card (with NCMC features) as per the Business requirement. Further, in future depending upon business requirement Bank may tie up with any of the card payment processing organizations after taking appropriate approval from the concerned Committee/Authority.

4.16.16 Compliance to regulatory norms

The instructions/guidelines on Compliance with Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/ Obligation of Banks under PMLA, 2002 applicable to banks, issued by RBI from time to time, may be adhered to in respect of all cards issued.

Issue of international debit cards would be subject to the direction issued under the Foreign Exchange Management Act, 1999, as amended from time to time.

The Bank shall adhere to and comply with the guidelines issued by GOI/RBI/NABARD/IBA/NPCI/VISA from time to time applicable to debit cards issuance and usage.

4.17 Data Retention & Archival Policy

4.17.1 Data retention policies

Data retention policies form an important foundation for helping manage an organization's electronic data. In addition to paper documentation, organizations increasingly are creating and relying upon large streams of electronic information that often are not cataloged or stored in traditional filing systems. Capturing customer correspondence, accounting records, financial and sales data, electronic communications and other digital business information is critical in helping ensure organization not only remain in compliance with legislative requirements and industry regulations, but also that organization possess sufficient data backups necessary for recovering

from catastrophes. Without strong data retention policies, organizations may find it impossible to resume operations following a disaster.

4.17.2 The Importance of Data Retention Policies

A data retention policy is the first step in helping protect an organization's data and avoid financial, civil and criminal penalties that increasingly accompany poor data management practices. Local, state, national and international laws and industry regulations not only specify the types of data, organizations and businesses must retain, legislation and industry policies also dictate how long specific types of data must be maintained and even the manner in which the data is to be stored. But legal considerations are not the only reason to develop and implement strong data retention practices.

4.17.3 Purpose

The Bank's Data Retention Policy exists to ensure all the information (business and operational) of the bank in electronic form are retained and stored in compliance with legal, industry and business regulations. Electronic Data covered by this policy includes but is not limited to:

- Transactional data (CBS data)
- Business, Client, agent and vendor correspondence
- Customer records
- Employee records
  Contracts
- Sales, invoice and billing information
- Accounting, Finance, earning and tax data
  Electronic communications
- Database
- Educational data like e-books, policy documents etc. published online
- Other electronic data produced and collected in fulfilling business activities.
- Documents kept in electronic mode/ scanned form.

Main objectives in developing data retention policy can be summarized as follows-

- To keep important records and documents for future use or reference.
- To organize records so that they can be searched and accessed at a later stage.
- To dispose of records or documents that are no longer needed.

4.17.4 Scope

• The scope of this policy is to implement standard procedures for storage, retrieval and disposal of Records / Reports / Data / other electronic documents to be preserved as per statutory/ regulatory requirements as amended by time to time, to be followed by the Bank.

The policies are applicable to all the departments of the Bank which manages electronic data and to preserve them in the following categories as per the regulatory guidelines.:

a. Records to be preserved permanently
b. Records to be preserved for not less than10 years
c. Records to be preserved for not less than 8 years
d. Records to be preserved for not less than 5 years
e. Records to be preserved for not less than 3 years
f. Records to be preserved in respect of Govt. transactions.

Note: Year means financial years post creation

• Records arise on account of transactions/functions performed by the bank and relate to the data and information arising from these. The record referred here is in electronic form. The provisions of the policy shall apply irrespective of the media in which records are maintained.

• The determination of Record Media will be based on the following:
  i. Compliance with the statutory/regulatory requirements.
  ii. The need to ensure that media chosen does not conflict with accessibility requirements of RBI inspectors/Internal/External auditors.
  iii. Physical condition under which the record will be stored.
  iv. Appropriate controls over the conversion process when records are converted from paper form to non-paper form. At the time of conversion, adequate security/precautions need to be taken. However, the original document has to be stored along with the soft copy as per the retention policy.

• Generally, Record Location will be in the same office where the records were generated / used. However, the electronic form of the records/data like CBS data, mail messaging data and for other software which are maintained centrally has to be stored centrally. In case of Document Management System although documents are scanned at different geographical locations, the data may be stored centrally.

• Should there be a need to maintain records in offshore locations, the department concerned at Corporate Office shall take up with RBI for its prior approval subject to the norms spelt out in.

4.17.5 Acceptable Use

- All the employees and representatives are responsible for ensuring bank's data is retained and stored according to the applicable Regulatory /government /business / industry regulations. As per these regulations certain records and documents are to be preserved permanently while some others are to be preserved up to 10 years, 8 years, 5 years, 3 years. An illustrative

list of the different types of documents to be preserved are given in Annexure A. Every care has to be taken for the preservation of records.

- Any reference to the records can be resorted to only if the preservation is made systematically and in an orderly manner.

4.17.6 Place of Storage

Bank will store the archived data at the central location where it is maintained taking into consideration all the security measures. The storage media has to be stored in a dust proof, fire proof, humidity-controlled environment and the restoration has to be tested on a periodic interval. Bank will use software for accessing the archived data.

4.17.7 Reference/Indexing

- All the records kept under preservation, should be given serial references / index number based on the number of years of storage is required. Separate references/ indexing to be used depending upon the year of preservation.
- However, such reference shall be only with the authentication of authorized official nominated for the office etc. the same number only to be referred to any of items in the records.

4.17.8 Procedure to be followed for storage, Retrieval and purging of old records

- The concerned department should submit the request for required data with clear purpose. Request to be sent DIT with proper authentication. Request to be considered for processing by the concerned office within the 24 hrs.
- Withdrawal of any item from the records has to be carefully made and it is to be ensured that, after reference, the item is placed back in the records without any delay, with necessary authentications.
- For data stored offline, the retrieval can be done using Data Archival and Retrieval software. The access to the data can be given on a need-to-know basis.
- In all cases, where records are to be taken possession by the Police/Governmental authorities, a written requisition has to be taken and an acknowledgement obtained from the recipient in respect of the particular record to be taken possession of or delivered to retaining copies of the records delivered.
- Bank's data shall be stored using the following formats:
  - The Electronic data are to be securely stored on readily accessible online media.
  - Archived data must be securely stored on non-rewritable, non-erasable media or storage (such as LTO optical media, WORM tape or WORM magnetic disks).
  - Proper labeling of the storage tapes has to be made so that retrieval of the required data can be made easily.

- All archived data shall be stored at an environmentally protected and access-controlled site. Archived data shall be tested for restoration.

Whenever doubt arises as to the retention requirements affecting specific data, the data should be securely archived and then after stored permanently in External storage devices.

No users (Bank employee, contractor, temporary worker, authorized agent, volunteer or any other representative) shall delete any information, records or data in violation of the retention policy, law or business and industry regulations. Only the Bank's authorized representatives may delete bank's information(s), records and data upon the conclusion of the data's proper and lawful lifecycle. Upon deletion, care must be taken to ensure data is adequately destroyed (as opposed to simply delete in a manner that enables data recovery). The In-charge, Information Technology department must approve the destruction of data on all disks, cellular telephones, personal digital assistants, computers, PCs, servers and systems, and verify that all organization data have been properly destroyed, prior to discarding, donating or otherwise decommissioning organization equipment.

4.17.9 Regulatory Compliance

NPCI

Clause 2.6 of Procedural Guidelines for Grid-based Cheque Truncation System (CTS)

A sound storage and archiving system of images is an integral part of CTS which takes care of disputes, complaints, reconciliation, etc. The present legal requirement for preservation of physical paid cheques is 10 (Ten) years as mandated by Reserve Bank of India. So, the physical instruments and the images have to be preserved for the statutory period.

The Information Technology ACT, 2000 and its subsequent Amendments

Sec-7 Retention of Electronic Records

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -

a. the information contained therein remains accessible so as to be usable for a subsequent reference;
b. the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
c. the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Prevention of Money Laundering (Amendment) Act, 2009 (PMLA, 2009)

1. Banks are advised to maintain records for at least five years **from the date of transaction** between the bank and the client,

4.17.10 Data Restoration

Various data stored in external storage devices must be readable at any point of time which associates with managing complex storage and backup environment. Hence the data stored has to be restored and tested at-least on a quarterly basis.

4.17.11 Data categorization

When implementing a data retention policy, an initial data categorization as per the IT Security policy of the bank has to be done. Data has to be categorized into the following 4 groups

- Public
- Internal
- Restricted
- confidential

4.17.12 Policy Review

Policy being complex, it requires periodic review of once in a year with regulatory requirements/Internal requirements or as and when considered necessary.

4.17.13 Data Archival

Data archiving software needed, as manual search and deletion of data is complex.

4.17.14 Violations and Penalties

All officers, managers, employees, contractors, temporary workers, authorized agents and volunteers are subject to the terms of the organization's Data Retention Policy. Any violation of the Data Retention Policy must be immediately reported to the In-charge Information Technology department.

4.17.15 Records Management

- Identification of Relevant Records

  The following requirements are designed to ensure relevant records are identifiable in accordance with legal, regulatory and corporate governance demands:
  - All records are required to be categorized as either relevant or non-relevant:
    Relevant records are those which must be maintained for legal or regulatory reasons (i.e. mandatory records), or those which demonstrate compliance with group or business unit policies and therefore have sufficient and reasonable business need/purpose to be managed in the same way as mandatory records. Non-Relevant records have no mandatory or policy related retention requirements.
  - A list of relevant records with retention periods must be maintained and reviewed annually (Data Capture Sheet, Business List of Records or local compliant equivalent).

- Retention of relevant records

  The following requirements are designed to ensure relevant records are retained in accordance with legal and regulatory demands:
  Relevant records must be retained in accordance with local legal and regulatory requirements and with the Retention Schedules which comply with these requirements and allow for operational efficiencies. Local schedules of retention periods, including the definition of minimum local controls, should be communicated and reviewed on a regular basis, in line with locally defined timescales. Master records of electronic relevant records must not be stored on local desktops and laptop hard drives.

- Retrieval of relevant records

  - The following requirements are designed to ensure records are retrievable in accordance with legal, regulatory and corporate governance demands:
    All Relevant Records must be retrievable within required timescales laid down by law and regulation. The following minimum standards apply:
  - ➢ Retrieve e-records within 5 working days (excluding backup tapes).
  - ➢ Retrieve backup tapes in-line with locally defined requirements and rules.
  - All Relevant records must be retrievable in compliance with the relevant local legislation, regulation or Business Unit specific policy, which may require quicker retrieval timescales.
  - Retrieval processes must be documented and tested annually.

- Disposal of records

  For disposal of records upon expiry of the period prescribed in the policy statement, control measures include authorization and approval prior to disposal to be obtained

  The following requirements are designed to ensure records are disposed of in accordance with legal, regulatory and corporate governance demands:
  - ▪



- Non-Relevant Records must be disposed of as soon as practical, and at least annually, (unless required longer for operational reasons), except if a relevant Disposal Hold applies.
- In each case, destruction of records must be in compliance with the relevant local legislation or the regulatory guidelines, regulation or Business Unit specific policy.
- Destruction processes must be documented, tested annually and physically exercised for Relevant and Non-Relevant Records.

- Disposal hold

  - The following requirements are designed to ensure records retained appropriately if required for a known or anticipated legal or regulatory enquiry.
  - Where there is a known or anticipated legal or regulatory enquiry, all records as defined for the individual disposal hold (including non-relevant records) must be withheld from destruction.
  - All relevant records must be identifiable within required timescales laid down by law and regulation.
  - Identify the location of records within 24 hours and freeze them from destruction.
  - Local legal and compliance must be consulted to support Disposal Hold requirements.
  - Following the lifting of a Disposal Hold, and upon receipt of Legal authorization, records must be released within 30 days.
  - Disposal Hold procedures must be established and managed.

4.17.16 Different types of information storage

- Scanned soft copy of Documents
  Soft copy information includes, but is not limited to, scanned copy of all printed documents, reports, faxes and letters. For each of the soft copy information, information classification as mentioned hereunder shall be applied.
- Removable Media
  Removable media includes, but is not limited to, backup disks / tapes, CDs, DVDS, USB drives, portable hard drives, digital cameras, digital audio players, disks, and magnetic media. For each of the removal media, information classification as mentioned hereunder shall be applied.
- Electronic Information
  Electronic information includes all electronic files (e.g. those created using spreadsheets, word processing programs, emails) and data (e.g. stored in databases, data stores, applications) containing Banks' information and any information transmitted via electronic means (e.g. email, ftp, web, instant messaging, client-server traffic etc.). For each of the electronic information, information classification as mentioned hereunder shall be applied.



Information Handling

		Public	Internal	Restricted	Confidential
Scanned soft copy of Documents	Labeling	Labeled where feasible.	All hard copy information containing 'Internal Only' information should carry a visible classification label	All hard copy information containing 'Restricted' information should carry a visible classification label Files used to store hard copies of documents should be marked as "Restricted".	All hard copy information containing 'confidential' information should carry a classification label on every page of the document. Files used to store hard copies of documents should be marked as "confidential" if any documents contained within are of this classification.
	Handling and Storage	No restrictions .	Follow secure workplace practices such as a clear desk policy; Follow secure remote working practices when taking 'Internal' information offsite. This includes ensuring that information cannot be overlooked in public places	Store documents securely, in accordance with the need-to-know principle, when not in use (e.g. in a lockable cabinet). Retrieve printed documentation immediately from printer trays, fax machines or photocopiers. Follow secure remote working practices whenever taking 'Restricted' information offsite (e.g. ensuring that information cannot be overlooked, documents are securely stored, and information is not left unattended).	Store documents securely in accordance with the need-to-know principle, when not in use; For large volumes of confidential information physical security should be consulted. Obtain approval from the Information Owner before any 'confidential' documents are taken offsite. Follow secure remote working practices whenever taking 'confidential'

		Public	Internal	Restricted	Confidential
					information offsite (e.g. ensuring that information is not left unattended); Possession of, and access to, confidential information should be tracked throughout its lifecycle.
	Distribution	No restrictions.	No specific restrictions, although information should be reviewed for appropriateness before distributing externally	'Restricted' information must only be distributed in accordance with the need-to-know principle. For external mail (e.g. being sent by courier or local postal service), do not mark the classification on the envelope. For fax, ensure the address is confirmed, accurately entered and confirm immediate receipt. Each page of the document must be clearly numbered, in a format that includes the total number of pages.	Confidential information must only be distributed in accordance with the need-to-know principal; Use care when sending confidential documents internally or externally. Only send to authorized named individuals and address the information accordingly. Obtain approval from the Information Owner before sending documents and follow any additional distribution controls they specify. For internal and external mail, mark the

		Public	Internal	Restricted	Confidential
					classification on an inner envelope. This inner envelope must then be placed in an unmarked outer envelope. Consider the use of tamper proof envelopes. Use recorded delivery for confidential information delivered by external mail; Do not send confidential information via fax. Maintain a distribution list for any confidential documents sent internally or externally and retain the list for as long as the document is relevant.
	Disposal	Consider Records Management requirements when disposing of information.	Consider Records Management requirements when disposing of information. Dispose of hard copy information using secure confidential waste service or Bank approved Cross-Cut Shredder.	Dispose of hard copy information using secure confidential waste service or a cross-cut shredder; Dispose of 'Restricted' data in accordance with business units documented data disposal procedures;	Dispose of hard copy information using secure confidential waste service or a Cross-Cut Shredder. Dispose of confidential data in accordance with business units documented data disposal procedures;
Removable Media	Labeling	Not required.	Label all removable media containing 'Internal Only' information accordingly,	Label all removable media containing 'restricted' information accordingly, e.g. mark CDs with a	Wherever possible, removable media is not to be used

		Public	Internal	Restricted	Confidential
			e.g. mark CDs with a permanent marker or sticker. Classify removable media to the highest classification of the information residing on it. Where labeling is not physically possible, ensure the classification of the media is communicated to all parties when handling or distributing.	permanent marker or sticker. Classify removable media to the highest classification of the information residing on it; Where labeling is not physically possible, ensure the classification of the media is communicated to all parties when handling or distributing.	to store or distribute 'confidential' information. If it must be used all removable media containing 'confidential' information must be labeled and marked accordingly (as per 'Confidential' information).
	Handling and Storage	No restrictions.	Lock away removable media containing 'Internal Only' information when not in use; All removable devices should be encrypted using Bank approved cryptographic protection mechanisms.	Lock away removable media containing 'restricted' information when not in use. Do not share the removable media with anyone that does have a need-to-know for the information stored on the device. Only store 'restricted' information on removable media for as long as it is explicitly required; All removable devices should be encrypted using Bank approved cryptographic protection mechanisms.	Obtain approval from the Information Owner for the storage of 'confidential' information on removable media. Where approval is given, the information must only be stored for as long as it is explicitly required; Removable media must be stored securely, in accordance with the need-to-know principle, when not in use (e.g. in a lockable cabinet). The Information Owner must approve any 'confidential' information that is to be taken offsite on removable

		Public	Internal	Restricted	Confidential
					media. All removable devices should be encrypted.
	Distribution	No restrictions.	Information should be reviewed for appropriateness before distributing externally (e.g. to auditors, regulators, consultants etc.).	Distribute in accordance with the need-to-know principle; For external mail (e.g. being sent by courier or local postal service), do not mark the classification on the envelope, container or case.	'Confidential 'information must only be distributed in accordance with the need-to-know principle; Use care when sending 'confidential' information internally or externally. Only send to authorized named individuals and address the information accordingly. Obtain approval from the Information Owner before sending documents and follow any additional distribution controls they specify. For internal and external mail, do not mark the classification on the envelope, container or case; Use recorded delivery for 'confidential' information

		Public	Internal	Restricted	Confidential
					delivered by external mail; A distribution list should be maintained for any "confidential" information distributed internally or externally, and the list retained for as long as the document is relevant.
	Disposal	Consider Records Management requirements when disposing of information.	Delete information on removable media when no longer required. Consider Records Management requirements when disposing of information.	At most major sites optical media (e.g. CDs and DVDs) can be disposed of through the secure waste bins. Information on reusable (e.g. USB removable media) must be sanitized before reuse. This must take the form of secure deletion via a complete overwrite of the media.	At most major sites optical media (e.g. CDs and DVDs) can be disposed of through the secure waste bins. Information on reusable (e.g. USB removable media) must be sanitized before reuse. This must take the form of secure deletion via multiple overwrite of the media. Where the necessary destruction mechanisms outlined above are not available internally, staff should make use of contracted secure waste services to meet the secure disposal requirements.
	Labeling	Not required.	Clearly mark 'Internal Only' electronic	Clearly mark 'Confidential' electronic documents with	The classification of all 'confidential'

		Public	Internal	Restricted	Confidential
Electronic Information			documents with the classification (e.g. within the header or footer or on the front page). Where possible, the classification of electronic data should be made explicitly clear to staff.	the classification (e.g. within the header or footer or on the front page); Where possible, the classification of electronic data should be made explicitly clear to staff.	electronic documents must be clearly visible. Consider the use of digital signatures or electronic watermarking for electronically labeling 'confidential 'information. Where possible, the classification of electronic data should be made explicitly clear to staff
	Handling and Storage	Not required.	Acceptable usage requirements for technology (e.g. email and Internet) must be followed. Follow secure remote working practices whenever accessing 'Internal Only' information offsite such as ensuring that information cannot be overlooked in public places.	Ensure that unauthorized persons cannot observe or access the information (e.g. through the use of restricted file shares, restricted access to applications. Protect 'restricted' information with technical controls.	Ensure that unauthorized persons cannot observe or access the information (e.g. through the use of restricted file shares, restricted access to applications. 'Confidential' information must be protected with appropriate additional technical controls including the use of Bank approved encryption
	Distribution	Not required.	Ensure the classification of the email is known so that 'Internal only' information is not distributed externally. For external e-mails if in doubt, users must check with the relevant information owner.	Ensure the classification of the email is known so that 'restricted' information is not distributed to those without a need-to-know. For external e-mails if in doubt, users must check with the relevant information owner. All 'restricted' electronic	Use care when sending 'confidential' information internally. Only send to authorized named individuals and address the information

		Public	Internal	Restricted	Confidential
				information that leaves the Bank network must be protected using Bank approved cryptographic protection mechanisms.	accordingly. Obtain approval from the Information Owner before sending information and follow any additional distribution controls they specify. For internal e-mails attachments must be encrypted using Bank approved encryption External emails and attachments must be encrypted using a Bank approved solution. All 'Confidential' electronic information that leaves the bank network must be protected using approved cryptographic protection mechanisms.
	Disposal	Delete files and e-mails when no longer required, unless there are contractual, legal or local business area requirements that specify a retention period (for	Delete files and e-mails when no longer required, unless there are contractual, legal or local business area requirements that specify a retention period. Proper consideration must be given for the secure destruction of any media or hardware that is used to store 'Internal Only' information.	Delete files and e-mails when no longer required, unless there are contractual, legal or local business area requirements that specify a retention period. All hardware and media that is going to be reused for another purpose or must be sanitized before reuse. This must take the form of secure deletion via multiple overwrite of the media. All hardware must be sanitized (e.g. through	Delete files and e-mails when no longer required, unless there are contractual, legal or local business area requirements that specify a retention period. All hardware and media that is going to be reused for another purpose must be sanitized before reuse. This

		Public	Internal	Restricted	Confidential
		more information.		degaussing, multiple overwrite) and proper consideration given to its physical destruction.	must take the form of secure deletion via multiple overwrite of the media. All hardware must be sanitized (e.g. through degaussing, multiple overwrite) and proper consideration given to its physical destruction.

4.17.17 Data Retention Period: --

The retention periods are maintained as required under the law and also as per requirements. The data will be kept available if an enquiry which requires data is going on. A proper system of Preservation and retrieval should be put in place to make the process trouble free.

Annexure-A:

Illustrative list of electronic data to be preserved are given below. The list is only illustrative and shall be revised from time to time.

Sl No	Records / Reports / Data / other Documents	Preservation
1	Data of Core Systems viz Finacle data, GBM data, Internet Banking, mobile Banking, LAPS data, RTGS/NEFT, SWIFT, ITMS, CCIL and other electronic data pertaining to Treasury and Payment systems etc.	Permanent **Online**:10 years **Tape**: Permanent **(Along with the application software)**
2	Records relating to transactions which are in dispute.	Permanent
3	Policies in electronic form	Permanent
4	ATM Card / Debit Card related records, Records pertaining to change of Debit card, PIN generation, PIN reset/ Password reset	Permanent

Sl No	Records / Reports / Data / other Documents	Preservation
5	Pre- migration Data Backup	Permanent
6	Electronic data of Confidential Files and files relating to Industrial Disputes and Writ Petitions/ Files pertaining to CBI/ Court Cases stored in electronic form	Permanent
7	Soft Copy of Purchase orders/SLA/ Vendor Agreements / Third party Agreements etc.	Permanent
8	RBI Inspection Reports/Notes etc. received/submitted, Data submitted to RBI in e-form	Permanent
9	Images of cheques (in the CTS scenario). Domestic branches	Min 10 Years
	Physical copies of the cheques are to be stored in a CTS authorized warehouse for 1 year. Cheque images should be archived and kept for a minimum period of 7 years. (Overseas branches)	
10	Daily/Monthly/Quarterly/Yearly Backup Register and Backup movement register.	Min 8 years
11	DR Drill/Data Restoration/User ID Review related reports	Min 8 years
12	Duly authenticated ATM Journal Print.	Min 5 Years
13	Parameter/Master modification Register.	Min 5 Years
14	Media in use / corrupted register.	Min 5 Years
15	Maintenance contract file and all related records relating to Computer Hardware.	Min 5 Years
16	Information Security Audit Reports	Min 5 Years
17	Activities, exception and security events pertaining to IT environment	Min 3 Years
18	Call Centre records	Min 3 Years
19	Information Security Management System records	Min 3 Years
20	Incident Management Report pertaining to IT environment	Min 3 Years
21	Results of internal audits, including implementation and effectiveness of any corrective action taken.	Min 3 Years
22	Appropriate record of training on Information Security aspects	Min 3 Years
23	Records of skill experience and qualifications in the area of Information Security Management System	Min 3 Years
24	Logs of Users activities, exception and security events pertaining to IT environment, application logs	Min 3 Years
25	Documents relating to Insurance of I.T assets.	Min 3 Years
26	Email	Min 10 Years
Records / Reports / Data / other Documents pertaining to Govt. Transactions		
26	In the case of documents, it should be from the date on which they cease to be effective.	Shall be preserved as per guidelines for each scheme.
27	In the case of ledgers and registers it should be from the date of last entry (debit or credit) in such ledger / Register.	Shall be preserved as per guidelines for each scheme.
28	The records involved in any investigation/fraud cases should not be destroyed without permission from the competent authority.	Shall be preserved as per guidelines for each scheme.

Sl No	Records / Reports / Data / other Documents	Preservation
29	In case of stipulation by IT Act/any other Law regarding retention period of documents beyond the period mentioned as above, such records have to be maintained accordingly.	Shall be preserved as per guidelines for each scheme.
	Retention of Data pertaining to CCTV	
30	A CCTV System or Closed-Circuit Television System formed from a system of one or more CCTV cameras placed at strategic locations such as corridors, Data Centre, UPS room, Network room, Server room, entry point, Generator set room and other places to capture and record movements in their surrounding areas.	
	Online data retention. (Domestic)	should be for a minimum of 180 days
	Offline data retention	For a further minimum period of 180 days.
	Note: 1. Offline data to be stored in tapes and the tapes should be restored on a periodical basis to check that the tapes are in workable condition. 2. Purging of data should be carried at the beginning of every month. 3. All information and data retained must be processed in accordance with the rules and regulations governing its use.	

4.18 Data Migration Policy

4.18.1 Introduction

Data migration is the process of transferring data between data storage systems, data formats or computer systems. Its is the process of obtaining data from the existing systems, mapping this to the new data requirements of other systems and importing data to the new system. The data mapping mainly highlight the transformations as well as the data cleansing activities to ensure the new system(s) is/are populated with current and corrected data.
This policy documents the strategy and approach to a data migration activity and lists out the guidelines to ensure a successful and effective data migration.

4.18.2 Scope

The policy covers the functional and technical requirements of the bank. It defines the project review and technical review to map out an effective and efficient data migration plan.
The policy applies to all users and contractors of the bank.

4.18.3 Terms and Definitions

Data replication- Data replication is copying of data from one device (the source) to another device (the target) with no input/output redirection: that is, the source device remains online during the copy.

Migration of data, from legacy/old systems to is a key activity. At a high-level, data migration consists of the following activities:

- Analyzing the data as to identify what needs to be migrated to new system
- Profiling the data present in the legacy/old systems to identify what data is available and/or needs transformation
- Extracting the required data from the legacy/old system
- Transforming the extracted data to the form/format as required.
- Cleansing the transformed data of any inconsistencies and errors – This can be also done in the legacy/old system

Loading the cleansed data into new system.

Source system - The existing system or data that is being migrated to a new system or a form of data.

Target system - The planned system or form of data which will exist when the migration is completed.

Data extraction - Data extraction refers to the process of drawing out data from the current source system into a required file format.

4.18.4 Roles and Responsibilities

Data owners: - Data Owners must have a proper understanding of the legacy system data design, data structures and business requirements.
Functional Team: - The Functional team should have a proper understanding of the target system design and new business requirements.
Migration Team: - In-depth understanding of data profiling, cleansing, transformation, and migration techniques.
Change Management Committee: - The change management committee is responsible for initiatives to establish an effective change management process. The committee must vet all the changes required and schedule them for implementation based on the analysis. This committee will be responsible for formation and defining roles and responsibilities of Data owners, Functional Team & Migration Team. Change Management Committee to be formed after due approval from Board.

4.18.5 Factors for consideration

Factors to be considered during data migration:

i) Include how long the migration will take;

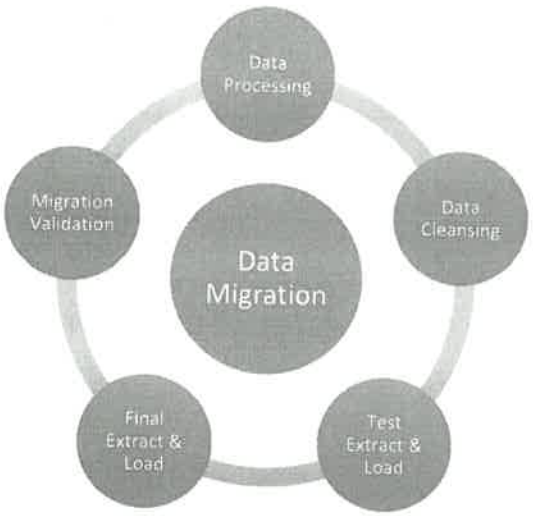
ii) The amount of downtime required;
iii) The risk to the business due to technical compatibility issues, data corruption, application performance issues, and missed data or data loss.

4.18.6 Requirements for Effective Data Migration

The following are the requirements for an effective data migration:

i) Complete documentation of legacy system
ii) Relationship between data defined accurately
iii) Ensure quality of data
iv) Ensure data security
v) Map data in accordance with business standards
vi) Deduplication of data
vii) Reconciliation of data
viii) Business as usual operations

4.18.7 Data Migration Life Cycle



4.18.8 Data Migration Strategy

Planning Phase

The planning phase for data migration consists primarily of data profiling and learning of the business knowledge. The bank's business data migration team will set expectations about the complexity of the migration, its timing and potential issues and concerns. The following are the processes involved in the planning phase:

- Requirement Analysis
- Identification of Stakeholders/Team
- Strategy Planning
- Optimal project delivery structure

- Project Initiation

Scoping

Scoping identifies the potential issues that may occur later on. This enables the migration team to plan for any risks. The migration team as part of the scoping process will prepare a project review and technical review plan.

The technical review is important to check the quality and appropriateness of:

- Proposed migration technology
- Data security plan
- Technical features of the data migration tool
- Structure, volume and quality of data

Source Data Identification

The primary step of a data migration process is to identify and assess the source system. The functional and migration team in collaboration will identify source data, define relevancy of data, identify the gaps in data and eliminate redundant data to develop an effective data migration system.

Data Assessment

The next phase is to assess the quality of this source data. Data profiling is required to assess the data.

Data profiling is the process of systematically scanning and analyzing the contents of all the columns in tables of interest. Profiling will identify the data defects at the table and column level. Data profiling is integral to the process of evaluating the conformity of the data and ensuring compliance to the requirements of the target system.

As per the profiling functions, the migration team will examine the actual record value and its metadata information. By including data profiling early in the migration process, the risks of project overruns, delays and potentially complete failures will be reduced.

Through the use of data profiling, the following will be achieved:

- Immediate identification whether the data will fit the business purpose
- Accurate planning of the integration strategy by identifying data anomalies up front
- Successful integration of the source data using an automated data quality process

Migration Design

In this phase, the enterprise architecture team will define the technical architecture and design of the migration processes. In addition, they will define the testing processes and how to transition them to the production system.

The business stakeholders of the bank will decide whether to go for parallel run migration, a zero-downtime migration, or completing the migration and decommissioning the old system.

Migration Build

The build phase of migration forms the design phase of the project. New data structures will be created within the database by the data migration team.

Once the physical data structures are in place, the mapping process will begin. During the mapping phase the business data migration team of the bank, having intimate knowledge of the historical data to be migrated and knowledge of both the source and target systems will help draft the mapping process.
A typical sequence to be followed when developing a migration is to subset the data and test one category of data at a time (e.g., product or customer). This approach will align with the data exploration stage that categorizes the data.

Testing

Testing of the migration solution is usually an iterative approach. Hence, the data migration testing team will start by checking the components individually in small subsets to ensure the mappings, transformations and data cleansing routines are working. Then, increase the data volumes and eventually link all of the components together into a single migration job.

Implementation

After comprehensive testing, the next step is to the run the migration. The business stakeholders of the bank will decide whether to shut the source systems while the migration executes or to adapt a zero-downtime migration approach.
For a zero downtime approach a tool will be required to provide the initial load processes, with additional data synchronization technology to capture any changes that took place during the initial load. After the initial load finishes, synchronization of the source and target data will be started.

Migration Validation

Migration validation will test the throughput of the migration process. The migration team will verify that the migration records are complete and of appropriate context.

Transition

During the execution phase, audit trails and logs will be created to ensure that all data has been correctly migrated and, when appropriate, that the correct synchronization has been achieved. The change management board of the bank will review the audit trails and logs, to make the decision to transition to the new system.
End user training for the new target system will be organized for a smooth transition and effective use of the system.

Post Transition

A production support team should be set up to deal with issues occurring post transition.
The function of the team will be to monitor the system, benchmark the results against the pre-defined business and technical goals and suggest improvements.



4.18.9 Data Migration Approaches

The bank based on its business requirements will decide which approach to adopt for its data migration plan. This is a critical decision because it is important to ensure that the migration strategy is aligned with the business plan.

The following are the different data migration approaches:

Big Bang

In this type of data migration the entire data is migrated in one go. For the big bang approach to work, the entire application is required to be shut for as long as the migration is completed.
The benefits of this approach are lower cost, no synchronization issues and a short implementation period. The drawbacks are failures have a cascading effect and fallback strategies are challenging. This approach is more suitable when the volume of data is low.

Phased

In this type of approach the data is moved in a phased manner. It helps to reduce stress and uncertainty related to data migration. This approach is usually suitable when the volume of data is large.
Phased migration approach uses a clear, programmatic approach with well-defined phases:

- In the initial phase, clients continue to have access to file data while an initial baseline copy of the file data from the source to the destination is done

- In the incremental phase, phased migration approach continues to copy file data from sources to destinations using the schedule specified, copies new files and updates files, as well as any files that were previously locked during the initial phase or during a previous incremental phase run.

- In the final phase, the approach prevents users from connecting to the source, performs a short final sync to copy any new, changed, or previously locked files, and then stops sharing file data on the source.

Parallel Run

In this approach during the migration, the legacy data continues to be used and changes are synchronized to the target. Transactions are posted on both the source and target systems until the migration is completed fully.
The benefit of this approach is that we can run the system in parallel without affecting the business operations. The downside is the cost to maintain two environments is considerably high and handling changing processes is very difficult.

4.18.10 Data Migration Process

Configuring Migration Tool

The data migration tool will act as a central repository to support storage and maintenance of data mapping. The tool selected by the board of the bank for migration should be flexible and scalable, ensuring efficient ETL (Extract, Transform & Load), and should also be capable of an automated transfer. The tool should be customizable as per the target system.

Configuring Staging Area

The enterprise architecture team will create a separate section in the production server to store extracted files generated after transformation. It will be used to store the intermediate results of the ETL process.

Executing data conversion

Once the staging area is configured, data from the legacy system will be moved to the target system by the development team. The data will be converted from the structural form that it exists in the legacy system to the required form in the target system.

Extract Transform Load Operations

ETL covers a process of how the data is loaded from the source system to the target system.

Extract

The Extract step will cover the data extraction from the source system and make it accessible for further processing. The main objective of the extract step will be to retrieve all the required data from the source system with as little resources as possible. The extract step will be designed by the ETL team in a way that it does not negatively affect the source system in terms of performance, response time or any kind of locking.

There are several ways to perform the extract:

- Update notification - If the source system is able to provide a notification that a record has been changed and describe the change, this is the easiest way to get the data.
- Incremental extract - Some systems may not be able to provide notification that an update has occurred, but they are able to identify which records have been modified and provide an extract of such records. During further ETL steps, the system needs to identify changes and propagate it down. Note, that by using daily extract, we may not be able to handle deleted records properly.
- Full extract - Some systems are not able to identify which data has been changed at all, so a full extract is the only way one can get the data out of the system. The full extract requires keeping a copy of the last extract in the same format in order to be able to identify changes. Full extract handles deletions as well.

Transform

The transform step will apply a set of rules to transform the data from the source to the target. This will include mapping any measured data to the same dimension (i.e. conformed dimension) using the same units so that they can later be joined.
The ETL team will join data from several sources, generate aggregates, generate surrogate keys, perform sort operations, derive new calculated values, and apply advanced validation rules.

Load

The load step will ensure that the load is performed correctly and with as little resources as possible. The target of the load process is often a database.

In order to make the load process efficient, the ETL team will disable any constraints and indexes before the load and enable them back only after the load completes. The referential integrity will be maintained by ETL tool to ensure consistency.

4.18.11 Testing Strategy

To reduce risk and ensure that the data has been migrated and transformed, the bank will implement a sound testing strategy. The following are the testing strategies that should be implemented:

Pre-Migration Data Testing

These tests occur early in the migration process, before any migration is completed. The pre-migration testing approach includes:

- Verifying scope of source systems and data with the bank and vendor. Verification should include data to be included as well as excluded and, if applicable, tied to the specific queries being used for the migration.
- Defining the source to target high-level mappings for each category of data or content and verify that the desired type has been defined in the destination system.
- Verifying destination system data requirements such as the field names, field type, mandatory fields, valid value lists and other field-level validation checks.
- Using the source to destination mappings, test the source data against the requirements of the destination system.
- Testing source and target system connections from the migration platform.

Unit Testing

The testing team through unit testing will verify the scope, data mapping, target system requirements and migration tool used. Also, each unit will be tested as part of the functional end-to-end strategy.

Functional Testing

Functional test cases will be created by the functional team in collaboration with the testing team and these test cases will be mapped to all the test scenarios which will in turn be mapped to scope items in the requirements document. Testing activities in a particular iteration will depend on the business output being delivered.

User Acceptance Testing

User acceptance testing should enable the user community of the bank to interact with legacy data in the destination system prior to production release. The key factors for this testing will be:

- Validating that the migration plan satisfies the business and technical requirements identified for the migration

- Finding and resolving potential risks to the production environment
- Importance will be given to reporting, downstream feeds, and other system processes that rely on migrated data. Both functional and technical scopes should be taken into account in this type of testing. The functional test on migrated data in the target system will be validated as per the requirement specifications.

Post Migration Testing

Post Migration Testing will validate the throughput of the migration process. The following are the steps involved in post migration testing:

- Testing the throughput of the migration process (number of records per unit time)
- Comparing migrated data as per the migration specification. The source values and the field level mappings are used to calculate the expected results at the destination.
- Data owners shall verify the correctness and consistency of Data.

Post Migration Audit

- Post migration, complete audit of same to be carried out.

4.18.12 Rollback & Reconciliation

Rollback

Rollback is the process of undoing or restoring any changes made to the system. The risk management team will devise a rollback strategy to mitigate the risks in the event of migration failure or reconciliation.

Reconciliation

During the cutover period, the source system will be brought to a logical accounting stage. No new transactions must be entered into the legacy system during the migration process and data must be frozen. Once the data migration is executed, reconciliation checks will have to be performed by the functional and technical team to ensure there are no mismatches before going live. Once the target system goes live, the support team will monitor the system to gauge success and note any improvements required.

All the stakeholders have to be informed of the planned downtime during migration. The channels interfaced to the system will not be functional during this period. If the bank is required to support any immediate transactions, they will have to be carried out in an offline mode by creating records that are fed into the system later.

4.18.13 Important point related to Data Migration

A well-defined migration strategy is essential to mitigate the risks involved and deliver a successful data migration. The best practices that should be incorporated in this process are:

- Ensure consistent alignment with the product delivery team.
- Timely meetings with the decision-making body of the bank to monitor progress and address any issues

- Document change control procedures so they can be incorporated into the migration procedures and plans
- Adopt a robust risk management strategy
- Establish data governance roles
- Set up data standards
- Perform mock runs before the actual exercise to ensure success and mitigate risks
- Verify the scope of data migration periodically
- Layout a proper action plan to back up both the source and target system
- Plan for contingencies and expected time
- Review and inspect the failures in data migration during testing
- Migration rollback should be planned in case of failure in migration or data reconciliation
- Establish postproduction support to avoid or reduce issues when the system goes live
- Audit and documentation of entire data migration process.

4.19 Social Media Policy

4.19.1 Introduction & Need for a Policy

Banking is a social activity involving interaction of the organization with the society. The last decade has seen the transformation of banking from physical to digital (ATM, e-Banking, Mobile Banking, eCommerce, SMS Banking). As human interaction (conventional society) goes from physical to digital (Social Networking), what's lacking is the digitization of the interaction/sharing part. Till such time, the communication is mostly one way through web portals, SMS etc. There is a need to cater to the demands of the ever-growing digital society. And it is time to embrace the "IN" thing, the "TOP TRENDING" thing that is "SOCIAL NETWORKING" or "SOCIAL MEDIA" (interacting with the society in a digital way).

In present times the end-user expects seamless interaction via multiple channels with faster, almost instantaneous response. The findings in this year's World Retail Banking Report demonstrate that retail banks need to be more agile, innovative, social and mobile in order to create a more meaningful experience to engage the customers. As the number and type of channels grow, knowledge of how the customers prefer to interact with their bank is critical. More and more people utilize social media and customers increasingly expect banks to offer services via these platforms.

Growth in business and profitability, especially from retail banking, is directly proportional to positive customer experience. A customer with more positive experience is more likely to stay with the Bank

and more likely to refer it to others. Given the increasing demand of Internet and social media in every walk of life, Bank must address the gaps and introduce social media banking to create this positive experience.

The potential benefits Organization can achieve by internal use of social media (staff interaction) are as follows;

- Speedier access to organizational knowledge and internal expertise
- Greater collaboration opportunities
- Monitoring of conversations (Positive and Negative) about the organization for correct feedback
- Reduced internal communication costs

Keeping in view of the importance of social media in today's world, Bank's presence is very much required in this space. Along with the benefits, there are few challenges as well. The Social Media scenario is also fast changing. Keeping in view of the potential benefits, challenges and dynamics of the Social Media scenario, every organization needs to have firm policy guidelines mentioning scope, responsibility and rules of its usages.

4.19.2 Policy Statement

- This policy covers use of social media for official use in official capacity as well as for personal use in personal capacity.
- This policy is intended to help staff make appropriate decisions about the use of social media such as social networking websites, blogs, micro blogs, video sharing sites, wikis, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook, and YouTube etc.
- This policy outlines the standards required for staff to observe when using social media, the circumstances to monitor the use of social media and the related action in respect of breaches of the policy.
- This policy supplements existing IT policy and e-mail Policy or related policies
- This policy does not form part of any contract of employment, and it may be amended at any time.

4.19.3 Who is covered by the Policy?

- This policy covers all individuals working in the Bank at all levels, scales, capacities, grades, including directors, executives, officers, employees, consultants, trainees, part-time and fixed-term employees, permanent staff or staff on contract (collectively referred to as staff in this policy).
- Here the term Bank refers to BSCB.

4.19.4 The Scope of the Policy

- All staff is expected to always comply with this policy to protect the privacy, confidentiality, and interests of the bank and its services, employees, partners, customers, and competitors.
- Breach of this policy may be dealt with Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to dismissal of staff member.

4.19.5 Using Work-related Social Media

- Bank recognizes the importance of internet particularly social media in shaping public thinking about the bank and its services, employees, partners and customers.
- Members of staff responsible for managing Bank's official presence are permitted to interact on approved social media portals about industry developments and regulatory issues.
- Approved social media websites are:

Platform Type	Approved Sites for official Use
Social Networking	Facebook
Social Messaging	WhatsApp
Blogs	BlogSpot
Microblogs	Twitter
Video Sharing Sites	YouTube
Wikis	Wikipedia
Image Sharing	Instagram

- Before using work-related social media identified staff must: Have read and understood this policy

4.19.6 Account Information/ Transaction Processing using Social Media Apps

- Bank will explore the possibility of providing account information along with transfer related transactions using Apps on Social Media portals.
- The apps will be physically hosted in Bank's server or the service provider's server but not on the social portal's server.
- The transactions will be fully secured transactions with double authentications as per RBI guidelines.

4.19.7 Personal Use of Social Media Sites

- Staff members are allowed to use any platform or any site for social media interaction in personal capacity. However, the Bank can't be held liable for any staff member's post/comments/blogs on Social Media since those are on personal capacity only.
- Staff should not create any group with Bank name or any reference to BSCB.
- The following conditions must be met for personal use to continue:
  - ✓ Use must be minimal and take place substantially out of normal working hours.
  - ✓ Use must not interfere with business or office commitments and should not reflect adversely on bank's policies, image, customers and fellow colleagues.

4.19.8 Rules for Use of Social Media

Whenever a member of staff uses social media in accordance with this policy, the member of staff must adhere to the following general rules:

- Wherever practical, staff member must use a disclaimer saying:
  "The article published is personal and do not necessarily represent the opinion or the position of BSCB."
- Think About Consequences:
  For example, consider what might happen if a Bank employee is in a meeting with a customer or prospect, and someone on the customer's side pulls out a print-out of a blog and says "This person at BSCB says that product sucks."
  Saying "Product X needs to have an easier learning curve for the first-time user" is fine; saying "Product X sucks" is risky, unsubtle and amateurish.
  Once again, it's all about judgment: using blog to trash or embarrass the Bank, our customers, or our co-workers, is dangerous and ill-advised.
- Keep professional and personal lives separate.
- Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Any member of staff who feels that they have been harassed or bullied or are offended by material posted or uploaded by a colleague onto a social media website should inform his/her department head.
- Never disclose commercially sensitive, anti-competitive, private or confidential information. If unsure whether the information falls within one of these categories, discuss this with the department head.
- It's perfectly acceptable to talk about the work and have a dialog with the community, but it's not okay to publish confidential information.
- Staff members are advised not to upload/post/forward any content belonging to a third party without third party's consent.
- Quote accurately, include references and when in doubt, link, don't copy. Before including a link to a third-party website, check that any terms and conditions of that website permit to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.
- Pay special attention to intellectual property and personal data protection before posting.

- Read before complying with its terms of use/acceptance guidelines of social media site.
- Do not post, upload, forward or post a link to chain mail, junk mail, derogatory cartoons, jokes or gossip, staff promotions, transfers etc. as these may not be in line with BSCB Marketing or Branding.
- Be honest and open but be mindful of the impact of the posting that might make to people's perceptions of the bank. If mistake is committed, be prompt in admitting and correcting it.
- Member of Staff are personally responsible for content published into social media tools – be aware that what is published will be public for many years.
- Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion with anger, return to it later in a calm and rational manner.
- If in doubt about a posting to be published, always discuss it with others before posting. Avoid positioning as an expert. Don't discuss about colleagues, competitors, customers or suppliers without their prior approval. Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.
- Avoid publishing contact details where they can be accessed and used widely by people who are not intended to see them, and never publish anyone else's contact details.
- Before contribution on any social media site, observe the activity on the site for a while before launching to get a feel for the style of contributions, the nature of the content and any 'unwritten' rules that other contributors might follow.
- Publishing rumors and/or internal and/or confidential information about the bank or related third parties on social networks can have a negative impact on the bank's image and reputation and may lead to legal action against the issuer.
- Activity on social media websites during office hours should complement and/or support current role and should be used in moderation.
- If any staff member sees misrepresentations made about the Bank in the media, he/she may point that out. Always do so with respect and with facts. If any staff member speaks about others, he/she should make sure what he/she says is factual and that it does not disparage that party. Avoid arguments.
- Do not blog anonymously, do not use pseudonyms or false screen names. We believe in transparency and honesty. Staff members are advised to use their real name. They may identify that they work for the Bank. They should not do anything that is dishonest, untrue, or misleading.
- It is critical that staff member show proper respect for the laws governing copyright and fair use or fair dealing of copyrighted material owned by others, including Bank's own copyrights and brands.
- Provide value by intelligently developing and sharing content so that Bank may be associated with what is published, thus, the opinions that are posted could strengthen the values and personality of the Bank.

4.19.9 Social Media Tips

The following tips are not mandatory but will contribute to successful use of social media.

- The best way to be interesting, stay out of trouble, and have fun is to write about what you know. There is a good chance of being embarrassed by a real expert, or of being boring if you write about topics, you are not knowledgeable about.
- Quality matters. Use a spell-checker. If you're not design-oriented, ask someone who is, whether your blog looks decent, and take their advice on how to improve it.
- The speed of being able to publish your thoughts is both a great feature and a great downfall of social media. The time to edit or reflect must be self-imposed. If in doubt over a post, or if something does not feel right, either let it sit and look at it again before publishing it or ask someone else to look at it first.

4.19.10 Monitoring Use of Social Media Websites

- Staff members should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under disciplinary procedure.
- Bank reserves the right to restrict or prevent access to certain social media websites if personal use is considered to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.
- Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against member of staff and bank. It may also cause embarrassment to bank and its customers.
- In particular uploading, posting, forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):
  - ✓ Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
  - ✓ A false and defamatory statement about any person or bank; Material which is offensive, obscene, criminal, discriminatory, derogatory or may cause embarrassment to bank, customers or staff;
  - ✓ Confidential information about bank or any of staff or customer.
  - ✓ Any other statement which is likely to create any liability (whether criminal or civil, and whether for member of staff or bank); or
  - ✓ Material in breach of copyright or other intellectual property rights, or which invades the privacy of any person. Any such action will be addressed under the disciplinary procedure and is likely to result in summary dismissal.
- Where evidence of misuse is found, bank may undertake a more detailed investigation in accordance with our disciplinary procedure, involving the examination and disclosure of monitoring records by those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.
- If member of staff notices any use of social media by other members of staff in breach of this policy, report it to Manager-IT.

4.19.11 Monitoring and Review of this Policy

As the platform is constantly changing, Bank's social media Policy may be reviewed at periodic interval, to ensure that it stays relevant, meets legal requirements and reflects best practices.

4.20 IT Skillset Development Policy

4.20.1 Purpose

This policy reflects Bank's commitment to ensure that the organization is served by skilled, well-trained and professional workforce having technical and managerial mastery over the entire gamut of banking technology covering Data Centre, Networks and Components, Application Software, Information Security, IS Audit, Digital Certificates, Electronic Commerce, Payment Systems, Data Warehousing, Data Mining, Business Intelligence and CRM, Technologies for Marketing, Technology Management, IT Planning and Project Management, IT Laws and Cyber Crimes, etc.
The IT Skill Development Policy lays down the guidelines about the different types of IT Skill Development / training that needs to be undertaken by employees of the bank to increase the efficiency of the bank. It would help staff members to attain competence in various IT Technologies and hence discharge their individual responsibilities efficiently. It would provide opportunities for staff to prepare for higher executive responsibilities.

4.20.2 Objective

The objectives of the Policy is to promote IT Skill development in the bank to manage various IT Projects, develop and customize new and existing IT Applications, ability to provide emergency support services for critical applications , and to impart various technology related training Officers and Staff of the Bank.

4.20.3 Roles & Responsibilities

Role	Responsibility
Policy Implementer and Sanctioning Authority for all IT Skill Development / Trainings	GM- Human Resources
• Assessment of Training needs of IT Employees • Type of training to be imparted such as External training, Internal, Seminars. • Maintaining the database of employees segregating them on the basis of skill set	GM (IT / HR)
Monitoring & Reviewing of Training	GM (IT / HR)

4.20.4 Training Segments

The training programs may be classified on the basis of target segment as under

Sl	Target Segment	Training Domain
1	All Employees	Awareness development on IT , Security and digital products.
2	IT Coordinator's working in IT Department and posted in various Office departments	Technical training for development, customization, programming, system analysis, design, project planning, execution, monitoring and administration of database, Network and systems, new technologies, IT Security.
3	Nodal Officers Asst General Managers, General Manager identified for Techno managerial training	Management of Technical Project, project planning, Project governance, Technology behind IT related products, New Technologies, IT Security etc. Training on IT from external institutes like IDRBT, NIBM, BIRD etc.
4	Training for Board members and Top management	Cyber Security guidelines given by RBI suggests awareness and sensitization of cyber risks among Board members and top management. Training programs offered by Reputed institutions for leaders in Information technology management may be considered.

4.20.5 Types of Training

All training shall be routed through HR Training cell for records and for making fee payments.
The following types of training may be considered while imparting training on various technologies

- **Internal Training:** Continuous Awareness creation among IT employees and other front office staff in branches on various systems such as Cyber / IT Security and new features being added to existing IT products such as Mobile Banking, Internet banking, UPI, etc. are to be carried out on regular basis. Internal training shall be the preferred method for imparting such trainings. Such trainings may be conducted by effectively utilizing the video conferencing facility available in the Bank and its Offices.
- **External Training:** Some of the needs of staff members may not be completely satisfied through the internal training. So, employees shall be deputed to attend external training conducted by reputed organization like NIBM, IDRBT or other such reputed institutions.
  In case training programs on specific technology as per requirement of Bank, is not readily available at above institutions, Bank may hire suitable competent resource personnel for training / approach private training institutes which provides such trainings. The cost of such trainings may be finalized through negotiation by the Negotiation Committee of the Bank. I.T department may also identify and empanel reputed training institutes through Open/limited tendering process.
- **On the Job Training:** IT Department has empaneled vendors for development and Customization of various products. Employees identified for software development and

customization may be involved in such customization jointly with the empaneled vendor so that they will acquire the required skill set.

- **Statutory & Mandatory Training:** These are the trainings which might be made mandatory by Government of India or regulatory bodies such as Reserve Bank of India, NPCI etc.
- **Short- and Long-Term Education Programs:** These are designed for sustained and continuous development of a specified target group such as Leadership Development and Executive Education on the lines of the already existing Management Education Program.
- **Seminars, Workshops, Quiz & Conferences:** The changing environment often throws up the demands in a specified area which can only be addressed by means of short duration Seminars, Workshops & Conferences conducted externally/internally. Occasionally IT quizzes will be held for groups of employees to enhance their IT knowledge skills. Security awareness programs like 2- or 3-day seminars will be held to create faster awareness among employees.
- **Distance Learning:** Training department should develop content to be used in this media. Learning material on typical subjects are also hosted on the Bank's Intranet.
- **E-learning:** The Bank should have the facility of E-learning though web-based learning management system. Online questionnaire can be designed, and employees made to answer them so as to enable them to realize their IT awareness.

4.20.6 Sanctioning Authority for IT Trainings

For all other IT Trainings Head- HR will be the Sanctioning Authority.

4.20.7 Strategic Areas identified for Training

All other Technology areas as mentioned below may be considered for imparting training by the policy implementer.

Sl	Name of the training
1	Emerging Banking Technologies and authentication techniques
2	Information Security, Cyber Law and Cyber Forensics, Cyber Defense – Vulnerability assessment & Penetration testing, Cyber Security Drills, Malware analysis, Website Security, Network Security
3	Information Systems Audit and IT Risk Management
4	Training for Security Operations Centre personnel on SOC technologies and incident monitoring
5	Digital Marketing in Banking
6	Data Centre Management, DR Drill
7	Data Analytics including social media analytics, Data warehousing, Business Intelligence
8	Data Protection Tools and Techniques
9	Mobile App development

10	Application Program Interface (API) Development
11	Secure Coding Practices
12	Mobile Banking Security and Testing
13	Payment Systems - Current Trends and New Initiatives
14	UNIX and Linux System Administration
15	Oracle DBA / PL-SQL Administration
16	Cloud Computing and Virtualization Technologies
17	Payment Systems Products using SFMS
18	Training on various programming languages as per requirement
18	Technologies for Financial Inclusion
19	IT Operational Risk Management
20	Registration authority operations
21	Technology Vendor Management
22	Metrics for IT Performance
23	Robotic Process Automation in Banking
24	Blockchain Technology
25	e-Learning/Learning management system
26	Governance of Enterprise IT
27	Customer Relationship Management (CRM)
28	Artificial Intelligence, Machine Learning, Blockchain Technology
29	Transaction through Aadhar based authentications
30	Internet Banking operations
31	Banking Application – Lifecycle Management
32	Website Security
33	IT Project Management
34	Secure Web Application Development
35	Network Security
36	IT Governance, risk & compliance
37	Other relevant Technology areas as per requirement

The list of programs suggested above is indicative and will be revised from time to time.

4.20.8 Motivating employees to undergo IT Certifications

In order to increase the knowledge base, capacity, performance &efficiency of employees, the bank should motivate employees to undergo and acquire Certifications in various areas of the Information Technology like Database, Networking, IT Security, Project Management, Systems etc.
On passing the respective Certification exams, the officers will be given incentives and reimbursement of all cost/fees involved (Both onetime costs & Annual recurring costs) in certification like Examination fee, training fee, Certification fee, annual maintenance fee , annual membership fee , course material cost etc. in accordance to circular issued/to be issued by HR department.
List of Certifications allowed under this is as follows: --

Sl.	Type of Technology	Certifications
1	Database Technology	OCP, OCA
2	Networking technology	CCNA, CCNP, MCSE, Network+
3	Programming	OCJA, OCJP
3	IT /Cyber Security	CISSP, CISM, CEH, SSCP, Security+, PenTest+
4	IS Audit	CISA
5	Project Management	PMP, Prince2
6	IT Service Management	ITIL
7	IT Governance	CGEIT, COBIT
8	IT Risk Management	CRISC

4.20.9 Center of Excellence

IT Department will create test / lab environment for all technologies in use by Bank for enhancing skills of officers and testing their knowledge post training as well as to increase their proficiency level.

4.20.10 Outcome and benefit of IT Skill Development/training

- Manage the project efficiently
- Reduce dependency on vendors
- Development of Inhouse Application reducing expenditure in procurement
- Increase productivity and efficiency
- Revitalize competency
- Create sincere and confident officials
- Making adequate succession planning becomes easier
- Decreases attrition

4.21 Mobile Banking Policy

4.21.1 Policy Statement

BSCB shall allow and register account holder(s)/Customers and Staff for doing mobile Banking. Mobile banking services shall be extended in a secured environment ensuring integrity, authentication, non-repudiation and confidentiality for all mobile banking transactions with remote users, business partners and regulatory agencies. All efforts shall be made to fully comply with the Reserve Bank of India guidelines on Technology and Security standards of Mobile banking security. Also Unified Payment Interface (UPI) provides payments linked to achieving the goals of universal electronic payments, a less cash society, and financial inclusion, using the latest technology trends, laid down in the RBI Payment System Vision Document 2025.

This Policy shall also apply to provide direction and framework for the regulation & supervision support involved in the issuance of Pre-paid Payment Instruments (PPIs- Mobile Wallet).

The services shall be restricted only to customers of banks and/or holders of debit cards issued as per the extant Reserve Bank of India guidelines. Only Indian Rupee based domestic services shall be provided. Use of mobile banking services for cross border inward and outward transfers is strictly prohibited. Bank may also use the services of Business Correspondent appointed in compliance with RBI guidelines, for extending this facility to their customers.

4.21.2 Scope

This document addresses Policies related to mobile Banking service provided by the Bank.
This Policy applies to all customer(s), employees of the Bank, Vendors, respective outsourced parties/entities identifying threats to information assets or information systems. Additionally, this policy applies to any and all usage of the Bank's mobile Banking.

4.21.3 Bank's responsibility

a) Bank shall ensure that Secrecy and Confidentiality of customers' data and integrity of transactions are protected.
b) It is necessary that the mobile banking servers at the bank's end, is certified by an accredited external agency.
c) Banks shall conduct regular information security audits on the mobile banking systems to ensure complete security.
d) The services shall be restricted only to customers of banks and/or holders of debit/credit cards issued
e) Bank is permitted to offer mobile banking services (fund transfer through UPI, IMPS, NEFT,RTGS,M-Passbook, bill payment, inter & intra Bank transaction). Mobile Banking services are to be made available to bank customers irrespective of the mobile network.
f) Only Indian Rupee based domestic services shall be provided. Use of mobile banking services for cross border inward and outward transfers is strictly prohibited.

g) Mobile banking needs to have very focused approach towards customer education.

4.21.4 Registration of customers for mobile service

Banks shall put in place a system of registration of customers for mobile banking. Banks should strive to provide options for easy registration for mobile banking services to their customers, through multiple channels, thus minimizing the need for the customer to visit the branch for such services. The time taken between registration of customers for mobile banking services and activation of the service should also be minimal. Currently, a customer can register for BSCB Mobile Banking service by submitting filled-in and signed application form at the BSCB branches.

4.21.5 Technology and Security Standards

Technology used for mobile banking must be secure and should ensure confidentiality, integrity, authenticity and non-reputability.
Bank is required to follow the Security Standards appropriate to the complexity of services offered, subject to following the minimum standards set out by regulatory authorities.
Bank is required to put in place appropriate risk mitigation measures like transaction limit (per transaction limit, daily/monthly), transaction velocity limit. depending on the bank's own risk perception, unless otherwise mandated by the Reserve Bank of India.
Proper level of encryption and security shall be implemented at all stages of the transaction processing. The endeavor shall be to ensure end-to-end encryption of the mobile banking transaction.
Conduct periodic risk management analysis, security vulnerability assessment of the application and network at least once in a year.

4.21.6 Inter-operability

Goal of mobile banking framework would be to enable funds transfer from account in one bank to any other account in the same or any other bank on a real time basis irrespective of the mobile network a customer has subscribed to. In addition to fund transfer facility through IMPS, RTGS, NEFT, UPI.

4.21.7 Authentication

Banks to comply with the following security principles and practices for the authentication of mobile banking transactions:

a) All mobile banking transactions involving debit to the account shall be permitted only by validation through a two factor or multi-factor authentication.
b) One of the factors of authentication shall be m-PIN or any higher standard.
c) Where m-PIN is used, end to end encryption of the m-PIN is desirable.

d) The m-PIN shall be stored in a secure environment.

e) Entering the wrong MPIN and TPIN thrice will block the mobile banking service to the account and the customer should approach the branch to activate it again or activate it online on providing the asked validation details.

f) MPIN and TPIN should not be same.

g) User shall be prompted to change MPIN/TPIN at a predefined interval.

4.21.8 Eligibility for Mobile Banking:

The Customer desirous of availing of the Mobile Banking Services should have at least one operative account with the bank however transactions through mobile banking channel should be allowed in following account types:

a) Savings Bank Accounts

b) Current Accounts – All individually operated accounts & Proprietorship accounts

c) Staff Overdraft & Cash credit accounts against deposit

d) Credit facility in loan accounts through IMPS/NEFT-RTGS.

e) In case of Joint accounts, accounts with the following mode of operation may also be allowed:

Mode of Operation	MBS Access provided to
Either or Survivor	Any Account Holder
Former or Survivor	Former Account Holder and in case of demise of the Former account Holder, access to survivor.
Anyone or Survivor	Any Account Holder
Proprietorship	Proprietor

4.21.9 Usage of Facility

- Mobile Banking application can be accessed through registered mobile number.
- Any change in the business rules of any of the processes will be notified on Bank's website, which will be construed as sufficient notice to the Customer.
- The customer can request for termination/suspension of the Mobile Banking Facility by requesting through the branch. Customer shall remain accountable for all the transactions on the designated account made prior to confirmation of any such cancellation request by the bank.
- It shall be the Bank's endeavor to give a reasonable notice for withdrawal or termination of the facility, but the Bank may at its discretion withdraw temporarily or terminate the facility, either wholly or partially, anytime without giving prior notice to the Customer. The

facility may be suspended for any maintenance or repair work for any breakdown in the Hardware/Software of MBS, any emergency or security reasons without prior notice and the bank shall not be responsible if such an action has to be taken for reasons of security or emergency.

- The Bank may terminate or suspend the services under the Facility without prior notice if the Customer has violated the terms and conditions lay down by the Bank or on the death of the Customer when brought to the notice of the Bank.

4.21.10 Customers Responsibility

- The Customer expressly authorizes the Bank to carry out all requests/transactions purporting to have been received from his/her mobile phone and authenticated with his/her MPIN and TPIN. In the case of payment facilities like fund transfer, mobile to pup, bill payment, the customer shall be deemed to have expressly authorised the Bank to make the payment when request is received from him/her.
- To advise the Bank of any change in his mobile number or loss/theft of mobile phone by adopting the procedure laid down by the Bank for the purpose.
- The Telecom Service provider of the customer may levy charges for each SMS/dial/GPRS Session and the Bank is not liable for any dispute that will arise between such telecom service provider and the Customer.
- The Customer shall keep the MPIN and TPIN confidential and will not disclose the se to any other person or will not record them in away that would compromise the confidentiality of the same or the security of the service.
- The Bank will not be responsible if the Application is not compatible with/ does not work on the mobile handset of the Customer.
- Customers need to fix thresholds for per day and per transaction limits. This is especially required for minor accounts.

4.21.11 Fees

Currently this facility is absolutely free for all eligible BSCB account holders. However, BSCB shall have the discretion to charge such fees as it may deem fit from time to time and may at its sole discretion, revise the fees for use of any or all of the facilities. Display of such charges on Bank's websites or otherwise would serve as sufficient notice and the same is binding on the customer.

4.21.12 Termination of BSCB Mobile Banking Service

Customers can Terminate from BSCB Mobile Banking service by requesting his/her home branch in writing.

4.21.13 Grievance Redressal

For assistance in Banking Service, a customer may contact toll free helpline number of customer care. For complaints of any nature, customers may contact the Branch maintaining the Primary account. Additionally, a customer may also send queries / complaints to the mobile Banking Cell or customer Care OR customer grievance section in Bank's website.
Any dispute or claim pertain to the Facility and /or the terms and conditions herein are subject to the exclusive jurisdiction of competent courts/tribunals/forums in Kolkata and the Customer agrees to such exclusive jurisdictions in Kolkata.

4.21.14 Regulatory & Supervisory Issues

The guidelines issued by Reserve Bank on "Know Your Customer (KYC)", "Anti Money Laundering (AML)" and "Combating the Financing of Terrorism (CFT)" from time to time would be applicable to mobile based banking services also.

Banks shall file Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) for mobile banking transactions as in the case of normal banking transactions. The Bank shall adhere to and comply with the guidelines issued by DFS, MOF, GOI/RBI/IBA from time to time applicable to Mobile Banking.

4.21.15 Amendment of the Policy

BSCB shall have the absolute discretion to amend or supplement any of the features and benefits in relation to the Facility.
BSCB shall communicate the amended Policy by hosting the same on Bank's website (www.BSCB.in) or in any other manner as decided by BSCB. The Customer shall be responsible for regularly reviewing this Policy, including amendments thereto as may be posted on the Bank's website (www.BSCB.in) and shall be deemed to have accepted the amended Terms and Conditions by continuing to use the Facility.

4.21.16 Disclaimer

The Bank, when acting in good faith, shall be absolved of any liability in case:

I. The Bank is unable to receive or execute any of the requests from the Customer or there is loss of information during processing or transmission or any unauthorized access by any other person or breach of confidentiality or due to reasons beyond the control of the Bank.
II. There is any kind of loss, direct or indirect, incurred by the Customer or any other person due to any failure or lapse in the Facility which are beyond the control of the Bank.
III. There is any failure or delay in transmitting of information or there is any error or inaccuracy of information or any other consequence arising from any cause beyond the control of the Bank which may include technology failure, mechanical breakdown, power disruption, etc.

IV. There is any lapse or failure on the part of the service providers or any third party affecting the said Facility and that the Bank makes no warranty as to the quality of the service provided by any such provider.

V. The Bank, its employees, agent or contractors, shall not be liable for and in respect of any loss or damage whether direct, indirect or consequential, including but not limited to loss of revenue, profit, business, contracts, anticipated savings or goodwill, loss of use or value of any equipment including software, whether foreseeable or not, suffered by the Customer or any person howsoever arising from or relating to any delay, interruption, suspension, resolution or error of the Bank in receiving and processing the request and in formulating and returning responses or any failure, delay, interruption, suspension, restriction, or error in transmission of any information or message to and from the telecommunication equipment of the Customer and the network of any service provider and the Bank's system or any breakdown, interruption, suspension or failure of the telecommunication equipment of the Customer, the Bank's system or the network of any service provider and/or any third party who provides such services as is necessary to provide the Facility.

4.22 Internet Banking Policy

4.22.1 Policy Statement

BSCB shall allow and register account holder(s)/Customers and Staff for doing internet Banking.

4.22.2 Scope

This document addresses Policies related to internet Banking service provided by the Bank.

This Policy applies to all Internet Banking Users of the Bank, Vendors, respective outsourced parties entities identifying threats to information assets or information systems. Additionally, this policy applies to any and all usage of the Bank's internet Banking.Exceptions to this policy must be approved by the IT Strategy Committee of the Board.

4.22.3 Introduction

Electronic banking provides the perfect platform to offer integrated remote financial services portal to customers – a one click access to routine banking products and services like savings account, current account, bill payment, online fund transfer and several other value added surround services. Electronic banking promises to be more efficient by providing low-cost operations and access, to financial services remotely.

4.22.4 Eligibility

a) Internet banking services will only be provided to the operative account holders of the Bank and

completion of KYC.

i) Retail

- Internet banking services can be provided to individual customers of our bank including staff who should have at least one operative account (Saving Bank account, Current account, Cash credit account, Overdraft Account) with the bank.
- Internet banking services cannot be permitted to illiterate and insolvent person.

ii) Kids

- Minors between the age group of 10 and 18 can avail the Kids internet banking facility with restricted transaction limit/services.

iii) Corporate

- The Corporate Internet Banking services shall be extended to non-individual entities that register for this service with the Bank. All Proprietary / partnership firms / HUF/ Private limited Co's / public Limited Co's having Saving Account (in the name of non-individual) / Current Accounts/ Cash Credit Accounts/ Fixed Deposit Accounts/ Loan Accounts are eligible for Internet Banking Services under Corporate Banking. However, in order to avail this facility, customer should have at least one operative account (Saving, Current or Cash Credit).
- Internet banking facility can't be provided in the case of Power of Attorney.

b) Internet banking services will be restricted to account holders of the Bank only.

4.22.5 Services Offered through Internet banking

Internet banking provided by the bank will have modularity and capability for expansion of services based on the demand and feasibility. The envisaged services are broadly segmented as follows:

- **Retail Internet Banking**
- **Internet Banking for Corporate**
- **Kids Internet Banking (Above 10 Years and below 18 years)**

The following facilities will be offered to different types of internet banking services:

S.N.	Facility	Retail Internet Banking	Internet Banking for Corporate	Kids Internet Banking
1.	Enquiries	Allowed	Allowed	Allowed
2.	Funds Transfer	Allowed	Allowed	Allowed (Fund transfer upto Rs. 10000 per day)

3.	Requests (including Online RD/ FD creation)	Allowed	Allowed (excluding Online RD/ FD creation)	Allowed(excluding Online RD/ FD creation)
4.	Bill payment	Allowed	Allowed	Not Allowed
5.	Bulk upload facility	Not Allowed	Allowed	Not Allowed
6.	Tax Payment	Allowed	Allowed	Not Allowed
7.	ASBA	Allowed	Allowed	Not Allowed
8.	PMNRF	Allowed	Allowed	Not Allowed
11.	Account Statement	Allowed	Allowed	Allowed
12.	Demand Draft	Allowed	Allowed	Allowed
13	Premature Closure FD/RD	Allowed	Allowed	Not Allowed
14	Sovereign Gold Bond	Allowed	Allowed	Not Allowed

4.22.6 Responsibility of Bank

a) After registration the retail user shall be provided with temporary unique user id, preferably the cust-id, and password. The PIN mailer (in case of offline request) containing the temporary user id and passwords (both the log-in and transaction passwords) shall be dispatched to the requesting branch and delivered to customer against acknowledgement.

b) The users shall also be advised to change their passwords at regular intervals for enhanced security.

c) Bank shall take all necessary steps to educate its eBanking customers against the phishing and other social engineering attacks in order to ensure that customer enjoy the complete benefits of the services offered without worrying about his/her data going to the wrong hands.

d) Forced change of password can be introduced after a particular number of months (12), for all customers.

e) Computer Automated Public Turing test to tell Computers and Human Apart (CAPTCHA) must be implemented in Bank's Internet Banking website as the additional layer of security

4.22.7 Responsibility of Customer

a) To avail the facility of internet Banking Customer can apply through offline & as well as online

mode (only Retail Customers). For offline mode customer shall be required to register with the bank and submit physical form to any BSCB branch.

b) Retail Customer can either choose to keep the Bank provided temporary user-id or change her/his user-id. In addition, during the first login, system will ask the user to mandatorily change his/her login and transaction passwords provided by the Bank.
c) A retail or corporate customer can subscribe for either view only or Transaction facility.
d) Customer needs to change password at "regular" intervals or at any time whenever required.

4.22.8 Online Registration and password reset facility to retail customers

Bank has provided the facility of online user registration along with the password reset facility. In such case, customer would be able to regenerate/activate his password(s) and create user id after proper online authentication by the system.

4.22.9 Customer Account blocking

a) For the security reasons customer account blocking shall be enabled. Any customer account shall be locked for indefinite period either through request to Bank officials or by using mobile app.
b) Customer's user id will be blocked, if wrong passwords are entered for a specified number of times. And user has to get user id unblocked for usage.

c) For Unblocking
   - Blocked by Bank Team-
     The user shall have to inform the administrator through proper channel for unblocking the respective account. Customer shall be required to validate her/his identity to the administrator prior to such an unblocking request being executed. The system administrator, on receipt of such notifications from the proper channel, shall check the user blocked position and after conforming shall unblock the password for the user. User shall be informed about the same through a proper channel.
   - Self-Blocked by Customer-
     Retail Customer can unblock himself/herself either by resetting the password online or through the mobile app (only if he has blocked himself by using app).

4.22.10 Terms And Conditions

The terms and conditions for Internet banking would be displayed on the Bank's Internet banking web site.

a. The customer shall acknowledge for having read and understood the terms and conditions which shall be annexed to the registration form.

b. The user shall also have to commit on "Agree" button appearing below the terms and conditions when he logs in to the Internet banking for the first time. All these modes shall amount to the acknowledgement by the user to the terms and conditions for Internet banking.

4.22.11 Termination of facility

Following are the various circumstances under which the Internet banking services may be terminated for a user:

a. The users shall be allowed to request termination of facility to the Bank.
b. Bank shall have the right to terminate the facility if the conduct of user's account is not found good and or if the User fails to comply with the terms and conditions attached to the usage of Internet Banking Facility.

c. The Internet banking services shall be terminated upon cessation of the Bank Customer relationship of the User.

d. The bank reserves the right to monitor the activity of suspicious user accounts through the internet channel and even block certain services if deemed suspicious.

e. The bank has the right to turn over to relevant governmental authorities any electronic records on their specific request and the customer will not have recourse to question the same on grounds of confidentiality.

4.22.12 Hyperlinks To and From Bank's Website

- Hyperlinks from and to the Bank's Internet Banking Website shall be confined to only those portals with which the Bank enters into a payment arrangement as per SLA.
- Hyperlinks from Bank's Internet Banking would normally be meant for passing on information relating to purchases made by the Bank's customers in the portal.
- Such hyperlinks shall not mislead the customer into believing that the Bank sponsors any particular products or any business unrelated to banking.
- Bank shall follow the minimum recommended security precautions as required by the RBI guidelines while dealing with requests received from other Web Sites relating to Customers Purchases.

4.22.13 Two Factor Authentication System

Bank shall offer the Two-factor authentication system to its eBanking customers to provide them with the safest and most secure Internet Banking environment.

4.22.14 Grievance Redressal

For assistance in Internet Banking Service, for transaction failure a customer may contact toll free helpline number of customer care helpdesk. For complaints of any nature, customers may contact the Branch maintaining the Primary account. Additionally, a customer may also send queries / complaints to the Internet Banking Cell, Head Office.

4.22.15 Transaction Limit Enhancement

Internet Banking users (Retail and Corporate) have daily fixed transaction limit, transaction limit is enhanced beyond the prescribed limit as per the business requirement/customer needs for a specified period.
The transaction limit is enhanced on Customer-id/e-Banking user id basis and all the accounts linked with customer-id/user id will get the enhanced transaction limit.

4.22.16 Regulatory & Supervisory Issues

c) The products should be restricted to account holders only and should not be offered in other jurisdictions.
d) The services should only include local currency (INR) products.
e) The Bank shall adhere to and comply with the guidelines issued by DFS, MOF, GOI/RBI/IBA or from the Regulatory Authorities from time to time applicable to Internet Banking.

4.23 Cloud Computing Policy

4.23.1 Introduction

Cloud computing is a technology that allows users to access and use shared computing resources and services via the Internet or a Virtual Private Network. It gives users access to resources . Cloud computing offers On-demand Service, Broad network access, Resource pooling, Rapid elasticity, Measured service etc. The Cloud strategy of the Bank shall be part of the overall IT or business strategic planning. At the backend, cloud computing can make use of virtualization and grid computing. In grid computing, networked computers are able to access and use the resources of every other computer on the network.

4.23.2 Scope

This policy covers for hosting in the cloud, competent authority from whom approvals need to be obtained, users who are authorized to access applications in the cloud, cloud computing models to be considered, selection criteria for the cloud service provider, audit and inspection of cloud services.

4.23.3 Guidance

- Cloud services shall be availed by the Bank only after obtaining approval from IT Strategy Committee of the Board.
- The use of such services must comply with Bank's existing policies such as IT Policy and its Sub-Polices and Information Security Policy.
- A committee comprising of two AGM/DGM/GM and CISO shall oversee the implementation aspects of availing cloud computing services. The committee shall comprise of AGM-IT / Chief Information Officer (CIO), General Manager (Risk Management), General Manager(Strategic Planning), General Manager(Compliance) and Chief Information Security Officer (CISO) of the Bank. Quorum for the committee will be three. The Manager (IT) will be the convenor of the committee. The committee will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing -service provider. The above committee shall decide what data may or may not be stored in the Cloud.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the CIO after getting views of CISO before placing in IT steering committee.
- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the service provider.
- Initially the non-financial (non-transactional) non critical applications may be considered for deployment in cloud and accordingly such applications need to be identified by the above committee. Depending on the application, cloud service providers must be made aware of the record retention requirements of the Bank.
- Concerned department whose applications are being hosted in cloud shall identify their officials and authorize them to have access to specific applications. Unauthorized users shall not access applications hosted in cloud.

- Bank and the cloud service provider shall mutually arrive at and frame a security policy specific to the cloud services taken by the Bank. The above policy shall take into consideration the IT Policy/IT Security Policy/Internet Usage Policy/Outsourcing policy etc. of the Bank.
- Bank or its Information System auditors shall conduct audit of cloud services taken by the Bank and audit clause shall be part of the agreement with the cloud service provider.
- Besides IS audit of cloud service, Bank shall also conduct pre-announced / unannounced site inspection at the service provider's facility. Procedure for inspection shall be framed and agreed upon mutually.

4.23.4 Other Concerns to be addressed

Many issues should be considered carefully before adopting a Cloud Computing solution. The list below features some of the more important issues to consider and to be addressed before shortlisting the cloud service provider:

- Integrating with existing applications and architecture
- Data security and confidentiality issues
- Performance issues
- Quality and credibility of cloud provider
- Low availability
- Not meeting compliance requirements
- Policies and regulatory issues

4.23.5 Cloud deployment model and Cloud service usage

Various cloud deployment model exists in the industry and hence bank shall determine the model best suited to it by assessing pros and cons of each model

- Private cloud (cloud infrastructure that is provided for exclusive use by single Bank or individual)
- Public cloud (cloud infrastructure that is openly used by general public)
- Community cloud (cloud infrastructure that is only for banks)
- Hybrid cloud (cloud infrastructure that is a combination of two or more of the above)
- Any other deployment model as applicable.
- At present all data of the Bank, for domestic and foreign operations resides in India. In the event of any IT service being hosted on a public cloud, the Cloud Service provider shall ensure and assure that the data will remain in India and will not be copied to any location/zone outside India, even for purposes of Availability.
- When the Bank decides to discontinue the service, Cloud service provider shall ensure and assure that all data, applications, configuration files and logs are handed back to bank, and all copies are effectively destroyed.
- Business continuity and disaster recovery plans must be well documented and tested. The cloud provider must understand the role it plays in terms of backups, incident response and recovery. Recovery time objectives should be stated in the contract.

- Since the cloud service providers are offering different cloud service usage models as given under, Bank may decide upon the same based on the requirement.

(i) Infrastructure as service
(ii) Platform as service
(iii) Software as service
(iv) Any other applicable usage model

4.23.6 Selecting the cloud service provider

Criteria for selection of cloud provider with quality and credibility are of utmost importance. Thorough Background check of the service providers shall be carried out by the Bank. The following major factors shall be considered while selecting the service provider:

- Function (simple, easy to understand the characteristics and process of products)
- Service (accurate, fast, focus on meeting customer's requirements)
- Flexibility (modify products in a timely manner to fulfill customer requirements)
- Safety (hold authoritative security certification and an auditable overall management and control)
- Reliability (high availability and minimize the impact on business)
- Stability (strong capital investment and good profit growth trend)
- Credibility (trusted brand and good reputation in the market)
- Compatibility (associativity with mainstream applications and systems)
- Transparency (clear billing table and detailed financial report)
- Price (deployment and operating costs are lower than similar other service)
- The service provider should have relevant standards or certifications such as ISO 27001/ cloud specific certifications like ISO 27017/ ISO 27018/ CSA STAR/ PCI / PA-DSS etc.
- Service providers should be able to provide the following minimum functions or services

(i) Enhance transparency, implement effective audit controls
(ii) Efficient data encryption
(iii) Real time log inquiry
(iv) Remote auditing service
(v) Forensics and forensic tools
(vi) Incident reporting mechanism
(vii) Clear responsibilities
(viii) Data Centre site audit
(ix) Clearer systems and tools for data portability
(x) Clearer systems and tools for service portability
(xi) Privacy protection technology
(xii) Better accountability framework
(xiii) Provide effective framework for data classification and grading
(xiv) Privilege Based Secure Access of Data or application.

4.24 Outsourcing of IT Technology

4.24.1 Introduction

The banking industry in India has witnessed an all-round expansion driven by changing consumer profile, intense market competition, emphasis on financial inclusion. regulatory environment and rapid technological innovation. To meet these challenges effectively in a time bound manner, it is necessary to hire the services of third-party vendors (service providers) having expertise in the area which are not core banking activities. Therefore, a well-defined "Outsourcing Policy" for the Bank is not only desirable but also imperative for Governance.

4.24.2 Objectives

The following are the objectives of the policy.

- To regulate the various financial and non-financial activities that are outsourced at present in the bank and proposed to be outsourced and to mitigate operational risks.
- To lay down the broad policy framework.
- To provide direction and guidance for effective oversight, due diligence and management of risks associated with outsourcing like Strategic risk. Reputation risk, Compliance Risk, Operational Risk, Legal Risk, exit Strategy Risk, Counter party Risk, Country Risk, Concentration risk etc.

4.24.3 Policy Framework

- The Policy shall contain basic risk management aspects, and dynamic aspects of Risk Management , Evaluation Criterion. Monitoring and Control etc.
- Bank shall engage the services of an outside agency herein after referred as service provider, to undertake permitted activities and shall perform its proper evaluation.
- The policy is applicable to all types of outsourcing arrangements entered into by the bank with a service provider located in India or elsewhere. The service provider may either be a member of the group/conglomerate to which the bank belongs, or an unrelated party.

4.24.4 Activities to be Outsourced

- The intended activities that are normally undertaken by the bank can be outsourced after ascertaining the regulatory norms and defining terms & conditions for outsourcing of particular activity taking into account the risk and materiality involved.

- Application/Document Verification.
- Marketing and research (product development etc.)
- Information system monitoring, management and maintenance (data entry and processing, help desks, back office related activities etc.)
- The type of activities those that are general in nature, which do not require high technical competence like sending due notices, escalation of ticketing etc.
- The type of activities those that are normally technical in nature and bank does not possess technical competence to handle the activity or the creation of infrastructure is not cost effective. e.g. Data warehousing & mining etc.
- Facility management services
- Recovery agents, Business Correspondents (BCs) & Security Guards, website maintenance, IT services etc.
- Activities permitted by Regulator.
- Activities not prohibited by law and as decided by Bank

4.24.5 Prohibited Outsourcing Activities

The following activities, which are part of the core management functions of the bank, shall not be outsourced like Internal Audit, Compliance Function, Determining compliance with KYC norms - verification of KYC norms, According sanction for loans and review of sanction, Management of investment portfolio, Putting through mortgage transaction, Safe custody of loan document, Corporate planning & performance budgeting . Compromise/Settlement of NPAs etc.

4.24.6 Legal obligations and regulatory and supervisory requirements

It is imperative for the bank, when performing its due diligence in relation to outsourcing, to consider all relevant laws, regulations, guidelines and

conditions of approval, licensing or registration. Bank will ensure adherence to extent CVC/RBI guidelines.

Outsourcing arrangements should not affect the rights of a customer against the bank, including the ability of the customer to obtain redress as applicable under relevant laws. Since the customers are required to deal with the service providers in the process of dealing with the bank, the bank should incorporate a clause in the product literature/brochures etc., stating that they may use the services of agents in recovery/sales/marketing etc. of the products. The role of agents may be indicated in broad terms.

4.24.7 Management of Risk

To enable sound and responsive risk management practices, due diligence and management of risks arising from outsourcing activities, all concerned Offices/HO departments who decide to outsource an activity shall follow principles applicable to arrangements entered by the bank with the service provider.

4.24.8 Evaluation of the Risks

Evaluation shall be carried out to ensure that the outsourcing does not result in the internal control, business conduct or reputation of the bank being compromised or weakened. For this purpose, user department/Circle Office/Zonal Office shall identify the role of outsourcing in the overall business strategy and objectives of the bank and its interaction with corporate strategic goals. Comprehensive due diligence on the nature, scope and complexity of the outsourcing shall be carried out to identify the key risks and risk mitigation strategies.

Analysis of the impact of the arrangement on the overall risk profile of the bank and whether there are adequate internal expertise and resources to mitigate the risks identified shall be carried out. Analysis of risk return on the potential benefits of outsourcing against the vulnerabilities that may arise. ranging from the impact of temporary disruption to that of an unexpected termination in the outsourcing and whether for strategic and internal control reasons, the arrangement should not be entered into. Such evaluation shall be performed by the user department planning to enter into an outsourcing arrangement and also re-performed periodically on existing arrangements, as part of the outsourcing approval and strategic planning or review processes of the bank.

Banks shall evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. Further, the following risks that are associated with outsourcing shall be addressed before finalizing the service provider.

- Strategic Risk - The service provider may conduct business on its behalf, which is inconsistent with the overall strategic goals of the bank.
- Reputation Risk - Poor service from the service provider, its customer interaction not being consistent with the overall standards of the bank.
- Compliance Risk- Privacy, consumer and prudential laws not adequately complied with.
- Operational Risk - Arising due to technology failure, fraud, error, inadequate financial capacity to fulfill obligations and/or provide remedies.
- Legal Risk - includes but is not limited to exposure to fines, penalties or punitive damages resulting from supervisory actions, as well as private settlements due to omissions and commissions of the service provider.

- Exit Strategy Risk- This could arise from over-reliance on one firm, the loss of relevant skills in the bank itself preventing it from bringing the activity back in-house and contracts entered into wherein speedy exits would be prohibitively expensive.
- Counterparty Risk – Due to inappropriate underwriting or credit assessments.
- Country Risk - Due to political, social or legal climate creating added risk.
- Contractual Risk - arising from whether or not the bank has the ability to enforce the contract.
- Concentration and Systemic Risk - Due to lack of control of individual banks over a service provider, more so when overall banking industry has considerable exposure to one service provider.

4.24.9 Liabilities of Principal employer

The Contract Labor Act provides respite and recourse to contract labor from non-payment of wage by allowing them access to the principal employer in the event of a default by the contractor. Bank shall therefore take necessary safeguards while outsourcing any activities

4.24.10 Appraisal of Service Provider

While outsourcing or renewing contract of outsourcing of an activity with a service provider, Bank shall take into consideration that the Service Provider is not owned or controlled by any Director or Officer/Employee of the Bank or their relatives having the same meaning as assigned under Section 6 of the Companies Act. 1956.

The outsourcing arrangements can be entered into by the Bank with a service provider located either in India or elsewhere.

Bank shall take steps to ensure that Service provider employs the same high standard of care in performing the services as would be employed by the Bank if the activities were conducted within the Bank without outsourcing.

4.24.11 Evaluating the capability of Service provider

In considering or renewing· an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with the obligations in the outsourcing agreement. Due diligence should take into consideration qualitative and quantitative, financial, operational and reputational factors. Bank should consider whether the service provider's systems are

compatible with its own and also whether their standards of performance including in the area of customer service are acceptable to it.

Bank should also consider, while evaluating the capability of the service provider, issues relating to undue concentration of outsourcing arrangements with a single service provider. Wherever possible, the bank should obtain independent reviews and market feedback on the service provider to supplement its own findings.

Due Diligence should involve an evaluation of all available information about the service provider. including but not limited to:-

- Past experience and competence to implement and support the proposed activity over the contract period.
- Financial soundness and ability to service commitments even under adverse conditions.
- Business reputation and culture, compliance, complaints and outstanding or potential litigation.
- Security and internal control, audit coverage, reporting and monitoring environment, business continuity management.
- External factors like political. economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact service performance.
- Ensuring due diligence by service provider of its employees.

4.24.12 Materiality of outsourcing

Material outsourcing arrangements are those, which if disrupted have the potential to significantly impact the business operations, reputation or profitability. Keeping in view the above, once the financial activity to be outsourced and its service provider is selected, Bank shall assess its materiality of outsourcing based on:

- The level of importance to the Bank of the activity being outsourced.
- The potential impact of the outsourcing on the Bank on various parameters such as earnings, solvency, liquidity, funding capital and risk profile.
- The likely impact on the Bank's reputation and brand value and ability to achieve its business objectives, strategy and plans, if the service provider fails to perform the service.
- The cost of outsourcing as a proportion to total operating cost of the Bank.
- The aggregate exposure to that particular service provider, in cases where the Bank has outsourced various functions to the same service provider.

4.24.13 The Outsourcing Agreement

The terms and conditions governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by bank's legal counsel on their legal effect and enforceability. Every such agreement should address the risks, risk mitigation strategies and service levels (SLA).

Pre contract integrity pact to be signed between the bank and the bidder. Under the Integrity Pact, two Independent External Monitors (IEMs) would be nominated by eve for BSCB to review the tendering process independently for all tenders above Rs. 50 Lacs

4.24.14 Confidentiality and Security

- Bank shall ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.
- Access to customer information by staff of the service provider shall be on 'need to know' basis. i.e. limited to those areas where the information is required in order to perform the outsourced function.
- The bank shall ensure that the service provider is able to isolate and clearly identify the bank's customer information. documents. records and assets to protect the confidentiality of the information. In instances. where service provider acts as an outsourcing agent for multiple banks. care should be taken to build strong safeguards so that there is no comingling of information/documents, records and assets.
- The bank should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.
- The bank should immediately notify Regulator in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the bank would be liable to its customers for any damage.

4.24.15 Business Continuity and Management of Disaster Recovery Plan

- The bank shall require its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. Bank shall ensure that the service provider periodically tests the business continuity and recovery plan and may also consider occasional joint testing and recovery exercises with the service provider.
- In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, bank shall retain an appropriate level of control over the

outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the bank and its services to the customers.

- In establishing a viable contingency plan, bank shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house. in an emergency and the costs, time and resources that would be involved

- **Outsourcing IT works and services**

IT outsourcing is defined as the significant contribution by external vendors in the physical and human resources associated with the entire or specific components of the IT Infrastructure. It is turning some IT activity of the Bank overall or part to an outsider.

Bank may outsource the works, where the services are cheaper, faster, better and justifiable. It also facilitates to have access to expertise, knowledge and capabilities that are not found within the organization. IT outsourcing covers wide spectrum of works and services like data centre infrastructure management (BMS), hardware and software maintenance (AMC), application management (ATS & FM Services), network management, ATM services, information security management and so forth.

Since banks specialize in financial intermediation, they implement IT by engaging external suppliers who can provide them IT expertise. Specialization and economies of scale ensure that banks get better quality products and services at lower costs. Outsourcing has thus become a business imperative and success of outsourced IT services depends on banks' ability to manage and monitor sourcing partners to maximize benefits from IT deployment. However, it may be noted that banks can outsource services or processes but never the responsibility and accountability.

Outsourcing is defined as turning over all or part of an organizational activity to an outsider. Outsourcing allows an organization have access to expert se, knowledge and capabilities that are not found within the organization.

a) Capability of outsource vendor

In considering or renewing an outsourcing arrangement, appropriate due diligence shall be performed to assess the capability of the vendor to comply with obligations in the outsourcing agreement. Due diligence shall take into consideration qualitative and quantitative, financial, operational and reputational factors. Bank shall consider whether the vendor's systems are compatible with their own and also whether their standards of performance including in the area of customer service are acceptable to it. Bank shall also consider, while evaluating the capability of the vendor, issues relating to undue concentration of outsourcing arrangements with a single service provider. Where possible, Bank may obtain independent reviews and market feedback on the vendor to supplement its own findings.

Due diligence shall involve an evaluation of all available information about the service provider, including but not limited to the following:

i. past experience and competence to implement and support the proposed activity over the contracted period.
ii. financial soundness and ability to service commitments even under adverse conditions.
iii. business reputation and culture, compliance, complaints and outstanding or potential litigation.
iv. security and internal control, audit coverage, reporting and monitoring environment, business continuity management and
v. ensuring due diligence by vendor of its employees.

b) Monitoring and Control of Outsourced Activities

The activities of outsourced vendor to be monitored & controlled. It shall ensure that outsourcing agreements with the service provider contain provisions to address their monitoring and control of outsourced activities.

Regular audits by either the internal auditors or external auditors to assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement should be done, the compliance with its risk management framework and the requirements of these directions. A robust system of internal audit of all outsourced activities shall also be put in place and monitored by the Audit Committee of the Board (ACB).

Certain cases, like outsourcing of cash management, might involve reconciliation of transactions between the Bank, vendor and other organizations. In such cases, bank shall ensure that reconciliation of transactions are carried out in a timely manner. An ageing analysis of entries pending reconciliation with outsourced vendors shall be placed before the ACB and bank shall make efforts to reduce the old outstanding items therein at the earliest.

c) Services cannot be Outsourced

Particularly, core management functions including Internal Audit, Strategic and Compliance functions and decision-making functions determining compliance with KYC norms for are not allowed to be outsourced to vendor.

d) Risk Management in Outsourcing Arrangements

Certain element of risk arises as responsibilities for critical initiatives are shifted in the hands of outsourced organization. Failure to mitigate and prevent these risks can result in significant financial loss, legal issues, and public opinion misconceptions, ultimately damaging the organisation. As such, the risks viz. Strategic risk, Reputation risk, Operational risk, Compliance Risk and systemic risk are to be thoroughly understood and assessed in regard to business and contractual relationships entered into with various third parties. Failure of a vendor in providing a specified service, a breach in security/confidentiality, or

non- compliance with legal and regulatory requirements among others may lead to reputation/financial losses for the bank and may also result in systemic risks within the banking system in the country.

Risk evaluation and management for outsourcing services to vendor should include the following steps:

- Identification of the role of outsourcing in the overall business strategy and objectives, and inter-linkages with corporate strategic goals.
- Comprehensive due diligence on the nature, scope and complexity of the outsourcing to identify the key risks and risk mitigation strategies.
- Analysis of the impact of such arrangement on the overall risk profile of the bank, and whether adequate internal expertise and resources exist to mitigate the risks identified.
- Analysis of risk-return on the potential benefits of outsourcing vis-a-vis the vulnerabilities that may arise.
- Banks should evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. All outsourced information systems and operations may be subject to risk management and security and privacy policies that meet the bank's own standards.

e) Off -shore outsourcing of Services

The engagement of service providers in a foreign country exposes a bank to country risk- economic, social and political conditions that may adversely affect the bank. Such conditions could prevent the service provider from carrying out the terms of its agreement with the bank. To manage the country risk involved in such outsourcing activities, the bank shall take into account and closely monitor government policies, political, social, economic and legal conditions in countries where the service provider is based, during the risk assessment process and on a continuous basis, and establish sound procedures for dealing with country risk problems.

This includes having appropriate contingency and exit strategies. In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified.

- The activities outsourced outside India shall be conducted in a manner so as not to hinder efforts to supervise or reconstruct the India activities of the bank in a timely manner.
- The outsourcing related to overseas operations of the bank would be governed by these as well as host country guidelines. Where any differences arise, the more stringent of the two would prevail. However, where there is any conflict, the host country guidelines would prevail.

f) Redressal of Grievances related to Outsourced services

Bank shall constitute Grievance Redressal Machinery within the bank. The name and contact number of designated grievance redressal officer of the bank shall be made known to general public.

For above, Committee of five (05) members to be formed with at least two (02) General Managers and Quorum for the meeting will be minimum three (03) members.

The operating guidelines (roles and responsibilities of stakeholders, review, reporting of activities etc.) for outsourcing of activities shall be prepared by the department.

4.25 Policy for Amendment

4.25.1 Introduction

Policy amendment is defined as an amendment to policy, new policy, or revisit of the existing policy in every 3 years or as and when required. Policy amendments are to be submitted to the Board of Director of the Bank for the approval.

4.25.2 Roles and Responsibilities

ROLE	RESPONSIBILITY
Board of Directors	To approve the amendment
AGM /GM- IT	To propose any amendment in the policy document.
Supervision &Monitoring	GM-IT shall monitor the procedure of amendment for the policy.

4.25.3 Procedure

1. The AGM/GM of the IT department should take request input from IT team (Application/Network/ Infrastructure / Support) for policy amendment.
2. The amendment will be put into the policy amendment format as per the Annexure by the respective IT team.
3. The AGM / GM -IT will submit the amendment to the next scheduled meeting of Board of Directors for input and approval.
4. Substantive changes to the policy amendment made at the first reading should be done by Board of Directors
5. As the policy amendment gets approved by Board of Directors ,It will be placed with Board resolution.

4.25.4 Annexure

Policy Amendment Form	
Policy Name:<insert policy name or identifier>	**Reference:**< insert circular number of the statutory authority>
Raised by:<Application/Network/Infrastructure/Support Team>	**Date raised:**
Priority:<Low/Medium/High>	
Part 1: Describe the original point of the policy	
Part 2 : Describe the amendment that is being requested in the policy	
Part 3: Reason for the amendment requested	
Part 4: Impact of the amendment	
Part 5: Supporting Documentation / Attachments	
Amendment made by:	
Date &Signature:	
Amendment checked & confirmed by:	
Date &Signature:	

4.26 IS Audit Policy and Procedures

4.26.1 Introduction

Information Systems (IS) auditing is a systematic independent examination of the information systems and the environment to ascertain whether the objectives, set out to be met, have been achieved. Auditing is also described as a continuous search for compliance. The Auditors may not necessarily examine the entire system. They may examine a part or parts of it only. Auditing covers primarily the following broad major areas of activity:

a. gathering of information
b. comparison of information and
c. asking why

The Information System Audit (also known as IS Audit) is an integral component of bank's pursuit of robust IT security and actionable oversight. Solid corporate governance requires that banks regularly undergo IS audits of security measures of its IT infrastructure. It helps management to understand the risks associated with the Information System function within an organization.

With the widespread adoption of technology by the Bank, technology-related risks have increased. This change demands the need for developing Internal Control Frameworks that address the IT controls.

An information system audit is conducted to evaluate the information systems and suggest measures to improve their value to the bank. The audit will be used as an effective tool for evaluation of the information system and controlling information systems misuse/improper use.

A periodic information system Audit is essential to monitor Bank's system of internal control and procedures. A proper information system Audit process helps Bank in the effective discharge of their responsibilities. It provides assurance of the risk and operational performance of the bank.

4.26.2 Scope of Audit

The IS auditor will require to include in the scope of the audit the relevant processes for planning and organizing the information systems activity and the processes for monitoring that activity.

The scope of the audit will also include the internal control system(s) for the use and protection of the information and the Information Systems, as under:

a) Data: -

Data objects in their widest sense, i.e., external and internal, structured and non-structured, graphics, sound, system documentation etc.

b) Application systems: -

Application system is understood to be the sum of manual and programmed procedures.

c) Technology: -

Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

d) Facilities: -

Resources to house and support information systems, supplies etc.

e) People: -

Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

4.26.3 Responsibilities of the owner of the business process

The IS auditor will require to review the responsibilities of the business process owners, as under and assess whether these are appropriate to support the policies set at the Board of Director's level.

Assessment of whether the business process owners have the skills, experience and resources necessary to fulfil this role.

Review of the information received by the business process owners and to assess whether it is appropriate to enable them to discharge their responsibilities and to monitor compliance with the policies.

Information that may be considered appropriate includes as under:

a) Reports of attempted access to the systems supporting business processes and follow-up action taken.

b) Reports of changes to user access rights, including new users and those whose access rights have been removed.

c) Reports of the results of business continuity tests and follow-up action taken.

d) Reports on the results of feasibility studies and tendering processes for systems acquisition.

e) Reports of the results of user acceptance testing of new systems or changes to the existing systems.

f) Reports on performance against agreed service levels.

g) Statistics on the availability, number of failures, number of system changes requested and implemented etc.

h) Status of system changes in progress.

i) Reports of changes to corporate data dictionary entries.

j) Assessment of the system which produces the above information and its reliability, integrity and potential for management override.

k) Where the Bank has internal audit resources, which is an important element of the corporate governance process, assessment whether the appropriate level of the involvement of the internal audit resources has been provided.

4.26.4 Reporting

The IS auditor will require to address reports on the corporate governance of the information systems to the Audit Committee/Board of Directors or any other designated authority in the Bank. In case of detection/identification of failures in corporate governance, the same will require to be urgently reported to the designated authority in the Bank. The IS audit report on corporate governance of information systems should, among others, include the following:

a) A statement that the Board of Directors is responsible for the Bank's Information Systems

and formulation and implementation of the system of internal controls.

b) A statement that a system of internal controls can only provide reasonable and not absolute assurance against material misstatement or loss.

c) A description of the key procedures, which the Board of Directors has approved/established, to provide effective internal control and the related supporting documentation presented to the Board of Directors.

d) Information on any non-compliance with the national or industry codes of practice for corporate governance.

e) Information on any major uncontrolled risks.

f) Information on any ineffective or inefficient control structures or control measures together with the IS auditor's recommendations for improvement.

g) The IS auditor's overall conclusion on the corporate governance of the information systems, as defined in the scope of audit

4.26.5 Information System Audit Methodology

The IS audit work includes manual procedures, computer assisted procedures and fully automated procedures, depending on whether it is around, though, with or a combination of all these types of audit. In many cases, a combination of these techniques is required. The IS auditors may utilize the manual procedures when they are more effective than the other alternatives or when these procedures cannot be partially or fully automated. He/she should also use computer assisted procedures known as Computer Assisted Audit Tools (CAATs) wherever required.

1) Steps of Audit Activity

Audit activity is broadly divided into five major steps for the convenience and effective conduct of audit.

a) Planning IS Audit

Planning is the first step of the IS audit. IS auditors should plan the audit work in a manner appropriate for meeting the audit objectives. As a part of the planning process, IS auditors

should obtain an understanding of the auditee department/ office/Bank and its processes. It includes understanding of the objectives to be accomplished in the audit, collecting background information, assigning appropriate staff keeping in mind skills, aptitude etc. and identifying the areas of risk. Risk analysis of the operational system is carried out to identify the system with highest risks, considering the critical nature of the information processed through such system as well as the number and the value of the transactions processed. This is to identify the systems having the highest risk and to decide on the extent of the detailed analysis and testing to be conducted on those systems.

In this phase, IS auditors are required to understand the internal controls used within the Bank. Various techniques can be used to understand the internal controls viz. review of previous audit reports/papers, interview/interaction with the management and Information Systems personnel, observation of activities carried out within the Information Systems function and review of Information Systems documentation.

b) Tests of Controls

During this phase of IS audit, Internal Controls are tested to evaluate whether they operate effectively. This includes testing of management controls and application controls. The objective is to evaluate the reliability of the controls and find out weaknesses of the controls for meeting the IS audit objectives. IS auditor is required to make recommendations to rectify the weaknesses, observed during the course of an IS audit. While carrying out tests of controls, the IS auditors should satisfy themselves regarding the following aspects of controls ----

Identification: Bank should identify the controls to minimize the occurrence of unlawful events.

Implementation: Identified controls should be implemented.

Existence: Sometimes it happens that controls have been implemented, but in reality they do not exist due to various reasons. For example, the Bank may have stipulated that the users should change their passwords every week. But, in reality this may not be happening. Physical existence of the controls is equally important.

Adequacy: IS auditors should examine the adequacy of the controls. They should see that the controls are adequate to cover all possible threats.

Documentation: All controls should be documented to make them effective.

Maintenance: Controls should be maintained intact on a continuous basis. For example, only the provision and installation of the fire extinguishers, smoke detectors, UPS etc. do not solve the problem. These instruments should be properly maintained, so that they serve the purpose, as and when needed.

Monitoring: Controls should be monitored by means of strict supervision, surprise checks, periodic inspection etc.

c) Tests of Transactions

Tests of Transactions are used to evaluate whether erroneous transactions have led to a material misstatement of the financial information and whether the transactions have been handled effectively and efficiently. The objective is to evaluate data integrity.

d) Tests of Balances

During this phase of IS audit, final judgment is made on the extent of the losses or account misstatement that occur when Information Systems fail to safeguard assets, maintain data integrity and achieve system effectiveness and efficiency goals. The system may provide outputs, but not of the required standards to make high quality decisions. During this phase of the IS audit, computer support is often required. General Audit Software can be used to select and print confirmations; expert systems can be used to estimate the likely bad debts and so on.

e) Completion of Audit

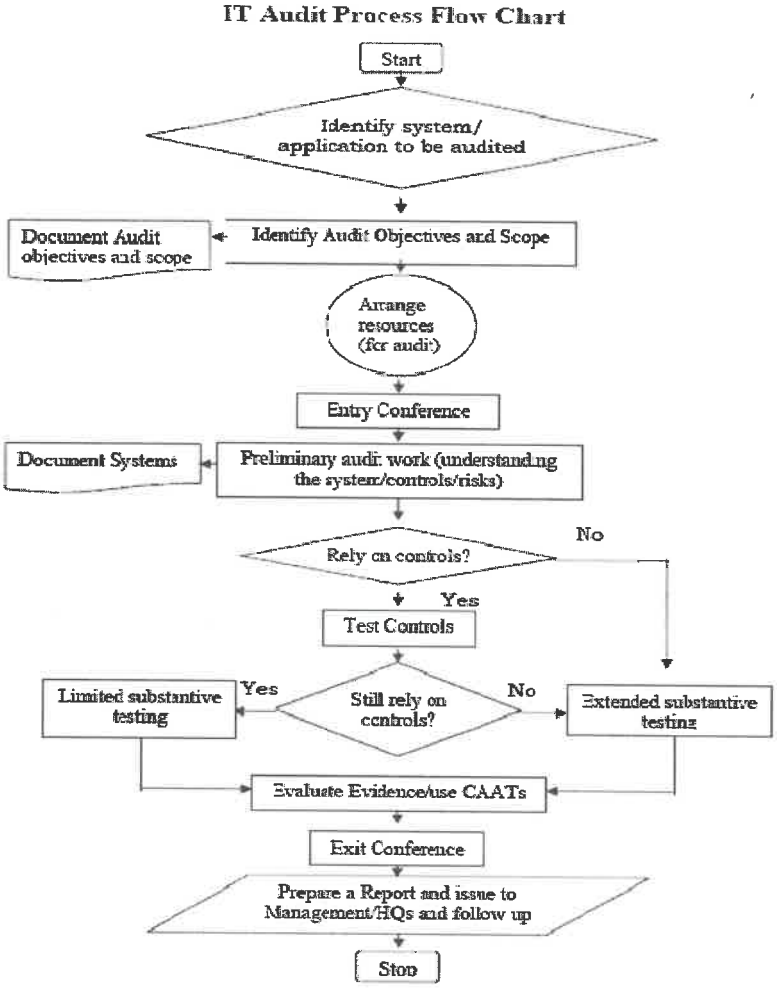
This is the final stage of IS audit. Auditors are required to form their opinion, clearly indicating their findings, analysis and recommendations. Potential IS audit findings should be discussed with the appropriate/authorized personnel throughout the course of IS auditing. Preliminary conclusions and the audit findings should be presented to the auditee during an exit conference. All potential findings with sufficient merits and preliminary IS

audit recommendations should be included for discussion in the exit conference. The exit meeting should document and include the auditee's comments and questions concerning the preliminary IS audit recommendations. The draft audit report should be the natural extension of the exit conference materials along with the discussions that took place during the exit meeting. Once the auditee's responses have been received, the final audit report should be prepared and submitted to the designated authority/ management of the Bank.

Work papers used in the auditing should be well organized, clearly written and address all the areas included in IS audit. IS audit work papers should contain sufficient evidence/information of the tasks performed and the conclusions reached, including the results achieved, issues identified and authorized signatures approving the final opinion.

A typical audit report will include, among others, an introduction to the audit objectives, scope, general approach employed, summary of the critical findings, the data to support the critical findings, potential consequences of the weaknesses, auditee's responses and recommendations to rectify the weaknesses.

2. STEPS IN IT AUDIT



4.26.6 Framework for Conducting IS Audit

A broad framework can be formed from the basic objectives of IS audit. In addition to this, IS audit evaluates the organizational set up and quality of administration of the Bank. It should be noted that IS audit is not limited by laid down procedures. It is also important to keep one's eyes and ears open. The IS auditors should, therefore, analyze what they observe and hear. The main issue involved in IS audit is confidentiality of programs, files, access rights to files and focus on software application packages. The major concerns of the IS audit, as derived from its objectives, are as under:

4.26.6.1 Safeguarding Assets:

One of the prime objectives of any audit is to ensure that the assets of the bank are safeguarded. In the computerized environment, the assets to be safeguarded are hardware, software, data and users. The yardstick to measure the importance of this objective is the expected loss that may be sustained by the Bank if the asset is destroyed, stolen, lying unutilized, service denied or used for unauthorized purposes. The IS auditors should verify that the assets are put to effective use in a secured environment. In order to determine whether the assets of the Bank are duly safeguarded, the IS auditors should inspect, among others, the following areas:

Environmental Security: It is very important for the effectiveness of all other protective measures stipulated or installed at the sites. The server room houses the all-important hardware. Its location should be a strategic one and not easily accessible. The server room should be exclusively for the server itself and the other items, equipment etc. should not be kept there.

Uninterrupted Power Supply: The uninterrupted power systems are meant for always supplying conditioned and stabilized power to computer equipment. It also provides stabilized power from battery storage when electricity fails. It is very important that the UPS functions properly when electricity fails. The UPS should be maintained regularly.

Electrical Lines: Electrical cabling and wiring constitute the basic components. Faulty electrical cabling and wiring are responsible for operational failures. There should be a separate and proper earthing for the dedicated electrical line.

Data Cabling: Most of the network problems are cable related. Hence, all possibilities of routing cables, locations of cable closets, sites of Switch, Router installation etc. should be explored before finalizing the plan. Detailed map of the cable lay out including Switches, Routers is very important to guide the hardware service engineer in the event of LAN cable fault. Further, electrical cable and data cable should not cross each other to avoid possible disturbance during data transfer.

Fire Protection: Fire alarm system, smoke detectors and fire extinguishers are very important to deal with the event of fire breaking out. Little care is required while operating gas-based extinguishers because they replace oxygen and thereby, extinguish the fire. Water is effective. But, it is dangerous to use in proximity to live equipment. Dry powder or foam type extinguishers are not advisable because they leave deposits on the equipment.

Insurance: All critical computer equipment's are required to be insured with reputed insurance firm/s to secure the Information System resources/assets of the Bank.

Annual Maintenance Contract: Periodic maintenance of the computers, network etc. is essential to ensure trouble free operations of the equipment. For this purpose, it is required that the annual maintenance contract is awarded and renewed in time. At the same time, it is also essential that the maintenance staff is available in time. There should be a proper record of the activities carried out during maintenance.

Logical Security: It restricts access to the system if the user fails to identify himself/herself to the system correctly. Login name/user ID and password are controls for this security Logical security at the application system level gives access rights to specific application software depending on the responsibility and authority of the user. IS auditors should verify the effectiveness of the logical security in place by evaluating its controls. Secrecy and security of the user ID and password, different levels of access rights and their allocation to the users, creation of users, its records, users created for maintenance purpose and their termination on completion of the work, user log in status report, presence of dummy user ID in the system etc. are some of the points which require consideration of the IS auditors.

4.26.6.2 Data Integrity:

Data is the most important resource in a computerized environment, which needs to be accurate, complete, consistent, up-to date and authentic. The IS auditors are concerned with the possibility of deviation from the standards. They are required to verify how well data integrity is maintained and find out any laxity therein.

The examination of the following points are very important in respect of data integrity:

a) Data Input Controls

The largest number of controls is available at the time of data entry in the system. Data Input Controls are error prone because the activities involved in data entry are of routine and monotonous nature. Data entry is also a major area for intentional fraudulent activity. It involves addition, deletion, modification or alteration of the input transactions or data. Hence, the IS auditors should minutely evaluate the effectiveness of the data input controls. The use of the scanner and inputs to the system through floppy should be monitored and controlled.

b) Data Processing Controls

The application system processes the data on-line on day-to-day basis. The IS auditors are concerned about the Data Processing Controls. They should examine that only designated/authorized officers perform start-of-day operation. The day end process should be completed with the generation of the prescribed reports. It is also required that proper record is maintained in respect of the corrections made in the database under authentication.

c) Patching of Programs

It uses the file structure of the existing database files and is capable of effecting changes in a data file. It bypasses the proper menu access controls provided by the application software system and does not leave any audit trail. It can add, modify, alter and delete the data. The behavior of the approved programs are known and certified, but it is uncertain in the case of such patch programs. They usually bypass all the safeguards available to the system programs. They conveniently flout all norms to achieve results at any costs. Therefore, the IS auditors should verify that only approved programs are loaded in the system and the application programs are exactly identical with the list of the approved programs in respect of file name, file size, date and time of compilation. It is also necessary that a record be maintained regarding the patch programs used indicating the reasons under authentication.

d) Data Backup

Data backup is an essential aspect of all computer operations. Some commonly used computer media include hard disk, floppy disks, tape cartridges, CDROMs, DVD ROMs etc. Off-site back-ups are taken on floppies or tape cartridges, while on-site back-up is taken on hard disks. Back-up is one of the measures of the business continuity planning and is also required for archiving of old records. It is necessary that the backups are taken regularly. One set of the backup requires to be stored off site. The backups have to be tested periodically by restoring the data therefrom. The backup media have to be verified periodically for readability. Backup media should be properly labeled and numbered. This is a very important area and requires proper attention.

e) Restoration of Data

It is defined as downloading of data afresh from magnetic media, in case of crash of the system, irrecoverable corruption or loss of data, for going back online. Backup is taken at a particular point of time like beginning of day operations, end of day operations etc. Thus, restoration of data is dependent on the magnetic media and the data stored thereon. Restoration of the data is required in the event of major corruption of data. In the event of a virus attack or destruction of a server or the computer site, the only

option is to fall back upon the restoration option. Restoration of data helps to obtain a position of data as of a particular date, to establish whether any data tampering has taken place. It assists in conducting system audit as of a previous date and generates ledgers of previous years. Transactions of purged period can also be retrieved.

4.26.6.3 Business Continuity Planning:

Disruption of operations can occur because of two types of problems. First, some minor problems like power failure, UPS failure, server failure, inability to read/restore backups, cable fault etc. can disrupt the operations. Second type of disruption can occur on account of natural calamities like fire, flood, building collapse or man-made calamities like bomb blast, radiation, virus attack, induced data loss etc. Business Continuity Plan is prepared to recover from such

kind of interruptions. It relates to a higher level of failure. It is all about anticipating any disastrous event and planning adequately for the business to live through it. The IS auditors should verify the existence and operability of the Business Continuity Plan. They should also examine the awareness of the staff regarding the execution of the plan in a genuine emergency and comment upon its effectiveness. Business Continuity Plan should be documented and tested at regular intervals to assess its effectiveness.

BCP is required to satisfy short, medium and long-term recovery. In the short term, the essential systems and services are restored. Medium term plans are for recovering the Bank's systems and services on a temporary basis. Long term plans are for total recovery of the processing environment.

BCP should outline the responsibilities for all the recovery processes, procedures for reproducing the computer media, location of the backup media, priorities for recovery, sources of replacement hardware and software and alternative data communication facilities.

Output Reports: One of the basic principles in the computerized environment is known as GIGO i.e. "Garbage in Garbage out". This means that, if the input to the system is garbage (or meaningless), the output will also be garbage. Reports and printouts are generated in computerized environment to ensure the correctness of the inputs and processing. Reports are also important to ensure that the application system programs serve the needs of the Bank. Any lacunae or bugs in the application software can be located by checking the reports and printouts. The importance of checking the reports can never be over emphasized. The IS auditors should scrutinize output reports on sample basis to identify the trend, the quality of follow up and the control exercised by the management. The audit trail report should generate the user ID of the data entry operator and the authorized official for any addition, change, modification and deletion of transactions effected in the database. It should provide the evidence/information of unauthorized access outside the application menu. The IS auditors should verify whether the audit trail reports are generated and checked by the designated officials. Exceptional transaction report is also a very important report.

Version Control: Data integrity is very much dependent on the version of the software running in the system. Authorized Version of the software can lead to accurate processing. Non-standard programs are potential threat to integrity. A complete listing of the programs loaded in the

system should be available on record for verification. The IS auditors should verify that licensed copies of the operating system and the application system software are used for computerized operations.

Virus Protection: Computer virus is a program that is self-replicating and can corrupt or destroy data irretrievably. It resembles biological viruses in behavior. It may have a dormancy period and gets activated on a certain date. It is potentially disastrous. Anti-virus software is available and is capable of countering against known viruses, malicious programs. Anti-virus software is updated by the manufacturers on a regular basis to counter against the new viruses coming up. It is necessary to keep the anti-virus software updated at all times. All extraneous floppies and other media should be checked/ scanned for virus before use.

4.26.6.4 System Effectiveness:

It is expected that the Information system should improve the overall quality of work including accuracy and time consumed in performing the tasks. Further, it should be user friendly. The IS auditors should judge how effective the system is in accomplishing the goals with which computerization was introduced.

4.26.6.5 System Efficiency:

The IS auditors should examine whether every computer asset is used to its maximum operational capacity.

4.26.6.6 Organization and Administration:

Efficiency in computerized operations is dependent on the efficiency of the personnel using the computer resources. Computer personnel should do their work completely, timely, accurately and that too, with minimum resources. They should deliver more output quantitatively and qualitatively. Proper placement of the computer personnel on the basis of their aptitude, skill, knowledge and experience is very important. Computer personnel should be used effectively and efficiently with proper security for the Bank to reap maximum advantages. Segregation of duties, job description for each level, proper training to the staff, dual control aspect in performing important operations, designated system administrator with suitable back-up

arrangement etc., are important points to be considered. Records of work assigned to the staff, rotation, training imparted, login name given etc. are to be checked/verified by the IS auditors.

4.26.7 Standard Guidelines for IS Audit

The specialized nature of the Information Systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. Such standards will require to be internationally accepted standards only. This will ensure that the IS auditor performs auditing, conforming to the minimum level of acceptable performance and meeting the required professional responsibilities. The IS auditing Standards define the mandatory requirements for IS auditing and reporting. The IS auditing Guidelines provide the guidance for the application of the IS auditing standards. The IS auditor should take care of how to achieve the implementation of the Standards, the use of professional judgement in the application of the Standards and should also be prepared to justify any departure/deviation therefrom in the IS auditing work. The IS auditor shall prepare the procedure including the information on how to meet the Standards while performing the IS auditing work. However, the procedure shall not set the requirements for IS auditing.IS auditing should be performed by personnel with the required expertise and skills such as Certified Information Systems Auditor, Certified Information Systems Security Professionals etc. The profitability and the future viability of the organizations in the banking and financial sector increasingly depend on the continued, secured and uninterrupted operations of the Information Systems. Therefore, it is essential for the IS auditors to be conversant with various aspects of Information Technology and the developments taking place in this area. The role of the IS auditors is to see that the organization's assets are protected and suitable internal controls are in place to protect its information and information resources. IS audit is responsible for providing an organization with independent and objective views on the level of security that should be applied to the Information Systems. Computer Security on the other hand is responsible for implementing security in the computerized environment. The IS auditor will learn to co-exist with the Computer Security function and work together for the benefit of the whole organization ensuring that professional standards are maintained at all times.

Major areas, which will require to be IS audited, are broadly as under:

a) Safeguarding of Assets

b) Data Integrity

c) System Effectiveness

d) System Efficiency

e) Organization and Administration

f) Business Continuity Operations

IS auditing of the above areas at the micro level are as under:

Safeguarding of Assets:

The IS auditors will require to concentrate on the following areas to ensure that the Information Systems Assets of the organization are safeguarded:

a) Environmental Security

b) Data

c) Uninterrupted Power Supply

d) Electrical Lines

e) Data Cables & Networking Products

f) Fire Protection

g) Insurance of Assets

h) Annual Maintenance Contract

i) Logical Security & Access Control - Operating System Level

j) Logical Security & Access Control – Application System Level

The IS auditor shall be required to verify/inspect the following points in respect of the areas mentioned above.

Environmental Security:

The IS auditors should verify whether:

a) There is separate room for the server.

b) Server room has adequate space for operational requirements.

c) Server room is visible from a distance but is not easily accessible.

d) Server room is away from the basement, water/drainage systems.

e) Server room can be locked and the key being under the custody of the authorized persons (System Administrator) only. Entry doors are protected by biometric/PIN or proximity key card access verification. Any failed attempts or system tampering as also unscheduled movement in restricted areas, glass breakage or the opening of doors will require to be logged and immediately reported to the Control Staff at the site. The biometric system will require to store all attempts at access.

f) To access any equipment in the Data Centre, one has to pass through (preferably) a minimum of two separate security doors, utilising biometric/PIN and/or proximity key card access verification facilities.

g) Server is not in close proximity to the UPS room.

h) Access to server room is restricted to authorized persons and activities in the server room are monitored.

i) Air-conditioning system provides adequate cooling.

j) Storage devices to keep stationary and other such items are not kept inside the server room.

k) All the walls with potential access will require to be heavily reinforced.

l) Humidity and heat measuring instruments like (Thermometer and Hygrometer) are installed in the server room.

m) Temperature readings are taken throughout the raised floor and equipment areas, power rooms, basement, diesel fuel storage area, roof, generator, cooling towers, waiting and display areas.

n) Smoking, eating and drinking are prohibited in the server room to prevent spillage of food or liquid into sensitive computer equipment.

o) Briefcases, handbags and other packages are restricted from the server room, tape library and other sensitive computer area to prevent unauthorized removal of data held on removable media as also to prevent entry of unacceptable material into the area.

p) Server room is neat and clean to ensure dust free environment.

q) Scanners are kept in safe custody and access is restricted.

r) Floppy disk drives on the nodes can be disabled, if necessary for better security.

s) Steel bollards to be placed in the front of the building to prevent vehicular ingress.

t) Data Centre to be so chosen to have police protection and fire prevention services within a very short time.

Uninterrupted Power Supply:

In addition to the availability of the Generator facility at the site, the IS auditor should verify whether:

a) There is a separate enclosure and locking arrangement for the UPS.

b) Maintenance agency provides battery service regularly.

c) There is a regular contract for maintenance of the UPS and the preventive maintenance is carried as per the contract.

d) The record of the tests undertaken is maintained to verify the satisfactory functioning of the UPS.

e) UPS cabin has adequate ventilation to take care of acid fumes emitted by the Lead Acid batteries.

f) Capacity of the UPS system is sufficient to take care of the electricity load required for computers installed.

g) UPS is free of the electricity load relating to the tube-lights, fans, water coolers etc.

h) UPS functions properly when electricity fails.

Electrical lines:

The IS auditors should verify whether:

a) There is a separate dedicated electrical line for the computer equipment.

b) Power supply to computer equipment is through UPS system only.

c) The electrical wiring looks concealed and is not hanging from ceiling or nodes.

d) The circuit breaker switches exist in locked condition only.

Data Cables:

The IS auditors should verify whether:

a) A map of the cable layout is kept in a secure place with proper authority. This is helpful in timely and fast repairs of LAN cable faults.

b) Cabling is properly identified and recorded as fiber optic, co-axial, unshielded twistedpair (UTP) or Shielded Twisted Pair (STP).

c) Electrical cable and data cable do not cross each other to avoid possible disturbanceduring data transfer within the network.

Fire Protection:

The IS auditors should verify whether:

a) Fire alarm system is installed.

b) Smoke detectors are provided in the server room and in the other areas of computer installations.

c) Smoke detectors are tested on a regular basis to ensure that they work.

d) Gas type (Carbon dioxide, Halon etc.) fire extinguishers are installed at strategic places like server room, UPS room and near the nodes and printers.

e) Dry powder or foam type extinguishers should not be used as they tend to leave deposits.

f) Staff knows how to use the fire extinguishers.

g) Fire extinguishers are regularly refilled/maintained.

h) An evacuation plan is documented and rehearsed at regular intervals for takingimmediate action in the case of the outbreak of fire.

Insurance :

The IS auditors should verify whether:

a) All the computer equipment's are covered under the appropriate electronic equipment insurance policy with a reputed insurance firm.

b) A record of the original policy is maintained with the detailed list of the equipment's covered under the policy.

c) Information regarding shifting of computer equipment to or from or within the department/office is conveyed to the insurance firm.

d) Adequacy of the insurance cover should be verified as per the policy of the organization.

Annual Maintenance Contract :

The IS auditors should verify whether:

a) Stamped agreements for maintenance contract are executed and available.

b) Activities carried out during maintenance have been reported in the registers and duly authenticated.

c) Contract renewal rates are maintained in the register.

d) Access for maintenance purpose is granted only on verifying the identity of the service person.

e) The maintenance staff support is available in time.

Logical Security & Access Control – Operating System Level :

The IS auditors should verify whether:

a) Access to the systems is only through password protected user IDs. b) Operating System (OS)allots unique user identity (ID) for all users.

b) OS provides for different levels of access rights to volumes, directories and files.

c) OS prompts for change of the user password after the lapse of specified periods.

d) OS ensures secrecy and security of the user passwords and the access rights granted to a user.

e) Unrestricted access to the systems is provided only to the System Administrator.

f) Administration level access is restricted to authorized and limited persons.

g) All the security features available in the OS are enabled/taken advantage of as far as possible for ensuring better security.

h) Administration access should not be available to the officials who are under noticeperiod, retiring shortly, under disciplinary action etc.

i) OS provides for loading of virus prevention software and is implemented.

j) Record is maintained and authenticated regarding the installation of the Operating System, its up-gradation, re-installation and maintenance.

k) A register is maintained in respect of all the OS level users, giving the details such as the date of creation, suspension, cancellation, access rights granted, purpose of creation etc.

l) Users created for audit/maintenance purpose are disabled immediately after the work is over.

m) The department reviews the number of the OS level users periodically.

Logical Security & Access Control – Application System Level :

The IS auditors should verify whether:

a) System provides for unique user IDs and password for all users.

b) System provides for different levels of access.

c) System prompts for change of user password after lapse of specified period.

d) System ensures secrecy and security of the user passwords and the access rights granted tousers.

e) Unrestricted access to the entire application system menus is provided only to a Super User.

f) Application makes use of all the security features available at the Application System level.

g) Super User access in application level is not given to staff who is under notice period, retiring shortly, under disciplinary action etc.

h) The application system user list is periodically reviewed.

i) The access privileges granted in the system are in accordance with the designation/duties performed.

j) None of the staff members has multiple level or duplicate access ID in the system.

k) Allocation of the suspended, disabled user ID to new users is avoided.

l) Active user IDs of the transferred, retired, suspended or dismissed employees are not present in the system.

m) There is no dummy user ID created in the system.

n) The user ID of staff on long leave, training etc. is suspended.

o) System logs out automatically if the user is inactive for a specified time (or user consciously logs out when he/she leaves a terminal).

p) System does not allow concurrent login to a single user ID from different nodes.

q) Users, created for maintenance purpose, are cancelled on completion of the job. r) The system does not allow user to cancel his/her own user ID. s) Authority periodically reviews the user login status report.

r) Users do not share their passwords.

s) Passwords of alphanumeric characters are used.

t) Users do not write their passwords on wall, desk diary etc. and are aware of the need for the secrecy of their passwords.

u) System automatically locks the user ID after unsuccessful login attempts.

v) User log indicating date, time, node, user ID, transactions performed etc. are generated by the system and evaluated by the System Administrator.

Data Integrity :

The IS auditor will require to address, among others, the following areas under IS auditing:

a) Data Input Controls

b) Data Processing Controls

c) Patch Programs

d) Purging of Data Files

e) Backup of data

f) Restoration of Data

g) Business Continuity Planning

h) Output Reports

i) Version Control

j) Virus Protection

Data Input Controls :

The organizations in the banking and financial sector undertake diverse activities relating to the receipt of deposits, advancement of credit, investment of funds etc. Further, the areas of operation and the level of economic activities could also be different. All these activities, the transactions resulting therefrom, the data inputs required therefor including the data input controls to be in place in the organisation will require to be judiciously addressed. However, illustratively, such data input controls may relate to the following areas of activity and the IS auditors will require to verify the same.

a) History of signatures scanned is available in the system.

b) The entire stock of cheque books is fed to the system.

c) The cheque books issued are entered and confirmed in the system on day-to-day basis.

d) The data fed into various accounts including the customer accounts is accurate and correct.

e) Clear administrative guidelines exist regarding the access to live data.

f) Clear guidelines exist for on-line transactions including those put through the INTERNET by the Customers.

g) Data Administration is a part of System Administration. However, Database Administration is separate from System Administration.

h) Data Owner (DA) and Database Administrator (DBA) are independent of both the systems development and operational activities.

i) The roles of DA and DBA are clearly defined in respect of, among others, (i) definition, creation & retirement of data, (ii) database availability to Users, (iii) information and services to Users, (iv) maintenance of database integrity and (v) monitoring and performance.

Data Processing Controls:

The IS auditor should verify whether:

a) The designated/authorized officials do start-of-day process.

b) The operating staff pay attention to the error messages displayed on the screen and initiates corrective action.

c) Entries are cancelled only by the appropriate authority.

d) Cash entries are not deleted from the system. Prescribed reports are generated at the end of-day process.

e) Printouts are scrutinized and preserved.

f) Proper record is maintained in respect of the corrections made in database under authentication.

g) Master data printouts are preserved carefully

h) Input to the system through floppy is monitored and controlled.

i) Use of the scanner is monitored and controlled.

Patch Programs :

The IS auditors should verify whether:

a) The application programs are exactly identical with the standard list of approved programs in respect of file name, file size, date and time of compilation.

b) Only approved programs have been loaded in the system.

c) There are programs other than the approved ones.

d) There is a record of the patch programs used and the reason thereof under authentication.

Purging of Data Files :

The IS auditors should verify whether:

a) Purging activity is recorded and maintained in a register.

b) Purged backup media is kept properly under safe custody.

c) Access to purged data is restricted.

E. Back up of Data :

The IS auditors should verify whether:

a) All the floppies/CDs/tapes, purchased, pertaining to the OS software, application software and utility programs, drivers etc. are recorded in a register and properly stored.

b) Hardware, software, operating system, printer manuals are properly labelled and maintained.

c) Latest user manuals of the application software and other end-user packages runningon the system are available for guidance.

d) Daily/weekly/monthly and quarterly back-up of data is taken without fail and isavailable (as per requirement).

e) Backup tapes are properly labeled and numbered.

f) Proper storage procedures and facilities are in place for backup copies.

g) There is offsite storage of one set of the backup data.

h) Backup tapes are verified/tested periodically by restoring the data and record maintained.

i) Back up media is verified periodically for readability.

j) Record is available in respect of such verification.

k) Backup media are phased out of use after a specified period.

l) Backup register is maintained wherein all the events pertaining to the backup including the procedure of backup are recorded.

m) Physical and fire protection is provided to backup media.

Restoration of Data :

The IS auditors should verify whether:

a) The instructions for restoration of the back-up data have been compiled.

b) The data integrity is verified after the restoration work is over.

c) Activities carried out during the restoration work are recorded indicating date, time, reason for restoration and size of the data restored.

Business Continuity Planning (BCP) :

The IS auditors should verify whether:

a) Business continuity plan has been documented.

b) BCP covers all levels of disaster from partial to total destruction of facilities andcontains guidelines to help determine the level of recovery necessary.

c) A copy of the plan is securely stored off site.

d) Detailed restart procedure has been documented in the plan.

e) BCP has been tested and is regularly tested to assess its effectiveness.

f) There is awareness among the staff members about the BCP and the modalities of its execution in case of an emergency.

g) Ready or alternate source of hardware/software is there to resume business activity within the shortest possible time after disruption.

h) A reliable backup of data and software is available all the times for restoration.

Output Reports:

The IS auditors should verify whether:

a) The audit trail report generates the user ID of the operator and the official for any addition / modification / deletion of the transaction data effected in the database.

b) Audit trail report is generated daily. Entries are scrutinized and verified.

c) Audit trail report indicates the evidence/information of unauthorized access outside application menu.

d) List of the cancelled entries is scrutinized and reasons for cancellation are recorded.

Version Control :

The IS auditors should verify whether:

a) The computer system has authorized version of an OS, authorized version of anti-virus software with its latest updates.

b) There exist the documentary evidence/information about the authenticity and the right to use the copy of the OS software, OS system utility, third party software, the runtime system of specified language or database in use and the anti-virus software.

c) Legally licensed copies of the software are used for computerized operations and the licenses are currently in force.

d) Changes made to the application software with the approval from the controlling office/ department.

Virus Protection :

The IS auditors should verify whether:

a) Antivirus software is loaded in the system.

b) Antivirus software is regularly updated to cover software updates against the latest viruses.

c) All extraneous floppies are checked for virus including the floppies carried by the IS auditors.

System Effectiveness:

The IS auditors should verify whether:

a) Computerized operations provide better customer service in terms of time and quality.

b) Staff serves a larger number of customers during the day than prior to the introduction of online operations.

c) Customer information is provided timely and accurately.

d) The system reflects any improvement in the overall quality of products and services offered.

e) System has improved the tasks accomplishment capacity of its users by enabling them to be more productive.

f) Users are satisfied with the performance of the system.

g) System is user friendly and takes less effort.

h) The users are putting the software to frequent use, which requires less effort and is easier to use and the users are satisfied with the performance of the software.

System Efficiency:

The IS auditors should verify whether:

a) Department/Office ensures the use of every computer asset.

b) Department/Office utilizes every computer asset to its optimum capacity.

c) Periodical maintenance of the hardware asset ensures its uninterrupted service.

d) The online operations help complete day's workload on the same day consuming less time than the time taken for the respective manual operations.

e) The online operations provide accurate, complete, and consistent data at each stage of processing.

f) Department/Office takes consistency check of balances daily to aid in the detection of errors or fraud.

g) Department/Office uses the hardware peripherals such as printers, nodes etc. efficiently.

Organization and Administration:

The IS auditors should verify whether:

a) There is an Information Systems Security Program for the entire organisation, approved by the Board of Directors.

b) There is a Corporate Information Systems Security Policy, well defined and documented and implemented including Information Systems Awareness Program.

c) There is an established hierarchy in the organization with a Senior Executive In charge of the implementation of the Corporate Security Policy with Information Systems Security Officials at various levels in an Office.

d) Identified System Administrator for each computerized Office / Department, as required.

e) Job description for each level is prepared and implemented (including System Administrator).

f) Training is imparted to all staff members in turn for better results and output.

g) The entire staff is involved/motivated for working in the online environment.

h) The department allots online jobs to staff members accessing performance parameters like willingness, aptitude, expertise, skill, experience, and knowledge.

i) Record is maintained showing details of the work assigned, period of assignment, rotation, training imparted, login name and acknowledgement obtained.

j) Dual control aspect is implemented for the important online operations.

k) The functions of initiating, authorizing, inputting, processing, and checking of the data are separated to ensure that no person has complete control over a particular function. Therefore, abuse of that function is not possible without collusion between two or more individuals.

l) Rotation of duties is carried out at regular intervals.

m) System Administrator is supervised and controlled with respect to the creation of user ids at the OS level and Application Software level.

n) There are at least 2 persons for key functions of online operations to take care of absenteeism.

o) Department/Office ensures to bring up the servers into operation readiness sufficiently in advance before the commencement of the business hours.

p) Computers are covered to keep them free from dust, rainwater etc.

q) Clear communication from the Management of the organisation to the effect that each member of the staff is responsible for maintaining security in the organisation, as per the Security Policy.

4.26.8 Type of Audit Evidence/Information

When planning the IS Audit work, the IS auditor should take into account the type of audit evidence/information to be gathered, its use as audit evidence/ information to meet the audit objectives and its varying levels of reliability.

4.26.8.1 Various Types of Audit Evidence/Information

The various types of audit evidence/information, which the IS auditor should consider using include as under:

a) Observed processes and existence of physical items

b) Documentary audit evidence/information

c) Representations

d) Analysis

4.26.8.2 Observed Processes

Observed processes and existence of physical items can include observations of activities, property and functions of the information systems such as:

a) Inventory of media in an offsite storage location

b) Computer room security system in operation

4.26.8.3 Documentary Audit Evident /Information

Documentary audit evidence/information, recorded on paper or other media, can include:

a) Results of data extractions

b) Records of transactions

c) Program listings

d) Invoices

e) Activity and control logs

f) System development documentation

4.26.8.4 Representations

Representations of those being audited can be audit evidence/information such as:

- ✓ Written policies and procedures
- ✓ System flowcharts
- ✓ Written or oral statements

4.26.8.5 Results of Analysis as Audit Evidence/Information

The results of analysing information through comparisons, simulations, calculations and reasoning can also be used as audit evidence/information. Examples include:

a) Benchmarking IS performance against other banks or previous periods.

b) Comparison of error rates between the application transactions and the users.

4.26.8.6 Availability of Audit Evidence/Information:

The IS auditor should consider the time during which the evidence/information exists or is available in determining the nature, timing and extent of Substantive Testing and if applicable, Compliance Testing. For example, the audit evidence/ information processed by Electronic Data Interchange (EDI), Document Image Processing (DIP) and dynamic systems such as spreadsheets etc. may not be retrievable after a specified period of time, if changes to the files are not controlled or the files are not backed up.

4.26.8.7 Selection of Audit Evidence/Information:

The IS auditor should plan to use the best audit evidence/information attainable, consistent with the importance of the audit objective and the time and effort involved in obtaining the audit evidence/information. Where the audit evidence/ information, obtained in the form of oral representations, is critical to the audit opinion or conclusion, the IS auditor should consider obtaining documentary confirmation of the representations, either on paper or on other media.

4.26.8.8 Nature of Audit Evidence/Information:

Audit evidence/information should be sufficient, reliable, relevant and useful in order to form an opinion or support the IS auditor's findings and conclusions. If in the IS auditor's judgement, the audit evidence/information obtained does not meet these criteria, the IS auditor should obtain additional audit evidence/ information. For example, a program listing may not be adequate audit evidence/ information until other audit evidence/information has been gathered to verify that it represents the actual program used in the production process.

4.26.8.9 Gathering Audit Evidence/Information:

Procedures used to gather audit evidence/information vary depending on the information systems being audited. The IS auditor should select the most appropriate procedure for the audit objective. The following procedures should be considered:

- ✓ Inquiry
- ✓ Observation

- ✓ Inspection
- ✓ Confirmation
- ✓ Re-performance
- ✓ Monitoring

4.26.8.10 Audit Documentation:

Audit evidence/information gathered by the IS auditor should be appropriately documented and organized to support the IS auditor's findings and conclusions.

4.26.8.11 Restriction of Scope:

Under those situations, where the IS auditor believes that sufficient audit evidence/information cannot be obtained, the IS auditor should disclose this fact in a manner, consistent with the communication of the audit results.

4.26.9 Audit Documentation

Sufficient, Reliable, Relevant and Useful Evidence/Information

During the course of IS auditing, the Information Systems Auditor has to obtain sufficient, reliable, relevant and useful evidence/information to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence/information. The Information Systems Auditor will require to provide a report, in an appropriate form, to the designated authority upon the completion of the audit work. Further, the audit report should, among others, state the scope, objectives, period of coverage and the nature and extent of the audit work performed. In addition, the report should also identify the bank, the designated recipients in the bank and restrictions, if any, on the circulation of the audit report. The report should state, among others, the findings, conclusions and the recommendations of the IS auditor including the reservations or qualifications, if any, which the IS auditor has with respect to the audit. The IS auditor will require to prepare and retain documentation to support the audit work performed. The IS auditor will require to apply internationally accepted IS auditing standards to the performance of the IS audit

work, use professional judgement in the application of such standards and should be prepared to justify departure/deviation, if any, therefrom.

4.26.9.1 IS Audit Documentation: Findings & Suggestions

The Information systems audit documentation is the record of the audit work performed and the audit evidence/information supporting the IS auditor's findings and conclusions. The IS audit documentation should:

a) demonstrate the extent up to which the IS auditor has complied with the IS auditing Standards.
b) assist in the planning, performance, and review of audits.
c) facilitate third-party reviews.
d) assist in the evaluation of the quality assurance programme relating to the IS auditing functions.
e) support matters relating to insurance claims, fraud cases and lawsuits; and
f) assist in the professional development of the staff.

4.26.9.2 IS Audit Contents

The IS audit documentation should, among others, include, a record of:

a) the planning and preparation of the audit scope and objectives.
b) the audit program.
c) the audit steps performed, and audit evidence/information gathered.
d) the audit findings, conclusions, and recommendations.
e) any report issued as a result of the audit work; and
f) Supervisory review

4.26.9.3 Extent of IS Auditor's Documentation

The extent of the IS auditor's documentation will depend on the needs for a particular audit and should, among others, include such things as:

a) the IS auditor's understanding of the area to be audited and its environment;
b) the IS auditor's understanding of the information processing systems and the internal

control environment;

c) the author and source of the audit documentation and the date of its completion;

d) the audit evidence/information and the source of the audit documentation and the date of completion; and

e) the auditee's response to recommendations.

4.26.9.4 Audit Information required by Law/Govt. Entities

Documentation should include audit information that is required by law, by government regulations and by applicable professional standards. The documentation should be clear, complete and understandable by a reviewer.

4.26.9.5 Appropriate Custody and Retention of Documentation

Policies and procedures should be in place to ensure appropriate custody and retention of the documentation that supports audit findings and conclusions for a period of time, sufficient to satisfy legal, professional and organizational requirements of the bank.

4.26.9.6 Safe Keeping of Documentation

Documentation should be organized, stored and secured in a manner appropriate for the media on which it is retained and should continue to be retrievable for a period of time, sufficient to satisfy the above policies and procedures.

4.27 VPN Access and Remote Working Policy

4.27.1 Introduction

Coronavirus Pandemic has forced many to work from home. Working remotely allows increased flexibility and autonomy for employees. To keep continue the banking operations and to provide better customer service and specially back-office activities, the employees need to access the incidents servers through IPsec tunnel or client-based SSL VPN

4.27.2 Scope

The purpose of the policy is to provide guidelines to necessary authorities while working remotely to access internal servers hosted at The Bihar State Co-operative Bank hereinafter called "BSCB" through Internet over IPsec or SSL.

4.27.3 Responsibility

The user, site I server I network administrator and BSCB coordinator shall follow the policy:

a. VPN connection is provided to user online registration available in www.BSCB.in. Dully filled form has to be verified by DGM (HRMD) IT reporting officers of the concerned department and forwarded through BSCB coordinator to VPN services division/Administrator.
b. VPN connection Is provided to authorize users from Department concerned/authorized service providers of BSCB Head Office/ branches decided by HRMD Department / Top Management of Bank
c. The concept of trust chain is the central theme. Trust chain consists of the users (applying for VPN), her/his Head of Department (HOD) / Reporting Officer (RO),BSCB Coordinator for the respective department and VPN Team/ Administrator.
d. Server access requirement for the user shall be checked by HOD/ Reporting Officer(RO) as well as BSCB VPN Coordinator with proper request and justification.

4.27.4 Operating Guidelines

4.27.4.1 Operating Guidelines for Remote Working Policy

- Employees availing remote working option should be present at base location during working hours. Any exception in this regard should be reported by the employee to their department head/ manager in advance preferably in writing through email.
- Employees should submit their reports of jobs carried out remotely in precision to the department head/manager after the job is done.
- Employees should choose an optimum location for a workspace at home / remote working environment. It is important that the employee is free of distraction and has adequate space, ease of access, robust data security, uninterrupted Power Supply, High speed stable internet connection.
- Employees must maintain compliance with the applicable lews and regulations pertaining to Insider trading and data protection. Use only BSCB-approved secured tools and technologies and maintain strict confidentiality regarding customer information and data, including UPSI (Unpublished price sensitive information).
- Not trade any securities issued by a customer during their Involvement in the customer engagement and for a minimum of six months or an applicable period after the involvement
- Keeping values at core and giving importance to client service as well as own wellbeing few things to be kept in mind:
  - Maintain a healthy work life balance.

- Stay connected and build relationship.
- Be collaborative and help each other.
- Respect Schedule and be flexible.
- Disturbances may be normal however its better to choose a comparatively quiet place.
- Dress appropriately.
- Maintain Quality as quality is the key

4.27.4.2 Operating Guidelines for VPN Policy

- VPN connection is provided for accessing the servers hosted in BSCB managed data centre for remote administration services and application access.
- The verification of the users shall be done by the authorized representative from the department concerned.
- The user shall apply his/her HOD / Reporting Officer(RO), BSCB Coordinator for the respective department and the VPN Team / Administrator.
- VPN Log Request as per BSCB log policy. Sharing of log request will be from controlling officer/ BSCB VPN coordinator with proper request and justification.
- VPN account issued for one year and if VPN needed for less than one year then user should clearly write the date till It Is needed and renewal or existing VPN can be done as per process of VPN renewal.
- The BSCB coordinator has to inform the VPN service provider to disable/ suspend the VPN account when the user leaves the organization before terms or transferred to a department I branch where he I she does require VPN service.

- Once VPN connected, all traffic between the user's PC I Laptop and VPN scrvwill be through VPN tunnel and user will have access to the servers listed in the- application form.
- In case of specific requirement, simultaneous access to other BSCB sites can be provided on approval of competent authority. No internet access will be allowed after connection of VPN.
- Users need to make sure that the client system used for VPN connection is regularly scanned and updated with latest patches and antivirus software.
- Any issues reported through BSCB Service desk / Official email only. The users need to raise issue through official email and VPN Support / Administrator will call the users on the contact number of the users. All software procedures and manuals are available with VPN support / Administrator.
- BSCB will not be responsible for any activities done in the server/ site even if the connection is established through remote VPN. The VPN administrator should take necessary precaution to secure their application /server.

4.28 IT Security Policy

4.28.1 Policy Statement

The primary objective of this Information Systems Security guidelines for The Bihar State Co-operative Bank Ltd. is to establish a comprehensive and robust framework designed to achieve several key goals. These include, but are not limited to, the protection of sensitive financial data, the unequivocal adherence to all relevant regulatory mandates, and the systematic mitigation of potential security risks. By adhering to these security guidelines, the bank endeavors to ensure the safeguarding of critical customer information, enhance and maintain client trust and confidence, minimize exposure to financial losses and reputational damage, and cultivate a culture of security awareness throughout the organization. Furthermore, these guidelines aim to provide the institution with the flexibility required to adapt to emerging security threats, thereby increasing operational efficiency, and affirm the bank's unwavering commitment to fulfilling its fiduciary duties in safeguarding assets and interests.

4.28.2 Objective Purpose

The purpose of this policy is to create the environment for protection of sensitive financial data, the unequivocal adherence to all relevant regulatory mandates, and the systematic mitigation of potential security risks

4.28.3 Scope

This document encompasses the strategic, operational, and technical measures necessary to protect the confidentiality, integrity and availability of sensitive financial data and the information systems that manage it. They provide a structured framework for regulatory compliance, risk mitigation, and the establishment of a security-conscious culture within the organization. The guidelines are intended to guide all personnel, contractors, and third parties associated with the bank in adhering to the highest standards of information security while adapting to evolving threats and preserving the bank's reputation and financial stability. The scope of these guidelines extends to all systems, processes, and practices that influence information security and business continuity. This document applies to all employees,

contractors, vendors, and third-party entities who have access to Bihar State Cooperative Bank's information assets and systems.

4.28.4 Information Classification

4.28.4.1 BSCB classifies information assets into different categories based on sensitivity and criticality. The classification levels are defined as follows:

a) Public: Information intended for public release, such as marketing materials and general product information.
b) Internal: Information for internal use only, including internal communications and non-sensitive operational data.
c) Confidential: Sensitive information that requires restricted access, such as customer personal data, financial records, and proprietary business information.

Highly Confidential: Highly sensitive data that requires the highest level of protection, such as encryption keys, critical infrastructure details, and top-level strategic plans.

4.28.4.2 Define appropriate access controls and handling procedures for each information classification level.

- Public Information:
  1. Access: Public information may be accessible to all employees and authorized public channels.
  2. Handling: Employees should exercise caution while disclosing public information to external parties and ensure it aligns with the bank's communication guidelines.
- Internal Information:
  1. Access: Internal information is restricted to employees and authorized personnel on a need-to-know basis.
  2. Handling: Internal information should not be shared outside the bank, and employees should be cautious about internal communication to avoid data leaks.
- Confidential Information:
  1. Access: Access to confidential information is granted only to employees with a legitimate business need.
  2. Handling: Confidential information should not be shared with unauthorized individuals or communicated through unsecured channels.
- Highly Confidential Information:
  1. Access: Access to highly confidential information is limited to a select group of authorized personnel.
  2. Handling: Highly confidential information should be strictly protected and accessed only when necessary for critical business operations.

4.28.5 Access Control

4.28.5.1 BSCB implements role-based access controls to grant privileges to authorized personnel based on their job responsibilities.

- Responsibilities of the IT department:
  a) Define user roles and access rights based on job roles and responsibilities, and regularly review them for accuracy and relevance.
  b) Establish procedures to manage access requests, approvals, and revocations efficiently.
  c) Implement a strong identity and access management (IAM) system to enforce role-based access controls.

4.28.5.2 Regularly review and update access rights based on changes in job roles or employment status.

- The HR department should promptly notify the IT department of any changes in employee status, including promotions, transfers, and terminations.
- The IT department should conduct periodic access reviews to ensure that access rights are appropriate and up to date.

4.28.6 Data Protection

4.28.6.1 BSCB employs encryption mechanisms to protect sensitive data at rest and in transit.

- Sensitive data, including customer information, financial data, and personally identifiable information (PII), must be encrypted using approved encryption algorithms (e.g., AES-256).
- Encryption keys should be securely managed and protected from unauthorized access.

4.28.6.2 Data masking techniques are used to protect sensitive data in non-production environments.

- Non-production environments (e.g., development and testing) should use masked or anonymized data to minimize the risk of exposure of real customer information.

4.28.6.3 Regular data backups are performed, and data restoration procedures are periodically tested to ensure data recoverability in case of data loss or disaster.

- The IT department is responsible for regular data backups, and the backups should be securely stored at an off-site location.
- Data restoration tests should be conducted to verify the effectiveness of the backup and recovery process.

4.28.6.4 BSCB employs encryption mechanisms to protect sensitive data at rest and in transit.

- Sensitive data, including customer information, financial data, and personally identifiable information (PII), must be encrypted using approved encryption algorithms (e.g., AES-256).
- Encryption keys should be securely managed and protected from unauthorized access.

4.28.6.5 Data masking techniques are used to protect sensitive data in non-production environments.

- Non-production environments (e.g., development and testing) should use masked or anonymized data to minimize the risk of exposure of real customer information.

4.28.6.6 Regular data backups are performed, and data restoration procedures are periodically tested to ensure data recoverability in case of data loss or disaster.

- The IT department is responsible for regular data backups, and the backups should be securely stored at an off-site location.
- Data restoration tests should be conducted to verify the effectiveness of the backup and recovery process.

4.28.7 Password Management

4.28.7.1 BSCB enforces strong password policies for user accounts.

- Password complexity requirements:
  - Passwords must meet specified complexity rules, such as minimum length, a combination of uppercase and lowercase letters, numbers, and special characters.
  - Use of a unique password for each account or system to prevent a domino effect if one is compromised.
- Password expiration:
  - Regular change of password especially for critical accounts.
  - Implementation of a password change policy that specifies the interval (eg. Every 90 days)

- Password reuse policy: Employees should not reuse the same password for multiple accounts.
- Password recovery: Use of secure ways to recover passwords such as security questions or email confirmation.

4.28.7.2 Multi-factor authentication (MFA) is implemented for accessing critical systems and privileged accounts.

- MFA should be required for accessing sensitive data, critical systems, and administrative accounts to add an extra layer of security.

4.28.7.3 BSCB enforces strong password policies for user accounts.

- Password complexity requirements:
  - Passwords must meet specified complexity rules, such as minimum length, a combination of uppercase and lowercase letters, numbers, and special characters.
  - Use of a unique password for each account or system to prevent a domino effect if one is compromised.
- Password expiration:
  - Regular change of password especially for critical accounts.

- Implementation of a password change policy that specifies the interval (eg. Every 90 days)

- Password reuse policy: Employees should not reuse the same password for multiple accounts.
- Password recovery: Use of secure ways to recover passwords such as security questions or email confirmation.

4.28.7.4 Multi-factor authentication (MFA) is implemented for accessing critical systems and privileged accounts.

- MFA should be required for accessing sensitive data, critical systems, and administrative accounts to add an extra layer of security.

4.28.8 Network Security

4.28.8.1 BSCB secures the network infrastructure using firewalls, intrusion detection/prevention systems, and regular security updates.

- Firewalls are implemented to control inbound and outbound network traffic and prevent unauthorized access.
- Intrusion detection/prevention systems monitor network activity and detect and block suspicious or malicious behavior.
- Regular security updates and patches should be applied to network devices and systems to address known vulnerabilities.
- Bank should carry forward IS Policy Audit, Vulnerability Assessment, Simulate attack conditions, Mitigation of the top risks, Check for the residual risks if any and compare with the Bank's risk appetite

4.28.8.2 Network segmentation is employed to isolate critical systems and limit the potential impact of a security breach.

- Network segments should be established to segregate sensitive systems from less critical areas, reducing the risk of lateral movement by attackers.

4.28.9 Physical Security

4.28.9.1 BSCB implements physical access controls to restricted areas, server rooms, and data centers.

- Access to critical areas, such as data centers and server rooms, should be restricted to authorized personnel only.
- Physical access controls may include biometric authentication, access cards, and surveillance systems.

4.28.9.2 Surveillance cameras and security alarms are deployed in critical areas to monitor and respond to security incidents.

- Surveillance cameras should provide adequate coverage of areas where sensitive data and equipment are located.
- Security alarms should be monitored 24/7 to detect unauthorized access or suspicious activities.

4.28.10 Incident Response

4.28.10.1 BSCB has established an incident response team to handle security incidents promptly and effectively.

- The incident response team is responsible for identifying, assessing, mitigating, and resolving security incidents.
- Incident response procedures should be documented in the Incident Response Plan (IRP).

4.28.10.2 An Incident Response Plan (IRP) outlines the procedures for reporting, managing, and communicating security incidents.

- The IRP should define roles and responsibilities during incidents and the communication process with internal and external stakeholders.
- Employees should be trained on the IRP to ensure a coordinated and efficient response to security incidents.

4.28.11 Security Awareness Training

BSCB conducts regular security awareness training for all employees.

- Training topics include phishing awareness, data protection, physical security, and incident reporting procedures.
- Security awareness training helps employees recognize and respond to potential security threats effectively.

4.28.12 Vendor Management

4.28.12.1 BSCB assesses the security posture of vendors and third-party entities before engaging their services.

- Vendor assessments should evaluate their information security practices, including data protection, access controls, and incident response capabilities.
- Due diligence should be conducted to ensure that vendors comply with industry standards and regulatory requirements.

4.28.12.2 BSCB assesses the security posture of vendors and third-party entities before engaging their services.

- Vendor assessments should evaluate their information security practices, including data protection, access controls, and incident response capabilities.
- Due diligence should be conducted to ensure that vendors comply with industry standards and regulatory requirements.

4.28.12.3 Security requirements are included in vendor contracts, and regular reviews ensure their compliance with security standards.

- Contracts with vendors should include clauses related to data protection, confidentiality, and incident reporting requirements.
- Regular reviews and audits should be performed to verify vendor compliance with contractual security obligations.

4.28.13 Compliances and Auditing

4.28.13.1 BSCB conducts regular internal security audits to assess compliance with

information security policies and procedures.

- Security audits evaluate the effectiveness of security controls and identify potential gaps or weaknesses.
- The audit results should be used to improve the bank's information security practices.

4.28.13.2 BSCB ensures compliance with all relevant regulatory requirements related to information security, including ISO 27001, PSI-DSS framework, RBI cybersecurity framework.

The bank should maintain a comprehensive understanding of information security regulations and requirements relevant to its operations

4.28.14 Review and Updates

This SOP shall be reviewed annually by the Information Security Team to ensure its relevance and effectiveness.

- The review process should include input from relevant stakeholders, including compliance, legal, and IT departments.
- The SOP will be updated promptly whenever there are significant changes to the bank's information security practices or regulatory requirements.

4.28.15 Document Control

All versions of this SOP will be properly controlled and maintained by [mention the department responsible for document control].

- A designated individual or department should manage the distribution and version control of the SOP.

4.28.16 Training and Awareness

All relevant personnel shall be trained on this SOP to understand their roles in implementing the bank's information security practices.

- The training should be conducted as part of the onboarding process for new employees and as a periodic refresher for existing employees.

Internet Usage

**********End of Policy**********