The Bihar State Co-operative Bank Ltd.

Ashok Rajpath, Patna – 800 004

Information Technology Policy

This document summarises of Information Technology Policy of The Bihar State Co-operative Bank Ltd. This is not a static document, it is subjected to periodic review and alteration, as required to accommodate changes in the Information Technology Systems of the Bank or in the Banking Industry /Statutory Authorities.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

Foreword→

Today's banking operations heavily depend on the use of Information Technology. Obviously, The Bihar State Co-operative Bank Ltd. is not any exception, almost all the operations of the Bank are computerized and the Bank has adopted industry standard Information Technology solutions such as Core Banking Solution (CBS), ATM/Debit Card Solution, Payment and Settlement Systems such as National Electronic Fund Transfer (NEFT), Real Time Gross Settlement (RTGS), Cheque Truncation System (CTS), National Automated Clearing House (NACH) operations, etc.

Other solutions include Email Solutions, Website, Payroll Application, ATM Reconciliation support, Old Banking Database, BAT Web Application, BCS _ Rupay Web Application, DMS Web Application, CCTV surveillance, etc.

Some of the IT operations of the Bank are outsourced. Bank has Annual Maintenance Contract (AMC) with IT vendors for maintenance of IT resources. New purchases and updation of existing resources are on-going activities of the Bank.

It is clear from the above facts, why we need to have a clearly defined Information Technology Policy for the Bank.

The bank needs to have IT-related strategy and policies that covers areas such as:

- Existing and proposed hardware and networking architecture for a bank and its rationale.
- Broad strategy for procurement of hardware and software solutions, vendor management.
- Standards for hardware or software prescribed by the proposed architecture.
- Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development
- IT Department's Organizational Structure.
- Desired number and level of IT expertise or competencies in bank's human resources, plan to bridge the gap (if any) and requirements relating to training and development.
- Strategy for keeping abreast with technology developments and update systems as and when required

Bank wishes to establish and maintain an enterprise architecture framework or enterprise information model to enable applications development and decision-supporting activities, consistent with IT strategy. Our aim is to facilitate optimal creation, use and sharing of information in a way that it maintains integrity, and is flexible, functional, cost-effective, timely, secure and resilient to failure.

We need to establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, or top secret) of enterprise data. This scheme includes details of data ownership, definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements (criticality and

sensitivity). It should be used as a basis for applying controls such as access controls, archiving or encryption. Banks also need to define and implement procedures to ensure integrity and consistency of data stored in electronic form.

Among executives, the responsibility of Senior executive in charge of IT operations is to ensure implementation from policy to operational level involving IT strategy, value delivery, risk management and IT resource and performance management.

Bank-wide risk management policy or operational risk management policy needs to be incorporated as IT-related risks also. The Risk Management Committee should periodically review and update the same (at least annually). The IT risk function needs to be integrated into the operational risk management function.

Finally, there needs to be an annual review of IT strategy and policies taking into account the changes to the organization's business plans and IT environment.

Date:

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

Managing Director

The Bihar Co-Operative Bank Ltd.

Chapter1:

POLICY ON SECURITY OF COMPUTER HARDWARE AND OTHER RELATED ASSETS

1. Introduction

Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, spilled tea, etc.). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Physical security is a vital part of any security plan and is fundamental to all security efforts. Without proper physical security, information security, software security, user access security, and network security, etc. are considerably more difficult, if not impossible, to initiate.

2. Secure Environment

- Costly and very sensitive IT equipment such as Server, Switch, Router etc. should be kept in a secured room.
- A secured room should have one or two doors- they should be solid, fireproof, lockable, and observable by assigned security staff.
- A secure room should not have excessively large windows. All windows should have Locks
- Keys of the secure room should be kept by appropriate authority responsively. If there is a breach, each compromised lock should be changed.
- Preparedness for fire emergencies: A secure room should be protected from fire by an effective fire-fighting system. Note that, water can damage electronic equipment, so carbon dioxide systems or halogen agents are recommended. If implemented, staff must be trained to use gas masks and other protective equipment.
- Maintenance of a reasonable climate within the room: Room temperature and humidity cannot be allowed to reach extremes.
- Eating, drinking and smoking in a secured room are strictly prohibited. Other non-essential materials such as curtains, reams of paper, and other flammables should not be kept in a secure room.

3. Guarding Equipment

- Keep critical systems separate from general systems
- On its criticality and its role in processing sensitive information and the equipment shall be stored it in secured areas based on those priorities.
- House computer equipment wisely: Equipment should not be able to be seen or reached from window and door openings, nor should it be housed near radiators, heating vents, air conditioners, or other duct work. Personal Computers or workstations that do not routinely display sensitive information should always be stored in open, visible spaces to prevent covert use.
- Protect cabling, plugs, and other wires from foot traffic: Tripping over loose wire sis dangerous to both personnel and equipment. Network cables shall be in concealed wiring from.

- Maintenance of Inventory of Equipment: The Information Technology department should maintain up-to-date logs of equipment manufacturers, models, and serial numbers in a secure location. The logs should include a list of all attached peripheral equipment also.

- Repair and Maintenance of Equipment: Bank should have plans in place for emergency repair of critical equipment. Either have a technician who is trained to do repair works or make an arrangement for Annual Maintenance Contract for maintenance of critical equipment.

- Technical support telephone numbers, maintenance contract numbers, vendor identification numbers, equipment serial numbers, and mail-in information should be posted or kept in a log book near the system for easy reference. Remember that computer repair technicians may be in a position to access your confidential information, so make sure that they know and follow your policies regarding outside employees and contractors who access your system.

- Office premises should be clearly demarcated for visitors or customers and staff. Customers or visitors are not allowed to enter the secure places such as server room, cubicles, tables of computer operators, staff, electrical equipment room, etc.

- Maintenances of important spares for quick replacement for the same.

4. Protection against Theft

- Mark the equipment in an obvious, permanent, and easily identifiable way or label the inside of equipment with the organization's name and contact information to serve as powerful evidence of ownership.

- Users should keep their laptop, mobile phone or any other portable devices that contain sensitive information of the Bank with them all times, especially if they are travelling or staying at a hotel.

- Limit and monitor access to equipment areas: Keep an up-to-date list of personnel authorized to access sensitive areas. Never allow equipment to be moved or serviced unless the task is pre-authorized and the service personnel can produce an authentic work order and verify who they are.

Chapter 2:

POLICY ON LOGICAL ACCESS CONTROL OF INFORMATION SYSTEMS

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

1. INTRODUCTION

Logical access to an organisation's information resources needs to be managed in a controlled manner and logical access permissions should be granted on the basis of business requirements. Lack of adequate logical access controls could lead to unauthorised access to information and information resources. The Management of The Bihar State Cooperative Bank Ltd has recognised this pertinent threat and have, therefore, formulated this Logical Access Control Policy in order to address the risks attached to this threat.

2. SUPPORTING CLAUSES

2.1 Scope This policy covers logical access to data networks, servers, and personal computers

(standalone or network-enabled) located at different locations, where these systems are under the jurisdiction and/or ownership of THE BIHAR STATE COOPERATIVE BANK Ltd., and any personal computers and/or servers authorised to access THE BIHAR STATE COOPERATIVE BANK 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.

This document focuses on THE BIHAR STATE COOPERATIVE BANK Ltd.'s corporate standard 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 Centres, Disaster Recovery Centres, Training Centres, etc.

2.2 Purpose The purpose of this policy is to ensure that logical access to information resources is controlled and managed based on business requirements. THE BIHAR STATE COOPERATIVE BANK 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 so as 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.

2.3 Applicability: This policy applies to THE BIHAR STATE COOPERATIVE BANK Ltd., its departments, regional offices, branches, data centres, DR centres, training centres, and their employees, including temporary staff, consultants, third parties and service providers making use of THE BIHAR STATE COOPERATIVE BANK Ltd.'s information resources.

3. Standard- Request Logical Access

3.1 General

- ➢ The official Access Request forms applicable to the office or department shall be completed whenever access to any information resources within THE BIHAR STATE COOPERATIVE BANK Ltd. is granted.
- ➢ The Access Request form shall, as a minimum, gather the following information from the user:

•Full Name

•Employee Identification Number

•Physical Location

•System / Application

•Authorisation

•Reference Number

- The business requirements for the authorisation 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 authorise 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 authorising parties shall indicate on the Access Request Form the duration for 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 for 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. An email from the registered branch mail can be sent with afore-stated details for change in access to the system.

3.2. Supporting Documentation

- A System Authorisation 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 authorise access to the system.

  •Level of access rights the person may authorise access for.

- Each branch shall create and maintain an access control matrix, ensuring that proper segregation of duties is established, in order 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 in order for the user to perform the work.
  - Segregation of duties requirements and Duration the access may be granted for.
  - Password protection procedure.

3.3. GRANT LOGICAL ACCESS

3.3.1 Granting access to a user is one of the most important activities performed on a daily basis within the organisation as this enables the user to perform his/her role in the organisation. 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:

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

- Access shall only be granted upon receipt of an official request via registered email and the original authorised 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 authorisation 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 organisation.
- Access shall be granted for the requisite/order time period needed to perform the user's specific role in the organisation.

3.3.2. User ID Management

a. All logical access administrators shall consistently observe the user ID naming standards, except where the Chief Executive Officer (CEO) has given explicit permission to use a different naming convention.
b. The use of a shared user ID for a group of users for individual user shall not be allowed.
c. No duplicate user IDs shall be allowed.
d. After resignation or contract expiry the user ID shall be immediately suspended from the system. Users shall not be allowed to have multiple sessions on the same system, unless appropriately authorized.
e. 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 IDs 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 IDs are used, and if not used, they shall be disabled. Monthly checks shall be performed to verify any attempts to access unauthorised information with anonymous and/or guest user IDs.
    - Guest ID only for viewing unless otherwise stated by appropriate authority.
f. 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.
g. During the log-on process information messages shall not convey information such as incorrect password or username. This will minimise the potential for access breaches, conveying information to potential intruders. 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.

3.3.3. User Responsibility

a. Users shall be held responsible for all activities performed with their personal user IDs.
b. User IDs shall not be utilised 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 unauthorised 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.
i. Whenever there is an indication of possible password compromise, the user shall:
    - Change the password.
    - Report the incident through the Incident Management System.

3.3.4. Minimum Password

a. User passwords shall be a minimum of eight (8) characters, recommended more characters, in length and consist of letters, numbers and special characters.
b. Password strength verification shall be performed by the various systems, that the user has access to, when logging onto the specific system (e.g., Core Banking System, TBA System, NEFT, RTGS, CTS, NACH, Email Solution, Bank's Website, etc.). Strength verification on password shall test that the password is adhering to the minimum length, as defined for the specific system or application and is not weak, e.g., 123456 as password.
c. Users shall be forced to change their passwords every thirty (30) days or as per the specific system.
d. As a minimum the previous four (4) passwords shall be recorded to prevent re-utilisation or as per the specific system.
e. Passwords shall at all times be entered in non-display fields.
f. Passwords shall be encrypted when transmitted over any network and when in storage or as per the specific system.
g. The exception to this is when scripts are used to perform various functions that contain passwords that are needed to perform the function. In this case the script shall be stored safely and securely by the person who is responsible for the.
h. Passwords shall not:
    - Be easily associated with THE BIHAR STATE COOPERATIVE BANK Ltd. or the user, i.e., identification number, employee number, address, date of birth, numerical equivalent of the user's name.
    - Contain words from a dictionary, movie or geographical location.
    - Be based upon month/year combinations such as "jan03" or "april2002".
    - Be cyclical passwords. For example, users cannot add a numeric at the end of the password in sequence.

3.4. Guidelines on Creating a Good Quality Password

a. String several words together also known as a pass phrase, e.g., the red car-there car.
b. Shift a word up, down, left or right one row on the keyboard, e.g., widepool-ajxslkkm.
c. Bump characters in a word for a certain number of letters up or down the alphabet, e.g., browndog -cspxoeph.
d. Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word, e.g. school -s2h4o6
e. Combine punctuation or numbers with a regular word, e.g., 2cool4school.

f. Create acronyms from words in a song, a poem, or another known sequence ofwords, e.g., ba-ba black sheep have you any wool - bbbshyaw.
g. Deliberately misspell a word but do not use a common misspelling, e.g. -Mississippi - misisipii.

3.5. RESETTING AND ISSUING PASSWORDS

3.5.1. Resetting Passwords

a. A formal request shall be submitted whenever a user needs to have his/her password reset.
b. Passwords shall only be reset upon positive identification of the user.
c. All users requesting password resetting shall be positively identified. The verification of the identity of a user shall be done by confirming the unique number and immediate manager's employee number and randomly confirming with the user at least two of the following:
- Branch or office code.
- Telephone number.
- Fax number.
- Cell phone number.
- Location / address / site.

d. If a user cannot be positively identified (as mentioned above) then the password shall not be reset and the user shall have to provide physical identification and written consent of password reset from his/her manager or appropriate authority.

3.5.2. Generating Passwords

The logical access administrators shall generate passwords in line with the guidelines on creating a good quality password for users or as per the specific system.

3.5.3. Issuing Passwords

a. The communication of the reset password shall be done in a secure manner to ensure that only the user receives the password or instruction from the administrator to immediate change the default password set by the specific system.
b. To the extent feasible, users shall be forced by the system they are accessing to change their initial password on initial reset, to one that meets the relevant password standards or as per the specific system.
c. Users shall ensure that the password assigned to them is changed after first login, before the end of the working day or as per the specific system.
d. To the extent feasible, systems shall be configured to suspend accounts of users who have not changed their initial password by the end of the working day or as per the specific system.

3.6. MONITORING AND REVIEWING LOGICAL ACCESS

3.6.1. Monitoring Areas

a. The following areas shall be monitored depending on:
- Authorised access
- User ID.
- Date and time of key events.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

- 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 authorised access rights.
- The actual access rights and the needed access right seven though actual access rights have been authorised.
- Logical access rights shall be changed based on the review of the access rights.

3.6.2. 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 THE BIHAR STATE COOPERATIVE BANK Ltd.'s information is appropriate and still required.

3.6.3. 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 head office.
b. All unauthorised access rights shall immediately be revoked.

3.7. MAINTAINING LOGICAL ACCESS

3.7.1. Dormant Logical Access

a. Accounts not used for an extended period of time demonstrate that no access to information on that system is needed.
b. Logical access administrators shall generate reports on accounts dormant for 30 days.
c. These reports shall be sent to the Head Office to determine the validity of the dormant accounts.
d. The Logical access administrator shall inform the user and his/her line manager

about the dormant account via an e-mail message.

e. The system department or Regional Manager / Branch Manager shall inform the logical access administrators whether the accounts need to be removed, disabled or left as is.
f. The logical access administrator shall enter a reason in the description field if an account is disabled.
g. A valid reason shall be entered in the description field for dormant account that should not be disabled e.g., user on maternity leave, privilege leave, medical leave, training, etc.

3.7.2. Updating Logical Access Information

a. Human Resources Department/Establishment Section shall inform the Information Technology Department of organisational changes, e.g., structural changes, appointments, moves and resignations impacting access lists.
b. 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.

3.7.3. 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 BIHAR STATE COOPERATIVE BANK 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 BIHAR STATE COOPERATIVE BANK Ltd. Information Security Manager when:
   - The user leaves the employment of THE BIHAR STATE COOPERATIVE BANK Ltd.
   - The user's 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 BIHAR STATE COOPERATIVE BANK 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 minimise the risk of dormant access permissions being inherited by a new user.

3.8. SECURITY CONTROLS

3.8.1. Automatic Lockout

a. 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.

3.8.2. Automatic Time-outs

a. 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
b. Users shall not attempt to circumvent automatic time-out controls, by implementing measures such as pinging the server to maintain connection.

3.8.3. Privileged access

a. The number of privileged user IDs shall be strictly limited to those individuals who require such privileges for authorised business purposes. A screening process shall be performed by THE BIHAR STATE COOPERATIVE BANK 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 for Disaster Recovery purposes.

3.9. CRITICAL SYSTEMS

a. A list of THE BIHAR STATE COOPERATIVE BANK 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 BIHAR STATE COOPERATIVE BANK Ltd. Critical Systems list. These audit trails shall, as a minimum, include the following information:
   - User IDs that logged in or attempted to log in.
   - 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 BIHAR STATE COOPERATIVE BANK Ltd.
d. Audit logs shall be secure and only authorised persons shall gain access to the logs.
e. All THE BIHAR STATE COOPERATIVE BANK 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 BIHAR STATE COOPERATIVE BANK Ltd. 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 IT section 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.

3.10. LOGICAL ACCESS TO SOURCE CODE, SCRIPTS AND FILES

a. Computer operations staff and programmers shall not be given any access to production data, production programs, or the operating system beyond that which they need to perform their jobs.
b. Logical access to source code shall be controlled to ensure that no unauthorised changes to source code are made.
c. Data files and documents containing passwords shall be stored in a safe and secure manner to ensure that the passwords are protected.

Chapter 3:

POLICY ON CHANGE MANAGEMENT OF INFORMATION TECHNOLOGY SYSTEMS

1. Introduction

THE BIHAR STATE COOPERATIVE BANK Ltd. acquires its technology systems and application software from third-party technology vendors. For example, the Bank's Core Banking Solution was acquired from TCS Ltd. These systems are primarily maintained by the vendor from whom they were purchased. In most cases, THE BIHAR STATE COOPERATIVE BANK Ltd. does not have possession of source code to make changes.

The Board of Directors and management are aware, however, that

a. Vendors make periodic changes to application software used by the Bank, including comprehensive changes in the form of new releases and "fixes" of immediate problems, and
b. The Bank has the option of changing parameters, options, etc which alters the functions of specific applications. Further, the Board and management understand that either of these categories of changes may affect the effectiveness of the Bank's information security program. Consequently, any change to the Bank's systems, application programs, computer hardware and data communications hardware and software may impair the effectiveness of Bank's Information Security Program. Consequently, this Policy has been adopted to provide guidance for the management of such changes.

2. General Obligations

When software changes are required, it is essential that the changes are appropriately authorized and approved. Authorization for any software change must come from a member of the senior management, or the Information Technology Committee. The only exception to this policy is for changes made to correct errors found in existing programs or procedures, or for "patches" to existing systems or Service Packs because it may not be convenient or advisable to delay applying such changes while waiting for approval, these types of changes (these kinds of changes can be made but should be communicated to appropriate management personnel as soon as possible).

It is equally important that all software changes adhere to the following guidelines:

- Changes must not violate any other policies or procedures.
- Changes must be thoroughly tested.
- Changes must be sufficiently documented.
- Changes or appropriate documentation must be reviewed by the Bank.
- Changes must be implemented at an appropriate time to reduce or eliminate disruption of customer activity, Bank workflow, and system operations.
- Proper record of changes shall be maintained.

3. Change Control Responsibilities

The following personnel may approve software changes:

- Board Of Directors.
- Chief Executive Officer.
- Information Technology Committee.

It is the responsibility of appropriate personnel within the Information Technology Department to implement software changes. Changes must be implemented (i.e., put into production) by personnel other than those initially responsible for evaluating the effects of a change and testing the change.

4. Change Control Environment

To the degree that it is economically feasible and practical, software changes should be implemented through the utilization of three separate steps:

a. **Development—** new program releases or significant program changes are typically prepared by a third-party technology Service provider. The Bank does little actual Programming, with the exception of custom report generations. It is the responsibility of the Information Technology Department to receive and review all release letters or other appropriate documentation or a system.

b. **Testing** — once a program change or new release is received from a vendor, it must be thoroughly reviewed by the Information Technology Department and the senior management of the Bank. The purposes of this review are to determine the effects of the proposed changes on the Bank's information security systems and on the operational systems. Information Technology Department will ensure that the implementation of the new release, or program change, will not materially impair the effectiveness of the Bank's information security systems. Program changes or releases must be deployed in a test environment by Information Technology Department or the service provider personnel not involved, or permitted to access the Production environment. The changes should also be thoroughly tested by the end-user department.

c. **Production** — this is the environment in which the current, active software resides. Only after a program has completed the testing phase satisfactorily and been approved by the senior management of the Bank should it be moved to the production environment. Once the user department is satisfied with the results from the testing environment, the Software Change Control form should be completed and signed by the end-user department. The completed Software Change Request Form should be sent to the in-charge of Information Technology Department, who will then allow the program into the Production environment.

5. Core Banking Solution Software

The core banking system vendor, for example TCS Ltd may release a new version of their Core Banking Solution Software one or more times per calendar year to the Bank. Because of the potential wide-ranging impact of these software releases, the scheduling, training, and implementation of the releases is more complex than with operating system software where the changes are usually transparent to the end user. The following outlines the basic steps performed while installing a core banking solution software release.

a. Prior to distributing a new release, the vendor will conduct training classes at various locations near the Head Office, Regional Officer or Branch Offices or Training Centres, as required.
b. Upon receipt of the release documentation, it should be distributed to a release installation team made up of key Bank management and staff members, appropriate to the nature and scope of the changes being made in the release. As soon as possible after those employees have reviewed the documentation, an implementation team meeting should be held to assign implementation tasks.
c. Training is to be scheduled for any employees who might be affected by the release. Training is to be conducted by the implementation team, or someone they designate. iv. Documentation of changes should be distributed to the appropriate departments prior to the installation of the release.
d. The actual release installation must be scheduled far enough in advance so that all employees are properly notified. All employees and the vendor should be notified of the release installation date.

6. ATM Reconciliation Application, NDS-OM, CTS, NACH, Pay Roll Application, BAT (Banking Analytical Tool) Web Application, BCS_ Rupay Web Application, etc.

a. The concerned department should follow the instructions of the software or application service provider as per schedule and defined procedure without fail for smooth operation of the applications.
b. A large number of other applications are used by the Bank. The respective application software provider releases regular or occasional updates for the system that must be executed as per the schedule and procedure as directed by the software or application provider.

7. Documentation

Appropriate documentation must be provided for the following:

a. Change control procedures — the procedures for implementing software changes should be fully documented and followed.
b. Software change requests — all requests for software changes should be submitted in writing on the appropriate Software Change Request Form. The form must be approved by the appropriate personnel.

c. Technical functions — a guide for the technical functionality of the software should be maintained by the Information Technology Department.
d. Operational functions — Any operational instructions required should be available to the appropriate department.
e. End-user functions — specific instructions for using the software should be available to the appropriate department

Chapter 4:

Policy on Anti-virus

1. Introduction

Antivirus software is used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. A variety of strategies are typically employed by Antivirus software. The Bihar State Cooperative Bank Limited is increasingly being dependent upon their usage Information and Communication Technology as a key tool for doing the business of banking and other ancillary services. A major threat to the delivery of such services is malicious software (malware) which has the potential to undermine the confidentiality, integrity and availability of those services/data hosted on Bank's systems or can adversely impact the underlying infrastructure hosting these systems and thus prevent access to the resources. THE BIHAR STATE COOPERATIVE BANK Ltd. has a responsibility to ensure that appropriate technical measures are implemented to protect against malware and to ensure that appropriate controls are in place to rapidly detect, isolate and remove any instances. A single technical solution cannot be relied upon and therefore a 'layered approach' will be implemented in order to provide the best overall protection against the omnipresent threat of malware from whichever vector it may appear.

2. Purpose

This 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 minimising the risk of a malware infection(s) and what to do if one is encountered.

3. Scope

This policy applies to Information Technology resources and to all staff authorised to use/access those computer systems and communications networks whether they are employed directly by the Bank, contractual and contingent staff, suppliers or AMC Vendor granted access for support purposes. Systems developed and managed The Bihar Stately by M/s TCS or other external providers (such as AGS, V-Soft, etc.) as contracted by the Bank are outside the scope of this policy.

4. Anti-Virus Protection

All 'end points and network 'entry' points should be protected from, and provide protection to the resources they host or provide access to from malware and its effects. Generally, an AV solution will be deployed on all assets and will mediate all traffic that may be processed on that end point. In the case of 'boundaries' the point of access to the environment is to provide protection from malware to any traffic it allows into and out of the environment. For example, email and web traffic is to be

scanned for malware at the point of entry/exit to/from the environment.

5. Layered Security, Reducing the Scope for Malware

5.1. Widespread use of AV software on all Endpoints

a. Wherever possible Anti-Virus software is to be installed on all suitable endpoints including all forms of client and server regardless of whether they are networked or standalone. This will ensure that any risks of cross infection between disparate systems are minimised.
b. The aim is that there is no less than 100% coverage of Anti-Virus installed on all endpoints that capable of running the software.
c. For the servers running Anti-Virus, new updates should be installed earliest of the current release.
d. For the workstations or personal computers running Anti-Virus, new updates should be installed within 7 days of the current release.

5.2. Isolation of devices that cannot be protected by AV Software

Whenever a networked device cannot have Anti-Virus software installed such devices are to be configured to operate in a separate isolated environment. This will minimise the risks to both the 'protected' and 'unprotected' devices minimising the risk on propagation between devices.

5.3. Patch Management

a. 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. For known weaknesses vendors quickly distribute software updates/patches to prevent exploitation via that particular mechanism, 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.
b. The exact process for patch management is contained within the Patch Management Process documents but should aim to ensure that relevant devices are routinely patched with security patches (patches which have failed testing may be excluded on a host-by-host basis):
   - Servers: should be no more than 2 months behind available and tested security patches.
   - Desktops and Laptops: should be no more than 3 months behind available and tested security patches. This should apply to no less than 90% of systems on or connected to the network.
   - Networks/Other: should be no more than 2 months behind available and tested security patches.

5.4. Restricted Download Rights

No software programs or executable files are to be downloaded from the Internet and installed on devices in any branch/ office/ training centre etc. without permission from the Information Technology Department. In most cases, the IT Department will supply the relevant software by downloading software from the internet or from the backup storage.

No software or files can be downloaded from any site or any storage media illegally.

5.5. 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.

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. Detailed policy for email is framed separately (See Chapter-8).

6. Anti-virus Deployment to End Points

This policy applies to all 'supported' assets used within the Bank regardless of who manages/operates them or whether they are hosted on the 'network'. Where departments manage/operate independent standalone Information Technology systems, the requirements mentioned below still apply although they may be fulfilled differently as directed by individual Information Asset Owners. Advice and guidance in the fulfilment of any conditions contained within this policy will be provided by the Information Technology Department.

Information Technology Department should have an enterprise anti-virus strategy with the deployment of Anti-virus software throughout the computer network and on assets they support. This software constantly scans networks and machines for virus attacks whilst running in the background and is virtually transparent to the user.

In instance where the installation of Anti-Virus software adversely affects the performance of the host or the installed software, every effort should be made to find a solution other than removing the software. For example, most Anti-Virus solutions can be configured to prevent scanning of particular files/folders/processes or on access scanning can be disabled and a scheduled scan used instead (outside of working hours if necessary). Any changes are to be kept to the minimum required to address the issue(s) and not be unduly excessive in relaxation of the default configuration.

Anti-Virus software must only be installed and configured by vendor hired by the Bank or by the branch/office on their own using the media kit supplied by the Information Technology Department of the Bank whenever no service provider is in contract to do so and the users must not disable, uninstall, reconfigure or interfere with the anti-virus software installed on any computer or attempt to install alternative solutions.

Users who operate their laptops on and off the network must regularly connect to the network to ensure that the Anti-Virus software virus definitions remain up-to-date.

Soft copies of files and/or applications should be backed up on external devices approved by the Bank on regular basis. If a virus infection does occur and the Anti-Virus software cannot repair any ensuing damage, it may be possible to restore files to a clean state from the backup media.

7. Suspected Malware Outbreak

If a user observes any unusual activity leading them to suspect a malware attack, the user must:

- Inform the Information Technology department immediately.
- Switch off the machine (at the wall socket) and ensure no one else uses it.
- Gather any media, such as floppy disks, CD-ROM disc(s), USB memory stick(s) that was used for transporting information in or out of the machine and make available to Information Technology Department.
- Not use the PC (or suspected media) until it has been cleared as being safe to use.

8. 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.

Chapter 5:

POLICY ON BACKUP PROCESS AND ARCHIVAL OF DATA

1. Introduction

Today's high rate of data growth and increasing number of regulations mean that Bank should frame a proper data backup and archiving policy. Backups help recover information and processes in current use in case they are interrupted, corrupted, or lost. Archives help discover details of information and processes not in current use, in case they become useful again because of some unanticipated legal or regulatory event.

Without a comprehensive archive strategy, the potential toll on an enterprise includes rising costs, increasingly complicated backup and recovery, inefficient search/access, potential regulatory issues, and the inability to unlock the value of data in the future.

2. Purpose

a. To provide secure storage for data assets critical to the work flow of Bank.
b. To prevent loss of data in the case of accidental deletion or corruption of data, system failure, or disaster, etc.
c. To facilitate timely restoration of business operations in the event of a disaster, system failure, etc.
d. To preserve inactive information as required by law and/or Bank policy.
e. Classifying and indexing archived documents for proper data mining and retrieval.

3. Difference between Backups and Achieves

Backup and Archive should not be treated as the same thing. Backups and Archives have entirely different purposes. The purpose of backup is to restore business operations after data loss, interruption, or disaster. On the other hand, the purpose of archive is to preserve inactive information as required by law and/or Bank policy.

4. Scope

This policy applies to all computers (desktops, laptops, servers, email server, etc.) and allied devices where original business data or information resides.

5. Backup

a. Backup of Ordinary Document Files:

The users of the computer systems should backup of their files on regular basis in secondary storage mediums or in a shared folder of another computer. If secondary storage mediums are disabled in their system, the users should backup their important files in a shared folder of another networked computer. It should be noted that backups taken on the secondary mediums are the property of the Bank and the contents of the secondary storage mediums (backup device) cannot be shared with outsiders.

b. Backup of Database Dumps

Wherever there is any database-driven application and the system is installed at the Bank premises, special care should be taken so that backup of the database (dump file) is generated on a regular interval (e.g., day-end) and the backup file is copied to a secondary storage and/or a different computer without fail. Backup of the databases cannot be shared with outsiders in any circumstances except for restoration of the system by the service provider, if any.

c. Backup of Application Software or Script Files or Folders

The backup of Application Software or script files that are being use by the Bank should be kept at the appropriate location or appropriate mediums so that a failed system can be restored using these backup file. For example, server setup files for CBS application should be kept in removable media and/or on a shared folder of a networked computer so that in case of server crash or system malfunction the files can be used for system restoration.

d. Backup of Report Files or Folders

The reports that are generated by the systems such as CBS, CTS, NACH, ATM, etc. should be preserved as backup file in a secondary media and/or a shared folder on a different computer on the network, so that required reports are not lost due to system failure. Periodical backups fortnight/monthly basis of the CBS reports shall be preserved by the bank/branch level by the authorised users of the system.

6. Archival

The system generated reports of other important files that may be required in future for business, legal, statutory, or other purposes must be archived.

7. Remote Backup and Archival Location

The storage of backup or archival equipment, vital software and information shall be at a location that is distant from the original storage location, so that events such as a natural disaster, war and the like shall not simultaneously damage the original equipment, software and information and backup/archive and shall not prevent the use thereof.

8. Business Continuity (BC) and Disaster Recovery (DR)

Business continuity (BC) is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. Disaster recovery (DR) is the processes, plan, and technology

needed to recover from an unforeseen incident at a data centre, server or at any other IT resource. Backup and Archival Policy (current chapter) together with Incidence Management Policy (see chapter 6) will serve as the main policy for Business Continuity and Disaster Recovery for the Bank.

Chapter 6:
POLICY ON INCIDENT MANAGEMENT FOR I.T. SYSTEMS

1. Introduction

During the course of all businesses, there will be a time when Bank may be faced with an incident. In some cases, wrong actions taken during an incident can cause destruction of evidence, financial loss or loss of reputation.

2. Objective

The main objective of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

3. Some examples of Incidents

a. System-down (server issue, network issue, power-supply issue, etc.
b. Smoke/ Fire in the Server Room/Water-leakage for Air-conditioners of the Server Room, etc.
c. Theft of IT equipment (e.g., Antenna)
d. Unexpected behaviour of the computing devices, such as files become inaccessible, folders become hidden or inaccessible, files are encrypted and ask for password, etc.

4. Prior to Incidence

a. All the departments or offices should create a contact list which includes all law enforcement, vendor and staff contacts which one may need during an incident.
b. Backups of all the systems to be kept as per Backup and Archive Policy of the Bank. (See Chapter 5).

c) Initial Response Teams should be formed for different kind of anticipated incidents such as Fire, Flood, Cyclone, Earthquake, Server Crash, Virus / malware attack, etc.

5. Incident Occurrence

a. One should not panic, handle the situation methodically without waiting.
b. Gather all relevant information, this is the evidence about the incident.
c. Contact Police Station, Fire Station, etc. whenever required.
d. Record all relevant information include things that you observe, and actions you took. This will provide a time frame of when things occurred and how the event progress from the time the incident started.
e. Inform the relevant department or personnel about the incident immediately and follow the guidelines as dictated by the relevant department or personnel.
f. DO NOT contact the suspected perpetrator, if any.

6. Incident Management

The affected department together with the Incident Response Team should act prudently for quicker recovery of the affected system or taking appropriate legal or departmental actions.

Chapter 7:

POLICY ON INTERNET ACCESS AND ITS USAGE

1. Introduction

Internet connectivity presents the Bank with new risks that must be addressed to safeguard the Bank's vital information assets. These risks include access to the Internet by personnel that is inconsistent with business needs and results in the misuse of resources. These activities may adversely affect productivity due to time spent for browsing or surfing the Internet. Additionally, the Bank may face loss of reputation and possible legal action through other types of misuse. Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

2. Purpose

The purpose of this policy is to define the appropriate uses of the Internet by THE BIHAR STATE COOPERATIVE BANK Ltd. employees and affiliates.

3. Scope

The Internet usage Policy applies to all Internet users (individuals working for the Bank, including permanent full-time and part-time employees, contingent and contractual personnel, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

4. Allowed Internet Services

a. Internet access is to be used for business purposes only and it will be granted based on an employee's current job responsibilities. User Internet access requirements will be reviewed periodically by Bank to ensure that continuing needs exist. Capabilities for the following standard Internet services will be provided to users as needed:
   I. E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).
   II. Browsing: WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP/ HTTPS) browser tool.
   III. File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP): Send data/files and receive in-bound data/files, as necessary for business purposes.
   IV. IT technical support team downloading software upgrades and patches.

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

5. Prohibited Usage

a. Using Bank's computer resources to access the Internet for personal purposes,

without approval from the user's manager and the IT department, are not allowed.

b. Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.
c. The Bank also prohibits the conduct of political activities, engaging in fraudulent activities, or knowingly disseminating false or otherwise defamatory materials.
d. Deliberate pointing or hyper-linking of Bank's Web site to other websites whose content may be inconsistent with or in violation of the aims or policies of the Bank.
e. Any conduct that would constitute or encourage a criminal offense or otherwise violate any regulations, local, state, national or international laws and regulations.
f. Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
g. Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
h. Unauthorized downloading of any shareware or commercial software / programs or files for use without authorization in advance from the IT Department and the user's manager.
i. Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, defamatory, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
j. Bandwidth in connecting to the Internet is a shared, finite resource. Users must make Reasonable efforts to use this resource in ways that do not negatively affect other employees

6. Expectation of Privacy

Users should consider their Internet activities as periodically monitored and limit their activities accordingly. Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on Bank's computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of Bank's information systems.

7.Email

Although email is accessed using internet, a separate policy has been framed for the same.

8. Maintaining Corporate Image

a. Representation:

When using Bank's resources to access and use the Internet, users must realize that they represent the Bank.

b. Bank's Materials

Users must not place Bank's material (examples: internal note sheets, press releases, product or usage information, documentation, images, etc.) on any mailing list, public news group, social media or such service without permission from the authority of the Bank.

9. Exceptions

Any exception to the policy must be approved by higher authority of the Bank.

10.Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

Chapter 8:

POLICY ON EMAIL USAGE

1. Introduction

Electronic email is one of the many modes of communications of the Bank. This policy of THE BIHAR STATE COOPERATIVE BANK Ltd. lays down the guidelines with respect to the use of e-mail services. Misuse of email can post many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications.

2. Purpose

The purpose of this email policy is to ensure proper use of THE BIHAR STATE COOPERATIVE BANK Ltd. email system and make users aware of what THE BSCB Ltd. deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email system of the Bank.

3. Scope

This policy covers appropriate use of any email sent from a THE BIHAR STATE COOPERATIVE BANK Ltd. email address and applies to all employees, vendors, and agents operating on behalf of BSCB Ltd.

4. Allowed Email Services

a. All use of email must be consistent with THE BIHAR STATE COOPERATIVE BANK Ltd. policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
b. All official email account should be used primarily for THE BIHAR STATE COOPERATIVE BANK Ltd. business-related purposes but personal use of BSCB Ltd. email system for commercial uses is strictly prohibited.
c. Email should be retained only if it qualifies as THE BIHAR STATE COOPERATIVE BANK Ltd. business record. Email is a BSCB Ltd. business record if there exists a legitimate and on -going business reason to preserve the information contained in the email.
d. Email that is identified as THE BIHAR STATE COOPERATIVE BANK Ltd. business record shall be retained according to BSCB Ltd. Data Backup and Archiving Policy.
e. New Email Ids to be opened only with proper approval of C.E.O. All such requests shall be sent to Head Office and processed by IT department.

5. Prohibited Email Services

a. THE BIHAR STATE COOPERATIVE BANK Ltd. email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any BSCB Ltd. employee should report the matter to their supervisor immediately.
b. Users are prohibited from automatically forwarding THE BIHAR STATE COOPERATIVE BANK Ltd. email to a third-party email system. However individual messages may be forwarded by the authorised user to any third-party email system as per case to case on requirement basis.
c. Users shall not download e-mails from their official e-mail account, configured on the THE

BIHAR STATE COOPERATIVE BANK Ltd. mail server, by configuring POP or IMAP on any other e-mail service provider. This implies that users should not provide their e-mail account details (id and password) to their accounts on private e-mail service providers.

d. Using a reasonable amount of THE BIHAR STATE COOPERATIVE BANK Ltd. resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from BSCB Ltd. email account is prohibited.
e. Employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
f. Auto-save of password in e-mail service shall not be permitted due to security reasons.
g. THE BIHAR STATE COOPERATIVE BANK Ltd. may monitor messages without prior notice, whereas BSCB Ltd. is not obliged to monitor email messages.

6. In Case of Compromise of Email-Id

a. Whenever a compromise of an e-mail id is detected by the Bank, an SMS alert shall be sent to the user on the registered mobile number. In case an "attempt" to compromise the password of an account is detected, an e-mail alert shall be sent. Both the e-mail and the SMS shall contain details of the action to be taken by the user. In case a user does not take the required action even after five such alerts (indicating a compromise), the Bank reserves the right to reset the password of that particular e-mail id under intimation to the higher authority of the Bank.
b. In case of a situation when a compromise of a user id impacts a large user base or the data security of the deployment, the IT Team shall reset the password of that user id. This action shall be taken on an immediate basis, and the information shall be provided to the user and the higher authority subsequently.

7. Exceptions

Any exception to the policy must be approved by the higher authority in advance.

8. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

Chapter 9:

POLICY ON OUTSOURCING OF I.T. SYSTEM

1. Introduction

a. A part of the Information Technology Systems may be outsourced to competent vendors as per the guidelines issued by the Reserve Bank of India (RBI) or National Bank for Agriculture and Rural Development (NABARD) or any other appropriate authority or as per industry best practices. All the business and support functions of the bank are mandated to adhere to this outsourcing policy.
b. Outsourcing involves transferring responsibility for carrying out an activity (previously carried on internally or a new venture) to an outsourcer for an agreed charge. The outsourcer provides services to the Bank based on a mutually agreed

Service Level Agreement (SLA).

c. Many commercial benefits have been ascribed to outsourcing, the most common amongst these being:
   I. Reducing the organization's costs.
   II. Greater focus on core business by outsourcing non-core functions.
   III. Access to world-class skills and resources

d. Despite the potential benefits, information security incidents such as inappropriate access to or disclosure of sensitive information, loss of intellectual property protection or the inability of the outsourcer to live up to agreed service levels, would reduce the benefits and could jeopardize the security posture of the organization.

2. Objective

This policy specifies controls to reduce the information security risks associated with outsourcing.

3. Scope

a. The policy applies throughout the Bank
b. Outsourcing providers (also known as outsourcers) include:
   I. Hardware and Software support and maintenance staff.
   II. External consultants and contractors.
   III. IT or business process outsourcing firms, etc.

4. Policy Axioms

a. The commercial benefits of outsourcing non-core business functions must be balanced against the commercial and information security risks.
b. The risks associated with outsourcing must be managed through the imposition of suitable controls, comprising a combination of legal, physical, logical, procedural and managerial controls.

5. Choosing an Outsourcer

a. Criteria for selecting an outsourcer shall be defined and documented, taking into account the:
   I. Company's reputation and history.
   II. Quality of services provided to other customers.
   III. Number and competence of staff and managers.
   IV. Financial stability of the company and commercial record.
   V. Retention rates of the company's employees.
   VI. Quality assurance and security management standards currently followed by the company (e.g., certified compliance with ISO 9000 and ISO/IEC 27001).

b. Further information security criteria may be defined as the result of the risk assessment (see next section).

6. Assessing Outsourcing Risks

a. Management shall nominate a suitable THE BIHAR STATE COOPERATIVE BANK Ltd. Owner (department or personnel) for each business function/process outsourced. The owner, with help from the local Information Risk Management Team, shall assess the risks before the function/process is outsourced, using Bank's standard risk assessment

processes.

b. In relation to outsourcing, specifically, the risk assessment shall take due account of the:
   - ✓ Nature of logical and physical access to Bank's information assets and facilities required by the outsourcer to fulfil the contract.
   - ✓ Sensitivity, volume and value of any information assets involved.
   - ✓ commercial risks such as the possibility of the outsourcer's business failing
   - ✓ Completely, or of them failing to meet agreed service levels or providing services to Bank's competitors where this might create conflicts of interest.
   - ✓ Security and commercial controls known to be currently employed by Bank and/or by the outsourcer.

c. The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if Bank will be benefited overall by outsourcing the function to the outsourcer, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g., if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

d. All contracts shall be submitted to the Legal Department for accurate content, language and presentation.

e. The contract shall clearly define each party's responsibilities toward the other by defining the parties to the contract, effective date, functions or services being provided (e.g., defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract.

7. Contracts and confidentiality agreements

a. A formal contract between Bank and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing.
b. If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between Bank and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).
c. Information shall be classified and controlled in according with Bank's policy.
d. Any information received by Bank from the outsourcer which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labelling.
e. Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.

8. Hiring and training of employees

a. Outsource employees, contractors and consultants working on behalf of the Bank shall be subjected to background checks equivalent to those performed on Bank's permanent employees. Such screening shall take into consideration the level of trust and responsibility associated with the position and (where permitted by local laws):
   - I. Proof of the person's identity (e.g., passport).
   - II. Proof of their academic qualifications (e.g., certificates).
   - III. Proof of their work experience (e.g., résumé/CV and references).
   - IV. Criminal record check.

b. Companies providing contractors / consultants directly to the Bank or to outsourcers used by the Bank shall perform at least the same standard of background checks as those indicated above.

Chapter 10:

POLICY ON PROVIDING ALTERNATIVE DELIVERY CHANNEL TO BANK CUSTOMER

1. Introduction

Alternative delivery channels, defined as those channels that expand the reach of services beyond the traditional bank branch channel, have emerged as a result of innovations in information and communication technology and a shift in consumer expectations. ADCs are transformative in nature, accommodating the demand for access to financial services "anytime, anywhere, anyhow". They rely heavily on information and communication systems and devices ranging from ATMs, Personal Computers or laptops, Mobile Phones, Tablets etc., all of which enable the instant transmission of financial and non-financial information between the customer and the banks or financial services providers. Changes in customer behaviour and preferences around products, distribution channels, and processes are also acting as catalysts for the development of alternative channels.

2. Objectives

This policy specifies controls to reduce the information security risks associated with alternative delivery channels of the Bank.

3. Scope

a. The policy applies throughout the Bank
b. Alternative Delivery Channels service providers include:
   I. ATM / Debit Card Service Provider.
   II. PoS/Mpos Service Provider.
   III. Internet Banking Service Provider.
   IV. Micro – ATM service provider.
   V. CSP service provider.
   VI. Any other alternative delivery channel that bank may introduce later

4. Policy for Issuance of ATM / Debit Cards

a. ATM or Debit Cards will be issued to the eligible customers who apply for the ATM or Debit Card in Bank's prescribed form. ATM or Debit Card will be issued on selected deposit products only.
b. The deposit products and eligibility of customers for ATM or Debit Card may be revised by the Bank on time to time as per industry best practice or as per norms of the regulatory bodies for Banks.
c. The ATM or Debit Card should be issued to customers whose KYC is up-to-date and the accounts are operative.
d. ATM or Debit cards should be mailed to the customer on his latest updated address by post or courier service or may be distributed manually from branches to the customer present in person.
e. The branches should keep the secrecy of the PINs before it is being delivered to the related

customers.

f. In no circumstances Debit Cards and PIN mailers should be kept at one place (same locker).
g. PIN should be collected by the customer from the branch on production of identity proof and signing on PIN collection register.
h. PIN should be supplied the account holder only (any one customer, in case of joint accountholder, required not objection from other)
i. Detailed inventory of ATM or Debit Cards should be maintained by the ATM section of the Bank. Branch should maintain a separate register of ATM or Debit Cards of the customers of the respective branch.
j. Limit for Cash Withdrawal, online transfer, PoS transaction should be fixed by bank in advance and it should be communicated to the customers by updating the details in Bank's website, Circular to the Branches or by any other means.

5. Policy for Internet Banking

a. Only the full KYC compliant customers of the banks who have applied for Internet Banking in the prescribed form be given the internet banking facility.
b. The detailed list of the internet banking customers will be maintained by the IT department of the Bank.
c. The PIN (Personal Identification Number) should be collected by the customer on his own from the branch where the account is being maintained.
d. The Information Technology department should keep the secrecy of the PINs before it is being delivered to the related branch.
e. The branches should keep the secrecy of the PINs before it is being delivered to the related customers.
f. The "Policy on Outsourcing of Information Technology" (See Chapter 9) is applicable for the Internet Banking Service provider.

Chapter 11:

POLICY FOR AMENDMENT OF I.T. POLICY

a. Repeal and savings:

I. Every rule, regulation, bye-law or any provision in any agreement or a resulting corresponding to any of the regulations herein contained and in force immediately before the commencement of these regulations and applicable to officers and employees is hereby repealed.

II. Notwithstanding such repeal, any order made or action taken under the provisions so repealed shall be deemed to have been made or taken under the provisions of these regulations.

b. The Board of Directors of the bank is empowered to make any amendments to this Information Technology Policy documents. Any amendment to this policy, if required, has to be proposed by the Information Technology Department or the senior level management of the Bank and the proposal should be passed in the meeting of Board of Directors.

Today on 04.01.2022 the Board of Directors of the Bank in its meeting approves the first amendment of Information Technology Policy of Bank.