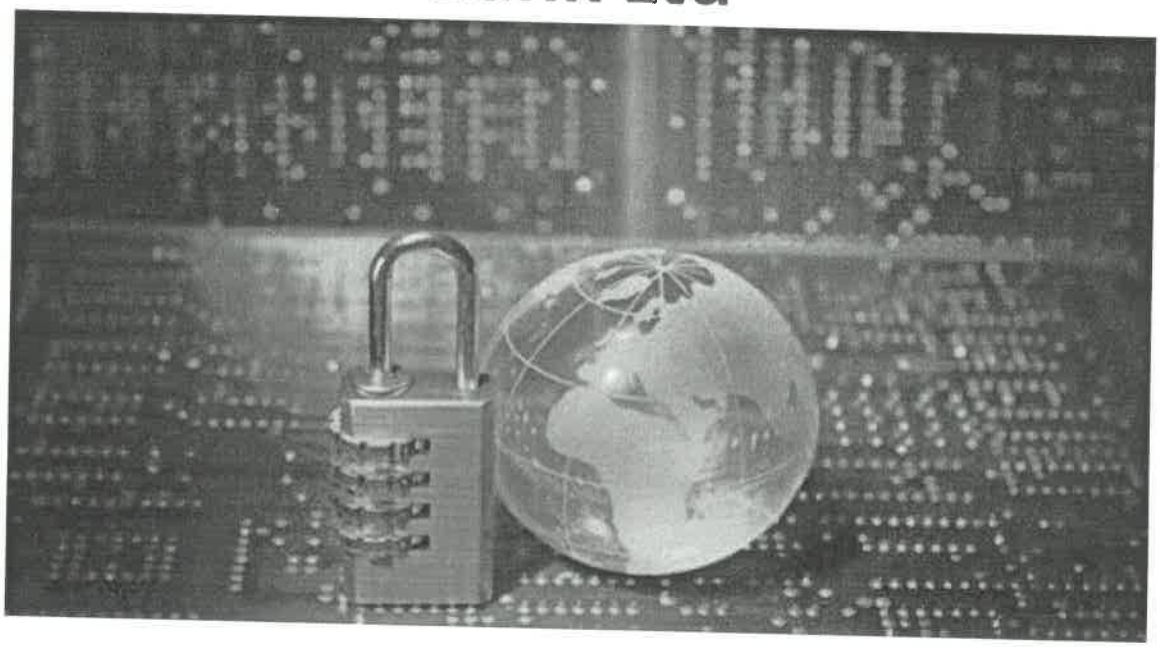
Cyber Security Policy & Cyber Crisis Management Plan

For

The Bihar State Cooperative Bank Ltd



BIHAR STATE CO-OPERATIVE BANK L... PATNA 1914

Cyber Security Policy

and

Cyber Security Crisis Management Plan

(CCMP)

The Bihar State Cooperative Bank Ltd

Ashok Rajpath,
Patna - 800004, Bihar.

Version 1.0

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

Document Details

Version: 1.0

Formulation Details

Drafted by:

1. IT Department
2. IT Steering Committee

Table of Contents

1 Purpose 10
2 Objective 10
3 Scope 10
4 Policies 11
4.1 Cyber Security Policy 11
4.1.1 Roles and Responsibilities 11
4.1.2 Approval Authority 16
4.1.3 CYBER/Information Security Awareness Team 16
4.1.4 Cyber Security Strategy 17
4.1.5 Cyber Security Policy Priorities 17
4.1.6 Cyber security framework 18
4.1.7 Operational Policies 18
4.1.8 Cyber Crisis Management Plan (CCMP) 23
4.1.9 Cyber Security Audit 25
4.1.10 Exceptions 26
4.1.11 Non - Compliance 26
4.1.12 Annexure 27

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

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 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.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

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	A computer virus is an unauthorized and malicious program, which replicates itself and spreads onto various data storage media such as, magnetic disk, tapes, Thumb/Flash drive, External Hard drive, SD/Memory card and across the network. The viruses are designed to spread from one file to another, from one program to another, from one machine to another, and even from one network to another. Viruses threaten the integrity and availability of data. The symptoms of virus infection include considerably slower response time from the system, inexplicable loss of data, erroneous change in file dates, 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.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

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 eare 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 "BANK WEBSITE" 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	This term refers to the system administrators of the respective systems/applications of BSCB.
IT Technical Team Leaders	IT Technical Team Leaders are responsible for managing & monitoring the following services processes:

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

	• 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.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

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 term refers to the system administrators of the respective systems/applications of the organization.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

1 Purpose

1. The Bihar State Co-operative Bank Ltd. (hereafter referred to as "BSCB" or "the organization" or "organization") has laid down the IT Policies 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 Cyber Security Policy

4.1.1 Roles and Responsibilities

Senior Management Team: Senior Management [Managing director, General Manager (IT), Deputy General Manager (IT)] of the Bank shall play its responsibility for implementing the business strategy in line with its risk appetite, while being cognizant of cyber threats. As such, the Senior Management will ensure to:

a) Implement the board approved cyber-security strategy, policy, and framework.
b) Understand cyber organizational scope as well as identify cyber threats, critical business processes and assets.
c) Ensure the creation of mitigation and recovery procedures to contain cyber risk incidents, reduce losses and return operations to normal.
d) Continuously improve collection, analysis, and reporting of cybercrime information. This can be achieved through understanding the business environment the Bank, potential cyber risk points and referring to the guidelines of the regulator and adopting best practices tools available.
e) Oversee deployment of strong authentication measures to protect customer data, transactions, and systems.
f) Ensure the provision of sufficient number of skilled staff for the management of cyber security, who should be subjected to enhanced background and competency checks.
g) Ensure timely and regular reporting to the Board/ NABARD on the cyber risk status of the institution.
h) Incorporate cyber security as a standard agenda in Senior Management meetings and provide regular reports of the Bank's cyber security posture to the board.
i) Document cyber security incident response plan providing a roadmap for the actions the Bank will take during and after a security incident.
j) Create a post incident analysis framework to determine corrective actions to prevent recurrence of the incidents in the future.
k) Oversee the evaluation and management of risks introduced by third party service providers; Bank may require attestation/assurance reports provided by reputable independent auditors for service providers.

Chief Information Security Officer (CISO): The role of CISO is aimed at creating an organizational culture of shared cyber security ownership. Ultimate responsibility for implementing this policy shall rest with the CISO of the bank. He/ She will be a senior level executive not below the rank of Assistant General Manager. CISO will report to the General Manager concerned or the Managing Director of the Bank. As such, the CISO is responsible for:

a) Overseeing and implementing the Bank's cyber security program and enforcing the cyber security policy.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

b) Ensuring that the Bank maintains a current bank-wide knowledge base of its users, devices, applications, and their relationships.
c) Ensuring that information systems meet the needs of the Bank and the ICT (Information and Communication Technology) strategy, in particular information system development strategies, comply with the overall business strategies, risk appetite and ICT risk management policies of the Bank.
d) Design cyber security controls with the consideration of users at all levels of the organization, including internal (i.e. management and staff) and external users (i.e. contractors/consultants, business partners and service providers).
e) Organizing professional cyber related trainings to improve technical proficiency of staff.
f) Ensure that adequate processes are in place for monitoring IT systems to detect cyber security events and incidents in a timely manner.
g) Reporting to the MD on an agreed interval but not less than once per quarter on the following:
    - Assessment of the confidentiality, integrity and availability of the information systems in the Bank.
    - Detailed exceptions to the approved cyber security policies and procedures.
    - Assessment of the effectiveness of the approved Cyber-security program.
    - All material cyber security events that affected the Bank during the period.
h) Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.
i) Incorporate the utilization of scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.
j) Ensure frequent data backups of critical IT systems (e.g. real time back up of changes made to critical data) are carried out to a separate storage location.
k) Ensure the roles and responsibilities of managing cyber risks, including in emergency or crisis decision-making, are clearly defined, documented and communicated to relevant staff.
l) Continuously test disaster recovery and BCP arrangements to ensure that the bank can continue to function and meet its regulatory obligations in the event of an unforeseen attack through cyber-crime.

Cyber/Information Security Department (ISO): Teams & functions

IT Committee/ GM-IT / heads the Cyber/Information Security Department (ISO) with the following teams for effective implementation and monitoring the Cyber/Information Security activities. All the teams report to Chief Information Security Officer (CISO).

Governance, Risk, and Compliance (GRC) Team: This team performs all activities required to ensure proper oversight, risk management, and compliance with legal. Regulatory, Guideline, and other cyber/information-security related requirements with which the organization is required to comply. The set of activities performed by the GRC unit includes the following:

- **Planning -** Identify an annual work plan to achieve security goals and objectives consistent with BSCB's strategic plan.

- **Development-** Lead in the development of information security guidelines, standards, guidelines, processes, and procedures. Develop, implement, and maintain an information security program, plan, and processes. Define information security roles and responsibilities.

- **Risk Management -** Establish an information security risk management strategy, process, and program. Conduct risk assessments manage incidents; provide internal and external reporting, involvement in security awareness education and training.

- **Governance:** Govern and oversee the information security program and plan. Evaluate the effectiveness of ongoing security operational processes, monitor compliance for internal and external requirements.

- **Compliance:** Ensure that controls are adequate to meet security requirements; and audit rectifications are done

Security Management Team

- **Guidelines:** Develop cyber / information security guidelines. Defining, implementing, and enforcing the acceptable use Guideline. Develop Secure Configuration Documents (SCD) for cyber/information assets.

- **Security requirements:** Specify, allocate and assign confidentiality, integrity and availability requirements to development and acquisition organizations and assets.

- **Security architecture:** Develop and maintain an enterprise security architecture.

- **Secure lifecycle:** Ensure that security requirements are adequately addressed throughout the development and acquisition lifecycles for all assets.

- **Certification and accreditation:** Perform certification and accreditation prior to releasing new systems and software to production.

Asset Management:

- Maintain inventories of network (including wireless devices), hardware, software, licenses, application and mobile device assets

- Define, assess, and maintain controls necessary to protect networks, hardware, software, application, and mobile devices in accordance with security requirements (This includes, for example, intrusion prevention and detection controls.)

- Define, assess, and maintain controls necessary to protect the network and Internet perimeters in accordance with security requirements (This includes, for example, firewalls, and VPNs.)

- Designate, prioritize, and categorize information and vital assets (Categorization is typically informed by the criticality and sensitivity of the information asset.)

BIHAR STATE COOPERATIVE BANK LTD. PATNA 1914

Security Implementation Team: This team shall be part of the IT department and a reporting arrangement with CISO.

- Coordination with IT Division & ISO in security implementations
- Design & Implement security projects in consultation with ISO
- Implement & manage Security Devices
- Implement & manage Anti-virus, Patch Management, Biometric,
- User access controls etc.
- Assistance to IT Division in conducting DR drills and business continuity activities
- Responsible for maintenance of certifications like ISO 27001
- Develop and maintain inventories of network (including wireless), hardware, software, application and mobile device assets
- Implement and maintain controls necessary to protect networks, hardware, software, application, and mobile devices in accordance with security requirements (This includes, for example, intrusion prevention and detection controls.)
- Implement and maintain controls necessary to protect the network and Internet perimeters in accordance with security requirements (This includes, for example, firewalls, and VPNs.)
- Manage configurations for networks, hardware, software, software, application and mobile devices
- Manage changes for networks, hardware, software, applications and mobile devices

Security Monitoring Team:

- Owner of Security Operations Centre (SOC) and Incident Management at the organization level. The Security Operations Center (SOC) is responsible for all day-to-day security operations. Collecting sources of intelligence (adversary behaviors, active incidents, national and international events, etc.)
- Analyzing and managing threats to BSCB's cyber/information security.
- Conducting situational awareness based on intelligence and threat information, and formulating and reporting an operational view of the external environment
- Conducting logging (users, applications, networks, systems access to physical assets, etc.)

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

- Monitor logs and other sources of information (users, applications, networks, systems, access to physical assets, etc.)
- 24*7*365 surveillance of the IT Infrastructure of BSCB to guard against Cyber/Information Security breaches and incidents.
- Managing vulnerabilities, viruses, and malicious code and take necessary actions
- Regular Penetration Testing, Vulnerability Assessment and liaison with local Computer Emergency Response Team (CERT), if it exists. Testing for vulnerabilities at reasonable intervals of time is very important. It is also essential that Cyber/Information Security Department ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.
- Planning for incident management and response, business continuity, and IT disaster recovery.
- Managing security incidents (detection, analysis, response, and recovery).
- Performing tests, exercises, and drills of all response plans.
- Performing problem management, root cause analysis, and postmortem reviews following the occurrence of an incident.
- Conducting forensic investigations and working with law enforcement and other regulatory bodies during and following an incident.
- Responsible for collection, aggregation, correlation, analysis, forensics and synthesis of information related to security incidents to learn effective lessons and to incorporate changes in policies and procedures accordingly on a continuous basis.
- Communicating with internal stakeholders and external entities, as required.

Cyber Incident Response Team (CIRT):- In order to strengthen the cyber incident response capabilities a Cyber Incident Response Team (CIRT) will be constituted with the approval of the appropriate authority/Board of the Bank to coordinate the response activities. The Cyber Incident Response Team is composed of various members like General Manager (IT)/CISO, along with CIRT core IT Cell members that make up the CIRT. The Cyber Incident Response Team's (CIRT) mission is to:

a) Limit the impact of cyber incidents in a way that safeguards the well-being of the Bank's users (employees, customers and vendors).
b) Protect the information technology infrastructure of the Bank.
c) Protect sensitive Bank data from disclosure, modification and exfiltration.
d) Collect the information necessary to pursue investigation(s) at the request of the authorized Bank authority.

Roles and responsibilities of CERT:

- Vulnerability Reporting
- Incident Reporting
- Penetration testing
- Incident Analysis
- Vulnerability Assessment of various bank Websites
- Log analysis
- Identify and classify cyber-attack scenarios.
- Determine the tools and technology used to detect and prevent attacks.
- Develop a checklist for handling initial investigations of cyber-attacks.
- Determine the scope of an internal investigation once an attack has occurred.
- Conduct any investigations within the determined scope.
- Promote cyber security awareness within departments.
- Address data breach issues, including notification requirements.
- Conduct follow up reviews on the effectiveness of the department's response to an actual attack.
- Prepare SOP for different types of crisis.

4.1.2 Approval Authority

The IT Steering Committee of BSCB shall approve the Cyber Security Policy. The Bank has identified Chief Information Security Officer (CISO) as the custodian of Cyber Security Policy. He/She will hold the primary responsibility to maintain the policy document in both electronic and paper format. The finalized Policy shall be reviewed by the Management once every year to incorporate any changes the components and parameters of this Policy may go through to ensure that they stay pertinent as the business needs change. IT Sub Committee of the Bank shall review the Policy at least half-yearly to assess its effectiveness and implementation.

4.1.3 CYBER/Information Security Awareness Team

a. Education, Awareness and Promotion of Cyber/Information Security initiatives across the organization.

b. Intensive Training of various types and for different levels on Cyber/Information Security.

c. Promoting customer education and awareness on Cyber/Information Security through appropriate channels, tools and interventions.

d. Proactive dissemination of Cyber/Information Security Policy initiatives, mechanisms and best practices.

e. Maintain a Resource Base of online tutorials, demos, quizzes and FAQ's on the Intranet for easy access within the organization.

f. Measurement and Monitoring of Effectiveness of Cyber/Information Security Policy implementation

g. Manage relationships with third parties (vendors, suppliers, contractors, partners, etc.)

4.1.4 Cyber Security Strategy

A cyber security strategy has been outlined to address the strategic objectives of securing BSCB's cyber space and shall be implemented through the following initiatives:

a. Cyber Security Policy, Compliance and Assurance: This Policy is distinct and separate from the broader IT Security Policy and IT Policy to highlight the risks from cyber threats and the measures to address / mitigate these risks.

b. Cyber Security Program: Policies/procedures shall be developed for securing the infrastructure, meeting the domain specific needs and enabling technologies. Global best practices shall be adopted in the protection of BSCB's information systems, including the systems of those transacting with government online. Secure, resilient and trusted electronic operating environment that supports BSCB's interests shall be promoted.

c. Cyber Security Incident Management and Response: Security Operations Centre (SOC) monitoring capabilities shall be updated & upgraded on continuous basis to meet the cyber challenges, protect BSCB's information, as well as its reputation by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

d. Cyber Security Awareness: Training, skills/competence development and end-user awareness shall be provided. Development of a skilled cyber security workforce to be promoted with suitable trainings to develop innovative solutions. All users shall be educated and empowered with the information, confidence and practical tools to protect them online.

4.1.5 Cyber Security Policy Priorities

a. Monitoring framework shall be strengthened for ensuring a secure cyberspace environment.

b. Cyber Crisis Management Plan (CCMP) shall be developed to enhance the protection of critical asset/data in the IT infrastructure by placing an effective BCP DR plan to recover rapidly from cyber-attacks/other incidents and safely resume critical operations. CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment.

c. Security practices shall be mandated in every phase such as design, development, implementation, testing and operation of IT resources.

d. Comprehensive set of metrics that provide measures such as key performance indicators and key risk indicators shall be developed.

e. BSCB should be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.

f. Security Operations Centre (SOC) shall be upgraded to Cyber Security Operations Centre (CSOC) and regularly updated to meet the emerging cyber threats.

g. Cyber security awareness programs shall be made mandatory for new recruits and web-based programs can be conducted for lower, middle & upper management every year.

h. Among other things, BSCB should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

4.1.6 Cyber security framework



4.1.7 Operational Policies

4.1.7.1 Allowed Internet Services

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. General Browsing—WWW' with 'https' services as necessary for business purposes will be allowed only in exceptional cases, through a centralized proxy with proper higher authority permission and separate register should maintain

b. 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 BSCB.

4.1.7.2 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 IT 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 as per provision.

4.1.7.3 Cyber Security Organization

a. Specific knowledge, skills, and abilities shall be identified for all functional roles in BSCB (prioritizing those mission-critical to the business and its security) to support the defense of the enterprise. An integrated plan shall be developed and executed to assess, identify gaps and remediate through Guideline, organizational planning, training, and awareness programs.

4.1.7.4 Server Deployment and Configuration Management/VA/PT

a. A detailed process flow document shall be defined for server deployment in Data Centre and Disaster Recovery Site, explaining the configurations done on the newly deployed server.

b. Synchronized time sources (i.e. Network Time Protocol - NTP) from which all servers and network equipment retrieve time information on a regular basis shall be deployed so that timestamps in logs are consistent.

c. The security configuration of network devices, laptops, servers, and workstations shall be actively managed and implemented using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

d. Audit logs of events that could help detect, understand, or recover from an attack shall be collected and analyzed. Automated vulnerability scanning tools shall be considered for detecting vulnerabilities in the systems Regular external and internal penetration tests shall be conducted to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

4.1.7.5 Internet Security

a. Access to Internet shall be given as per acceptable usage Policy as well as on the basis of user roles and responsibilities in respective department.

b. All internet connections shall pass through a firewall and / or a proxy server.

c. Dial up internet access from the Office Network shall be strictly prohibited

d. Users shall adhere to Internet usage Policy as defined in acceptable usage Policy defined in this document.

e. Internal users shall be prohibited from accessing Web Sites that are deemed inappropriate.

f. The DGM / AGM / Chief Officer IT shall define the protocols/services/sites to be allowed for use.

g. Monitoring World Wide Web activity shall ensure that users are not accessing sites containing

- Inappropriate material and shall ensure that proper levels of security are used.
- All access to Internet services shall be logged.
- The System Administrator / In-charge shall review the log files on a pre-defined frequency (probably on daily basis).

4.1.7.6 Vendor Risk Management

a. The need for outsourcing critical processes shall be evaluated and selection of vendor/partner shall be made on the basis of comprehensive risk assessment.

b. Risk assessment shall be conducted to identify the criticality of all third party/outsourced service providers.

c. Effective due diligence, oversight and management of third-party vendors/service providers & partners shall be conducted regularly.

d. Appropriate framework, guidelines and procedures supported by baseline system security configuration standards shall be established to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities shall be put in place.

e. It has to be ensured that the service provider adheres to all regulatory and legal requirements of the country.

f. BSCB may necessarily enter into agreement with the service provider that provides for right of audit by BSCB and inspection by the regulators of the country.

g. Non-Disclosure Agreement (NDA) from the vendors, who access the information or provide IT services, shall be obtained.

h. Vendor supplied default passwords shall be changed during the time of installation itself.

4.1.7.7 Cloud Security

a. BSCB shall exercise due diligence while choosing a cloud service provider. Reputation, history and sustainability should be the factors to consider. BSCB shall not avail any cloud service where the organization's data resides outside India. Cloud Service Provider shall ensure and assure the organization of this.

b. Third-party access to sensitive information shall be restricted to ensure the protection of intellectual property (IP), trade secrets and confidential customer information.

c. Business continuity and disaster recovery plans must be well documented and tested. Recovery time objectives shall be stated in the contract.

4.1.7.8 Cyber Security Preparedness Indicators

a. Define indicators to assess and measure adequacy of and adherence to cyber security framework.

b. Use Indicators for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals.

4.1.7.9 Cyber Security Monitoring & continuous surveillance

a. Security Operations Centre shall be established and periodically upgraded. SIEM (Security Incident and Event Management) or log analytic tools shall be deployed for log aggregation and consolidation from multiple machines and for log correlation and analysis.

b. Systems to collect and share threat local/national/international sources information be established implemented.

c. Methods to identify root cause of attacks shall be established. Such attacks shall be classified into identified categories and solutions to contain further attacks of similar types shall be found.

d. Dynamic Behavior Analysis tools which analyses the static & dynamic behavior, and which can collect Indicators of Compromise (IOC) shall be established and implemented.

e. Analytics with good dashboards showing the Geo-location of the IP's shall be established.

4.1.7.10 Cyber Incident Management/Response

a. Effective Incident Response programmer shall be put in place with due approval of the Board and Top Management.

b. A Cyber Crisis Management Plan (CCMP) shall be evolved and shall be a part of the overall Board approved strategy.

c. BSCB's information, as well as its reputation shall be protected by developing and implementing an incident response infrastructure for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

d. Incident Management Policy and Incident response Policy shall be followed when an incident is reported.

e. Systems to collect and share threat local/national/international sources information following legally accepted/defined means/process shall be established and implemented.

f. Strategies to respond to advanced attacks containing ransom ware/cyber extortion, data destruction, OOOS, etc. shall be documented and implemented.

g. Overall strength of BSCB defenses (the technology, the processes, and the people) shall be tested periodically.Periodic exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively shall be performed.

h. Counter response and Honey pot services shall be established.

4.1.7.11 Cyber Security Awareness

a. A comprehensive cyber security awareness training program shall be established to enhance the overall cyber security awareness level in BSCB and to reduce the technology risks.

b. Security Policies covering secure and acceptable use of BSCB's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level shall be communicated to users/employees, vendors & partners.

c. Reporting of suspicious behavior incidents to the incident management team shall be encouraged among users.

d. Targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.) shall be conducted.

e. Awareness level shall be evaluated periodically.

f. Mechanism for adaptive capacity building for effective Cyber Security Management shall be established. Cyber security awareness programs shall be made mandatory for new recruits and web-based quiz & training for lower, middle & upper management every year.

g. Board members may be sensitized on various technological developments and cyber security related developments periodically.

h. Board members may be provided with training programs on IT Risk and Cybersecurity Risk and evolving best practices in this regard to cover all the Board members at least once a year.

4.1.7.12 Customer Education and Awareness

a. Customer awareness and education with regard to cyber security risks shall be maintained and improved upon.

b. Customers shall be encouraged to report phishing mails/ Phishing sites and on such reporting take effective remedial action.

c. Customers shall be educated by various communication channels on the downside risk of sharing their login credentials, passwords etc. to any third-party vendor and the consequences thereof.

d. In addition to the directions provided in this Policy, all other Policies of IT Security Policy and its sub-Policies of BSCB will apply.

4.1.8 Cyber Crisis Management Plan (CCMP)

4.2.8.1 Purpose:

The purpose of this Cyber Crisis Management plan is to establish BSCB Bank's strategic framework and guidelines to prepare for , respond to, and begin to coordinate recovery from a cyber incident.

Another purpose of Cyber Crisis Management Plan is to ensure that interruption or manipulations of critical functions or services in BSCB are in detail, occasional and controllable and cause least possible damage.

Also, to assist BSCB to place mechanisms to effectively deal with cyber security crisis and be able to identify responsibilities and accountabilities right down to individual level.

4.2.8.2 Scope:

Cyber Crisis Management plan (CCMP) covers different type of cyber crisis, possible targets and related impact, actions and responsibilities of concerned user. Also covers the cyber incident response of BSCB to deal with cyber crisis situations.

The field of cyber security is technology intensive and new vulnerabilities arise with progress in technology giving rise to new types of incidents. As such, the plan of response to cyber security incidents need to be updated on regular basis or whenever is required.

4.2.8.3 Impact of Cyber Crisis:

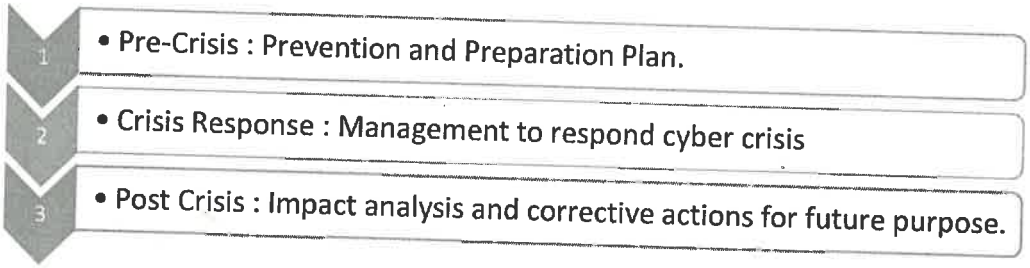
Cyber-attacks may create influence on standalone systems /multiple systems/networks and may result in complete breakdown of important services, this may lead to reputational loss / financial loss / Sensitive data loss etc.

4.2.8.4 Classification of Cyber crisis:

- Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure
- Large scale defacement of websites
- Malicious Code attacks (virus/worm/ /Trojans/Botnets)
- Malware affecting Mobile devices
- Large scale SPAM attacks
- Identity Theft Attacks
- Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks
- Domain Name Server (DNS) attacks
- Application-Level Attacks
- Cyber Espionage and Advanced Persistent Threats

4.2.8.5 Structure of Cyber Crisis Management Plan

Three important pillars of Cyber Crisis Management Plan are as follows



4.2.8.6 Effective Management of Cyber Crisis Management Plan

Cyber Crisis Management Plan can be made effective by following instructions such as:

- Proactive monitoring of network assets and traffic for any visible signs of changes from normal situation
- Being in continuous touch with CERT-In/NABARD/RBI to receive actionable cyber security alerts and advice
- Empanelment of IT security auditors to verify effective implementation of technical, managerial, and operational security controls.
- Proactive and timely security alerts and advice to remain fully updated with regard to possible virus/worm infections, latest security patch status and work arounds for zero-day exploits
- Duly reporting security incidents and sharing all relevant information that can support real-time incident analysis & rapid response
- Identify a member of senior management as a 'Chief Information Security Officer (CISO)' to coordinate security policy compliance efforts across the organization and interact regularly with CERT-In and sectoral 'Point of Contact'
- Establish a Cyber Crisis Management Group, on the lines of Sectoral Crisis Management Committee, with head of organization as its chairman

- Prepare a list of contact persons complete with up-to-date contact details
- Prepare an Organizational level CCMP on the lines of CCMP of CERT-In, outlining roles, responsibilities of organizational stakeholders, CCMP coordination process.
- Implement the CCMP, including security best practices and specific action points as outlined below:

  a) Prepare a Security plan and implement Security control measures.

  b) Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with business impact assessment and criticality of business function.
- Collaborating with CERT-In to keep a watch on cyber space to look for malicious traffic, virus/worm infections and visible signs of build-up or emergence DDoS attacks
- Regularly participating in CERT-In trainings/workshops on contemporary topics/issues to remain updated on technology and security best practices.
- Develop and implement a business continuity strategy and contingency plan for IT systems
- Develop and implement disaster recovery and security incident management processes
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks and it can include:
- Penetration testing
- Vulnerability assessment
- Application security testing
- Web security testing
- Carry out audit of information infrastructure on an annual basis and when there is a major upgradation/change in IT infrastructure, by an independent IT security auditing organization.

4.1.9 Cyber Security Audit

Cyber security audit shall be a part of IT/ IS audit and the report for the same should be presented to the management by CISO followed by the closure tracker of gaps identified in the audit. The bank should conduct cyber security audit on annual basis. The scope of cyber security audit shall include:

a) Determining effectiveness of planning and oversight of cyber activities.
b) Evaluating adequacy of operating processes and internal controls
c) Determining adequacy of enterprise-wide compliance efforts, related to cyber policy and procedures.

d) Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions.

4.1.9.1 Planning Cyber Security Audit:

The bank shall use Risk Based Audit Approach while planning a cyber- security audit. Bank should develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.

4.2.9.2 Execution of Cyber Security Audit Policy

The bank in consultation with auditor would describe steps for executing the audit, covering activities such as understanding the business process and cyber environment, refining the scope and identifying internal controls, testing for control design and control objectives, audit evidence, documentation of work papers and conclusions of tests performed.

4.2.9.3 Reporting and Follow-up

The cyber security audit findings shall be reported to the management with the closure status/ roadmap provided by GM (IT)/CISO. Auditors would prepare an audit summary providing overview of the entire audit processing from planning to audit findings, discuss the findings with respective personnel and obtain responses.

4.2.9.4 Compliance with Security Recommendation

The Based on the findings of the audit all security recommendations must be implemented within an appropriate timeframe to ensure that all risks are addressed, and appropriate measures are taken. Practices in accordance to the Cyber Security Policy along with compliance of security recommendations from cyber security audit reports should be followed by all concerned.

4.1.10 Exceptions

Any exceptions to this policy must be duly approved by the Board/Special Officer/MD of the bank.

4.1.11 Non - Compliance

Any non-compliance shall be subject to disciplinary action, up to and including termination of employment, contractual agreement/ obligation.

4.1.12 Annexure

Template for Reporting Cyber Incidents (as per Annex-3 of RBI Cyber Security Framework) to RBI and NABARD (within 6 hours)

Basic Information	
1. Particulars of Reporting	
• Name of the Bank	
• Date and Time of Reporting to RBI, CERT-In, other agencies (please mention separately time of reporting to each)	
• Name of the Person Reporting	
• Designation/Department	
• Contact Details (e.g. official email-id, telephone no, mobileno)	
2. Details of Incident:	
• Date and Time of Incident Detection	
• Type of Incidents and Systems Affected	
• **Outage of Critical ITSystem(s)** (e.g. CBS, Treasury Systems, Trade Finance Systems, Internet Banking Systems, ATMs, Payment Systems such as SWIFT, NEFT, RTGS, NACH, IMPS)	

ii.	**Cyber Security Incidents** (e.g., DDOS, Ransomware/ crypto ware, data breach, data destruction, web defacement, etc.)	
iii.	**Theft or Loss ofInformation** (e.g. sensitive customer orbusiness information stolen or missing or destroyed or corrupted)?	
iv.	**Outage of Infrastructure**(e.g. which premises- DC/Central Processing Unit, branch, etc., power/utilities supply, telecommunications supply)?	
v.	**Financial** (e.g. liquidity, bank run)?	
vi.	**Unavailability of Staff** (e.g. number and percentage on loss of staff / absence of staff from Work	
vii.	**Others** (e.g. outsourced serviceproviders, business partners, breach of IT Act/any other law and RBI/SEBI regulations,etc.	

BIHAR STATE CO-OPERATIVE BANK LTD PATNA 1914

• What actions or responses have been taken by the bankat the time of first reporting/till the time of subsequent reporting?	
3. **Impact Assessment (examples are given but not exhaustive):**	
• Business impact including availability of services-BankingServices, Internet Banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement Systems, etc.	
• Impact on stakeholders- affected retail/ corporatecustomers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc.	
• Financial and market impact- Trading activities, transactionsvolumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds, etc.	
• Regulatory and Legal impact	
4. **Chronological Order of Events**	
• Date of incident, start time and duration.	

• Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
• Stakeholders informed or Involved	
• Channels of communicationsuserd (e.g. email, internet, sms, press release, website notice, etc.)	
• Rationale on the decision/activation of BCPand/or DR	
5. **Root Cause Analysis (RCA):**	
• Factors that caused the problem/Reasons for occurrence, Cause and effects of incident	
• Interim measures to mitigate/resolve the issue, andreasons for taking such	
measures, and	
• Steps identified or to be takento address the problem in the longer term. List the remedial measures/corrections affected(one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. **Date/target date of resolution** (DD/MM/YYYY)	
•	

•	
•	

Annexure- A: Cyber Incident Reporting by Branches/Offices to Head Office

The Bihar State Co-operative Bank Ltd.

Cyber Incident Report (From Branches/Offices to Head Office)

Reporting Date :

Branch Id :

Name of the Branch/Office :

Name of the Person Reporting :

Designation of the Person Reporting:

Contact Details- Email ID:

Tel: Mobile:

Date Incident Occurred: Approximate Time:

Brief description of the incident:

Impact on Incident: Data Theft/Service Disruption (downtime)/System (Software/Hardware) sabotage/ Other (Please explain):

Number of users affected:

Duration of the incident: from - to -

Details of Compromised Machine:

Physical Location :

Operating System :

IP Address :

Physical security of the machine : Yes/No

Logical security of the machine : Yes/No

Is the compromised machine connected to CBS? Yes/No

Is the compromised machine connected to Internet? Yes/No

Is any anti-virus software running in the system? Yes/No

If yes, name of the anti-virus software and last update date:

Was the compromised machine had to be removed from the network? Yes/No

Root Cause Analysis:

Factors that caused the problem/reasons for occurrence, cause and effects of incident:

Interim measures to mitigate/resolve the issue, and reasons for taking such measures:

Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected (one time measure) and/or

corrective actions taken to prevent future occurrences of similar types of incidents:
Status of the incident:

Your comment and recommendation:

Date: **Signature:**

Annexure- B: Vulnerability Reporting Form

(from Branches/Offices to Head Office)

1. Reporter's Details:
   a. Full Name :
   b. Designation :
   c. Branch/Office :
   d. Contact Email ID :
   e. Contact Mobile No. :
   f. Contact Tel No. :
2. Vulnerability Details: (brief write up)
3. Type of Vulnerability (please tick):
   [ ]Web Application [ ] Operating System (OS) [ ]Hardware
   [ ]Others_____(please mention)
4. Date when issue found:
5. What action need to be taken:

6. Vulnerable Product type:

[ ] Web Application [ ] Client Software [ ] Server Software

[ ] Operating System [ ] Firmware [ ] Hardware

7. Vulnerable Product Name and Version:

8. If reported, Email ID to whom details sent

9.

10. If reported, date when reported:

11. Patch released? (Please tick) Yes [ ] / No [ ]

12. If patch released, date of patch release:

13. Reporter's comment:

Date: **Signature**

Annexure-C: Form to Report Incidents to CERT-In

Form to report Incidents to CERT-In			
For official use only:		Incident Tracking Number : **CERTIn-**	
1. Contact Information for this Incident:			
Name:	Organization:	Title:	
Phone / Fax No:	Mobile:	Email:	
Address:			
2. Sector : (Please tick the appropriate choices)			
Government Financial Power	Transportation Manufacturing Health	Telecommunications Academia Petroleum	InfoTech Other _____
3. Physical Location of Affected Computer/ Network and name of ISP.			
4. Date and Time Incident Occurred:			
Date:	Time:		
5. Is the affected system/network critical to the organization's mission? (Yes / No). Details.			

6. Information of Affected System:				
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Last Patched/ Updated	Hardware Vendor/ Model

7. Type of Incident:		
Phishing Network scanning /Probing Break-in/Root Compromise Virus/Malicious Code Website Defacement System Misuse	Spam Bot/Botnet Email Spoofing Denial of Service(DoS) Distributed Denial of Service(DDoS) User Account Compromise	Website Intrusion Social Engineering Technical VulnerabilityIP Spoofing Other_____

8. Description of Incident:

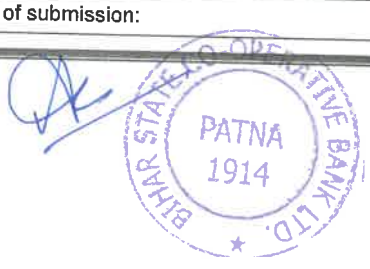
9. Unusual behavior/symptoms (Tick the symptoms)	
System crashes New user accounts/ Accounting discrepancies Failed or successful social engineering attempts Unexplained, poor system performance Unaccounted for changes in the DNS tables, router rules, or firewall rules Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user A system alarm or similar indication from an intrusion detection tool Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Anomalies Suspicious probes Suspicious browsingNew files Changes in file lengths or datesAttempts to write to system Data modification or deletion Denial of service Door knob rattling Unusual time of usage Unusual usage patterns Unusual log file entries Presence of new setuid or setgid files Changes in system directories and filesPresence of cracking utilities Activity during non-working hours orholidays Other (Please specify)

10. Has this problem been experienced earlier? If yes, details.

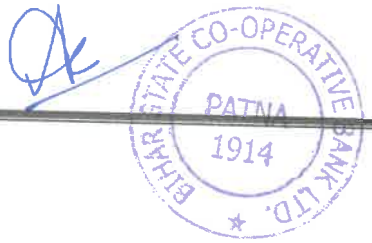
12. Agencies notified?			
Law Enforcement	Private Agency	Affected Product Vendor	Other_____

11. When and How was the incident detected:

13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)	
Whether log being submitted	Mode of submission:



OPTIONAL INFORMATION				
14. IP Address of Apparent or Suspected Source:				
Source IP address:		Other information available:		
15. Security Infrastructure in place:				
	Name	OS	Version/Release	Last Patched/Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				
16. How Many Host(s) are Affected				
1 to 10	10 to 100		More than 100	
17. Actions taken to mitigate the intrusion/attack:				
No action taken System Binaries checked	Log Files examined System(s) disconnected form network		Restored with a good backup Other _____	
Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident				
Mail/Fax this Form to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in				



BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914