Approved in 60th Board Meeting dated 27/3/2018

Uttar Bihar Gramin Bank

CYBER SECURITY POLICY

- **Document Control**

Document Name: Cyber Security Policy

Document ID Reference Number: Cyber Security Policy Ver 1.0

- **Authorization**

Prepared by	Reviewed by	Authorized by
Name: Suryanarayanan. K CM - Info. Sec.	Name: Dr. S. K. Mishra CISO	Name: Board

- **Security Classification: Internal**
- **Version history**

Version	Issue date	Effective date	Prepared by	Authorized by	Description
1.0	21.12.2016	21.12.2016	Suryanarayanan. K	Board	Final

- **Distribution list**

- Board
- Information Technology Department
- End Users
- Interested Parties (As and when required)

- **Placement**

- "For Staff Only" and "Information Security Department" Portals on Intranet
- Via HTTP access

Table of Contents

1 Introduction

Uttar Bihar Gramin Bank (henceforth collectively referred to as the bank) information systems, and the data these information systems process, are fundamental for its daily operations and effective service provision. The bank shall implement adequate security policies, procedures and controls to protect confidentiality, maintain integrity, and ensure availability of all information stored, processed and transmitted through its information systems. To build a secure and resilient cyberspace for customer there is a need to have an effective cyber security policy in the bank.

Cyberspace is a complex environment consisting of interactions between people, application, IT systems and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks (critical information infrastructure).

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, man-made or natural and the data exchanged in the cyberspace can be exploited for nefarious purposes. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

Use of Information technology by the bank has grown rapidly and is now integral part of the operational strategies of bank. It is therefore important to develop policies, procedures and technologies based on the new developments and emerging concerns and fine tune the same as per evolving cyber threats.

The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

There are various on-going activities and programs of the bank to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyberspace. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a cyber security policy, with an integrated vision and a set of sustained and coordinated strategies for implementation.

Cyber security policy is an evolving process and it caters to the whole spectrum of people, process and technology. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace.

This policy, therefore aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of Bank"s cyber space.

2 Cyber Security Scope and Applicability

1. This policy applies to all employees, contractors, consultants and third party users (internal and external) accessing bank"s information systems from within or outside.
2. This policy covers the usage of all of the bank"s information technology and communication resources, including, but not limited to:
   a. All computer-related equipment like PCs, workstations, telecomm equipment, databases, printers, servers, shared computer resources etc., and all networks and hardware to which this equipment is connected.
   b. All software including purchased or licensed business software applications, in-house applications, vendor/supplier-provided applications, computer operating systems, firmware, and any other software residing on bank-owned equipment.
   3. All intellectual property and other data stored on the bank"s system.

3 Policy Statement

The bank shall strive for the preservation of the Confidentiality, Integrity and Availability of bank"s information assets pertaining to customer"s data, for safe & secure computing environment in order to build adequate trust & confidence in electronic transactions.

4 Objective

1. Define robust/cyber security framework to ensure adequate cyber security preparedness for addressing cyber risks. Identify the inherent risks and the controls in place to adopt appropriate cyber-security framework
2. Define cyber security measures/controls to ensure protection of bank"s and customer information and to maintain confidentiality, integrity and availability of the data across the data/information life cycle.
3. To design IT architecture in a manner that it takes care of facilitating the security measures at all times.

5 Governance of Cyber Security Policy

5.1 Roles and Responsibilities

Chief Information Security Officer (CISO) / Information Security Department

- Establish appropriate standards and controls and to direct the establishment and implementation of cyber security policy.
- Ensure the implementation, operation, monitoring, reviewing, maintenance and improvement of the Cyber Security policy and procedures by concerned Departments.
- Coordinate activities to ensure that information\cyber security audits and regulatory requirements are performed in an effective, efficient and timely manner.
- Review of information security incidents / crisis reported/identified and action plan adopted for mitigation/resolution.
- Ensure effective & efficient communication and coordination of cyber security requirements and decisions across the bank for information/cyber security related matters.
- Review and update this policy and get it approved from board. Bring new information/cyber security risk issues to the attention of the top management / Board and promote security best practices across the Bank.
- Maintain contact with regulatory bodies for information/cyber security related matters.

Information Technology Department

- To provide IT products support and services to the divisions and functions in accordance with the cyber security requirements of the bank
- Provide alternative solutions on industry practice to satisfy increased protection requirements
- Provide relevant support to other divisions on meeting cyber security objectives and plans
- Provide periodic metrics to evaluate the cyber security posture of the organization on a quarterly basis.
- Coordinate all activities necessary for compliance to the cyber security policy

- Oversee the execution of the cyber security planning at the functional level
- Maintain and update the relevant documents

Legal & Compliance

- Provide guidance and support in contract negotiations, and advise on legal issues (such as levels of liability), arising in connection with the contract and on regulatory requirements.

Business group

- Support Business / Divisions in meeting the bank"s requirements around cyber security risk management
- Help in identifying inherent risks in business/processes and communicating the same to IS department

Human Resource

- Ensure that all personnel are made aware of their information/Cyber security responsibilities
- Assign relevant information\cyber security trainings to staff.
- Provide guidance and support on the procedures that ensure compliance with applicable HR policies and employment regulations
- Address security requirements for all personnel before, during, and at termination or change of employment which include trigger access to system, email and physical access at time of on-board/off boarding of employee

Employees

- Comply with bank"s cyber security policy
- Practice reasonable care to protect their bank provided assets and access credentials
- Follow established cyber security incident reporting and escalation procedures

Third party

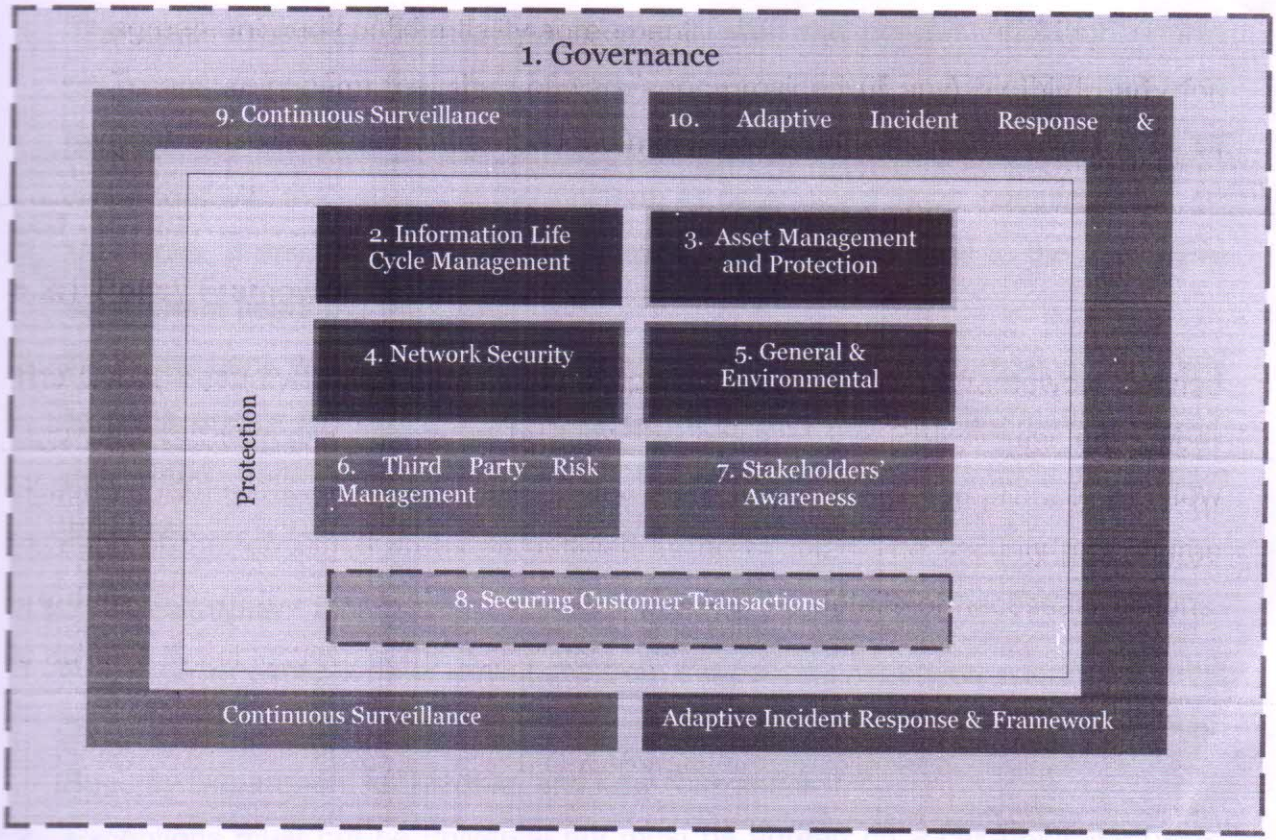
- Comply with bank"s cyber security policy

- Practice reasonable care to protect their bank provided assets and access credentials
- Comply with the terms and conditions as per the banks non-disclosure agreement and confidentiality agreement.
- To ensure/confirm that the software/apps provided (if any) by third party for Bank"s use are free from embedded malicious/fraudulent code.

5.2 Policy Governance

5.2.1 Policy Framework

The Cyber Security Policy is designed as per the cyber security framework defined below. The framework has been built on the basis of the RBI circular on "Cyber Security Framework in Banks" dated 2-Jun-2016 to provide a compliance overview for each of the functional areas as outlined in the circular. The security procedures are derived from the policy statements and provide the details of necessary actions to achieve the objectives of the policy statement.



5.2.2 Policy Owner

The ownership and responsibility for the maintenance of cyber security policy lies with the Chief Information Security Officer. CISO must be contacted in the event of any questions on the contents of this policy, suggestions for improvements, specific security recommendations and any other areas relating to the security of automated systems, data or information of the bank.

5.2.3 Policy Review and Approval

This policy document shall be reviewed at least annually by the Information Security Department or in events of any significant changes in the existing IS environment (internal/external) affecting policies and procedures. The policy owner must be responsible to make the changes to the policy document and to get approved from the Board.

5.2.4 Compliance

1. The bank expects all employees to comply with the policies. Violation or any attempted violation of the cyber security policy shall result in disciplinary action to be taken by the bank as per the extant guidelines. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation.
2. Violations, if any, of the cyber security policy must be reported to the respective department head and the CISO.
3. While the bank would like to respect privacy of its employees, it reserves the right to audit and/or monitor the activities of its employees and information stored, processed, transmitted or handled by the employees using bank"s information systems.

5.2.5 Exceptions

1. Approval for exceptions or deviations from the policies, wherever warranted, must be provided by CISO for High Risk items and Chief Manager – Information Security Department for Medium and Low Risk items.
2. Exceptions must not be universal but must be agreed on a case-by-case basis, upon official request made by the information asset owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at

any point of time. Exceptions to the cyber security policy may have been allowed at the time of execution/updating or on ad-hoc basis if needed.

3. All exceptions during implementation must be submitted by the concerned stakeholders to CISO or any other official (CM and above) of the Information Security team. All the exceptions are to be raised as per the bank"s cyber security policy exception form. The bank"s CISO must record the decision on the exception form.
4. For any ad-hoc exception required by a user, a request for exception must be submitted by the user through the exception form to the CISO. This request must be approved by the User Department Head / information asset owner.
5. The Information Security Department must review all exceptions, as the case may be, every year for validity and continuity. The summary of high severity exceptions allowed should be reported to Executive Director (In-charge of RMD/IS) on a quarterly basis.

5.2.6 Inquiries

Any inquiries relating to policy or the application of this policy should be referred to the CISO.

5.3 Performance Evaluation of the Cyber Security

5.3.1 Key metrics and effectiveness parameters for evaluating performance of Information and cyber security posture are maintained through IS Balance Score Card

5.3.2 The bank should continually improve the effectiveness of the Information and cyber security objectives through audit results, analysis of monitored events, corrective and preventive actions and management review.

6 Cyber Security Domains

6.1 Asset Management and Protection

6.1.1 Inventory Management of IT Assets

6.1.1.1 The bank should maintain an up-to-date inventory of IT assets. IT assets include systems and network, including disaster recovery systems and networks with their supporting facilities but limited to information, software, physical, services and people indicating their criticality.

6.1.1.2 To ensure confidentiality, integrity and availability of information, an information classification scheme designed by the bank should be adhere to.

6.1.1.3 The bank should secure information accessible by the internal teams, external agency and partners through approved methods, including information in electronic form, information in physical form and information during transit.

6.1.1.4 Any remote administration connections authorized by the bank should use strong authentication (typically two-factor authentication) as well as corresponding encryption methods (such as SSH, SSL and VPN) to secure communication traversing the network.

6.1.1.5 Bank should ascertain the risk related to critical information stored, transmitted, processed and accessed.

Related Procedures

- CBI ISMS-L2-8-Asset Management Procedure.

6.1.2 Secure Configuration

6.1.2.1 The bank should document minimum baseline security standards (MBSS) for IT platforms.

6.1.2.2 The MBSS should be tested before any major release on an IT platform.

6.1.2.3 The MBSS should be reviewed at least once annually and before major upgrade.

Related Procedures

- MBSS documents

6.1.3 Application Security Life Cycle

6.1.3.1 The bank should adhere to the secure coding practice as defined in the SDLC framework covering acquisition, design and development stages of software development practices.

6.1.3.2 Secure coding practices should be adhere to for all applications developed by bank or in collaboration with third parties.

6.1.3.3 The bank shall consider conducting source code review for critical business application to ensure that all internally developed as well third party applications are free from embedded malicious / fraudulent code.

6.1.3.4 Any vulnerabilities identified should be remediate in a timely manner. Source code review by an independent third party may also be considered, wherever necessary.

6.1.3.5 For outsourced third party and off the shelf application development, bank should seek undertaking from the service provider that the application is free from embedded malicious code and malwares.

6.1.3.6 The bank should capture security requirements at the initial and ongoing stages of system development/acquisition/implementation. At minimum, the security requirements must include access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling along with business functionalities.

6.1.3.7 Production and test environments should be segregated logically and physically.

6.1.3.8 Software/application development should cover threat modelling, incorporating secure coding principles and security testing.

6.1.3.9 Development procedures shall adopt the principle of defense-in-depth to provide layered security mechanism.

6.1.3.10 Software/application development team should incorporate security best practices for application development such as Open Web Application Security Project (OWASP).

6.1.3.11 The bank shall implement measures like installing a "containerized" apps on mobile/smart phones for exclusive business use that is encrypted and separated from other smartphone data/applications.

6.1.3.12 The bank shall implement measures to initiate a remote wipe on the containerized application.

6.1.3.13 Regression testing should be undertaken before new technologies are introduced in the bank"s environment for evaluating existing/evolving security threats.

Related Procedure

- CBI/ISMS/L2/14/ System Acquisition, development and maintenance.

6.2 Information Life Cycle Management

6.2.1 Data Leak Prevention

6.2.1.1 The bank should define data leakage prevention controls for information system and networks that process, store and transmit sensitive information.

6.2.1.2 Bank should implement DLP tool that is capable of detecting and preventing information leakages.

6.2.1.3 All confidential and critical data including information in use (e.g. User devices), information in motion (e.g. Network transmission) and information at rest (e.g. Data storage outside of Data centre) should be protected at all times.

6.2.1.4 Bank should define data leakage prevention controls mechanism including configuration, information classification, rules set based on users, roles, enforcement actions, monitoring capabilities and reporting.

6.2.1.5 Confidential, critical and other sensitive information of bank at vendor managed facilities should be protected.

6.2.2 Secure Mail and Messaging Systems

6.2.2.1 The bank should implement effective systems and procedures to ensure that e-mails are used as an efficient mode of business communication.

6.2.2.2 The bank should ensure that e-mail service and operations remain secure, efficient while communicating within intranet as well as through internet. (From ISMS)

6.2.2.3 Email specific server controls should be documented.

6.2.2.4 Security of email communication should be enhanced by use of disclaimer, hashes or encryption.

6.2.2.5 The bank should control permissible attachment types in email systems.

Related Procedures

- CBI/ISMS/L2/13/Communications Security Procedure

6.3 Network Security

6.3.1 Network security architecture should be documented at organizational level. Network security architecture should be updated as and when there are major changes in bank"s environment or at least annually.

6.3.2 Security architecture and standard security management principles should be applied in network devices configuration, vulnerability and patch management and change in routing table or setting of network devices.

6.3.3 Access to network"s device should be restricted to only bank"s authorized network staff and appropriate access control mechanism that support individual accountability and access restriction.

6.3.4 Bank should define standard operating procedures for all major IT activities.

6.3.5 Bank should ensure that certain events are logged and these logs are collected using various types of log collection software and infrastructure.

6.3.6 A central repository for the log collection should be established which would be used to generate alerts, based on established parameters.

6.3.7 Bank should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect its IT infrastructure from security exposures originating from internal and external source.

6.3.8 Bank should periodically conduct configuration review of network components.

6.3.9 Bank shall deploy mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

6.3.10 Bank shall implement solutions to automate network discovery and management.

Related Procedures

- CBI/ISMS/L2/13/Communications Security Procedure

6.4 General Environmental Controls

6.4.1 Environmental Controls

6.4.1.1 A cyber risk profile based on activities at various locations such as Administrative offices, branches, data centre and disaster recovery site, should be documented and maintained which help risk based decision and implementation of cyber security controls.

6.4.1.2 The bank should ensure that physical access to information processing areas and their supporting infrastructure (communications, power, and environmental) are controlled to prevent, detect, and minimize the effects of unintended access to these areas (e.g., unauthorized information access, or disruption of information processing itself).

6.4.1.3 Bank should monitor compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc.

6.4.1.4 The bank shall evaluate the cyber security risks and take up cyber insurance of an appropriate value from time to time. The need will be assessed on a yearly basis.

Related Procedures

- CBI/ISMS/L2/11/ Physical and Environmental Security Procedure

6.4.2 Preventing Execution of Unauthorised Software

6.4.2.1 The Bank should maintain central inventory of all software(s).

6.4.2.2 Bank should develop mechanism to control installation of unauthorized software in the organization.

6.4.2.3 Bank should track use of authorized / unauthorized software (if any) in the organization.

6.4.2.4 Bank should define procedures for granting and approving exceptions which at minimum should cover justification of exceptions, duration of exception and authority for approving.

6.4.2.5 Bank shall whitelist authorized applications / software / libraries, etc.

Related Procedures

- CBI/ISMS/L2/12/Operations Security Procedure

- CBI ISMS-L2-8-Asset Management Procedure

6.4.3 Removable Media

6.4.3.1 By default, access to removable media drives (USB ports, CD / DVD ROM drives, floppy drives) should be disabled.

6.4.3.2 Critical and sensitive information stored in removable media should be sanitized before disposal. Removable media should be disposed of securely and safely when no longer required.

6.4.3.3 Bank should deploy governing mechanism for use of personally owned and official mobile devices.

6.4.3.4 Bank should deploy mechanism to scan removable media for malwares, before granting any read /write access.

6.4.3.5 Bank should implement centralized policies through active directory or endpoint management systems to restrict use of removable media.

6.4.3.6 Exceptions for granting write access to removable media should be granted after approval of CISO and regular recertification process should be established, tracked and documented.

Related Procedure

- CBI/ISMS/L2/8/Asset Management Procedure

6.4.4 User Access Control/Management

6.4.4.1 The bank should deploy mechanism to protect data at rest and in transmit by implementing secure access controls to the bank"s network.

6.4.4.2 The bank should deploy mechanism in place to protect customer access credentials against data leakages.

6.4.4.3 The bank should provide access rights on a need to know basis for specific duration.

6.4.4.4 Users should not be granted administrative rights on end-user workstations /laptops.

6.4.4.5 The bank should implement centralized authentication and authorization system for accessing IT assets including but not limited to applications, operating systems, databases, network and security devices/systems, point of connectivity.

6.4.4.6 The bank should enforce strong password policy for all critical assets.

6.4.4.7 The bank should implement appropriate systems and controls to log and monitor administrative access to critical systems.

6.4.4.8 The bank should implement controls to minimize invalid logon counts and deactivate dormant accounts.

6.4.4.9 The bank should deploy measures to control installation of software on end user devices.

6.4.4.10 The bank should deploy controls to restrict use of VBA / macros in office documents.

6.4.4.11 The bank shall deploy controls to monitor abnormal changes in pattern of logon.

Related Procedure

- CBI ISMS/L2/9/Access Control Procedure

6.5 Vendor Risk Management

6.5.1 The bank should deploy vendor risk management process for identifying, assessing, mitigating and tracking cyber security risks associated with bank"s vendors.

6.5.2 The bank should carefully evaluate the need for outsourcing critical activities.

6.5.3 The bank should develop mechanism to assess security risks in outsourced and partner arrangements while on-boarding vendor, on-going services and during termination of services.

6.5.4 An audit plan should be developed and implemented for conducting vendor assessments.

6.5.5 Security controls and service levels of critical third parties should be assessed, reviewed and monitored by conducting vendor assessments.

6.5.6 The vendor should adhere to the bank"s security obligations, relevant legal and regulatory requirements relating to geographical location of infrastructure and intra border movement of data if any.

6.5.7 Sufficient background check of vendor should be carried out before deploying vendor.

6.5.8 Non-Disclosure Agreement (NDA) and security policy compliance should be mandated for all third party service providers.

Related Procedure

- CBI/ISMS/L2/15/Monitoring Supplier Relationships Procedure
- Outsourcing policy of the Bank

6.6 Stake Holder's Awareness

6.6.1 User / Employee/ Management Awareness

6.6.1.1 The bank should conduct periodic security awareness training programs to enhance awareness level among the customers, top management, employees, and outsourced staff, vendors.

6.6.1.2 Objective of the training program should be defined and measured to ensure that cyber security awareness improves.

6.6.1.3 Cyber security awareness program should be provided for staff members including new recruits on regular basis.

6.6.1.4 The bank should periodically update Board members on various cyber security related development.

6.6.1.5 Users/ Employees should be encouraged to report suspicious behaviour incidents etc.

Related Procedure

- CBI ISMS-L2-7-Human Resources Security Procedure.

6.6.2 Customer Education and Awareness

6.6.2.1 Customer education and awareness program should be designed and implemented.

6.6.2.2 Customers should be encouraged to report any phishing mails/websites, etc.

6.6.2.3 Customers shall be educated on the downside risks involved in sharing of their login credentials to any third party and the consequences arising of such situations.

6.6.2.4 Communication medium such as E-mail, SMS, banner, advertisements, Audio-Visual at branch offices should be used to improve customer cyber security awareness.

6.7 Securing Customer Transaction

6.7.1 Authentication Framework for Customers

6.7.1.1 The bank should implement mechanisms to provide positive identity verification to its customers.

6.7.1.2 Process and mechanism for securing customer identity information should be deployed.

6.7.1.3 Appropriate identification and authentication technologies should be deployed by the bank in order to act as identity provider for customer access to partner systems

6.7.2 Risk Based Transaction Monitoring

6.7.2.1 Fraud Risk Management System (FRMS) should be deployed by bank across each delivery channel for monitoring risk based transactions.

6.7.2.2 Continuous surveillance should be used to monitor and detect fraudulent or large transactions in the bank.

6.7.2.3 Immediate notifications through alternate channels like E-mail and SMS are provided to customers on transactions executed by customer across various means i.e. online, cheque, ATM.

6.7.2.4 For transaction above tolerance limit Call Back Verification (CBV) control shall be implemented.

6.8 Adaptive Incident Response and Cyber Crisis Management

6.8.1 Incident Response and Management

6.8.1.1 Bank should adhere to incident response procedures to respond consistently to attacks, minimize all loss, leakage or disruption during an attack.

6.8.1.2 Learnings from information security incidents should be documented and communicated to stakeholders. This information shall be used in improving the processes and systems to reduce recurrence and/or future impact of the security incident.

6.8.1.3 Employees and third parties shall report any observed or suspected information security weaknesses in systems or services through proper communication channels.

6.8.1.4 Bank should develop recovery strategies to ensure critical application systems are resumed within the agreed Recovery Time Objectives (RTO).

6.8.1.5 Management responsibilities should be assigned to ensure a quick, effective, and orderly response to information and cyber security incidents.

6.8.1.6 For information security incident that involves legal action (either civil or criminal), evidence should be collected, retained, and presented as per laws to conform to the rules laid down in the relevant jurisdiction(s).

6.8.1.7 Contacts with relevant authorities such as law enforcement agencies, regulatory bodies and national nodal agencies should be maintained.

6.8.1.8 The bank should have process for collecting and sharing of threat information from local, national or international sources following legally accepted/defined means/processes.

6.8.1.9 Advance cyber security incident like containing ransom ware/cyber extortion, data destruction, DDOS, etc. should follow cyber crisis management plan.

6.8.1.10 Cyber-attacks should be controlled by implementing security controls like shielding, quarantining the affected devices/systems.

6.8.1.11 Policy for aligning Security Operation Centre (SoC), Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy should be in place.

Related Procedure

- CBI ISMS-L2-17-Business Continuity Management Procedure

- CBI ISMS-L2-16-Information Security Incident Management Procedure
- Cyber Crisis Management Plan (CCMP)

6.8.2 Forensics

6.8.2.1 The bank should conduct preliminary investigation and evidence gathering and involve external forensics service on case to case basis.

6.8.2.2 The bank should have a forensic risk evaluation criteria to decide on incidents that qualify for forensics.

6.8.2.3 Security function must coordinate legal, HR.

6.8.2.4 Digital evidence related to information security incidents should be collected, stored and processed to facilitate necessary forensic investigation as per the applicable laws and regulations.

6.8.2.5 The bank should periodically and actively participate in external cyber drills.

6.8.3 Cyber Crisis Management

6.8.3.1 Cyber crisis management plan that includes identification, validation, activation, response, recovery and containment of cyber crisis should be documented, implemented and reviewed at least annually.

Related Procedure

- Cyber Crisis Management Plan (CCMP)
- CBI ISMS-L2-17-Business Continuity Management Procedure
- CBI ISMS-L2-16-Information Security Incident Management Procedure

6.9 Continuous Surveillance

6.9.1 Cyber SoC

6.9.1.1 The bank should set up a Security Operations Center (SoC) to enable continuous monitoring in order to combat against the changing threat landscape.

6.9.1.2 A cyber SoC should have capabilities to continuously monitor and provide analysis, forensics, intelligence and adequate response to safeguard critical systems.

6.9.1.3 Cyber SoC should have ability to protect critical business and customer information, demonstrate compliance with internal guidelines, country regulations and laws.

6.9.1.4 Cyber SoC should provide real-time/near-real time information on and insight into the security posture of the bank.

6.9.1.5 Cyber SoC should have ability to effectively and efficiently manage security operations by preparing for and responding to cyber risks, facilitate continuity and recovery.

6.9.1.6 Cyber SoC should have ability to assess threat intelligence and proactively identify/visualize impact of threats on the bank

6.9.1.7 Security event logging and monitoring should be enabled for all critical systems and applications.

6.9.1.8 Logs from applications and systems should be integrated with log aggregators deployed to allow sophisticated detection and analysis.

6.9.1.9 SoC should engage the cyber security incident and respond processes to provide analysis, forensics, intelligence and adequate risk mitigation actions to a cyber security incident.

6.9.2 Advanced Real-time Threat Defense and Management

6.9.2.1 The bank should implement security controls to provide robust defense against the installation, spread, and execution of malicious code at multiple points in the enterprise.

6.9.2.2 Mechanisms such as web security, anti-malware and continuous monitoring to detect advanced threats such as ransom ware, cyber extortion, data destruction, DDOS should be implemented.

6.9.2.3 Anti-Virus should be installed on all end points, servers and centrally managed for policy configuration management, virus definition updates.

6.9.2.4 The bank should implement and maintain preventive, detective and corrective measures across the enterprise to protect information systems and technology from malware.

6.9.2.5 Anti-Malware packages for operating systems should be deployed and definitions should be periodically updated.

6.9.2.6 Malware protection should be installed on all web-gateways, exchange servers and centrally managed for policy implementation.

6.9.2.7 The bank should implement whitelisting of internet websites/systems.

6.9.2.8 Bank should have threat intelligent mechanism that collect & analyses threat related information from different internal and external sources.

6.9.2.9 Based on the analyze threat intelligence, bank should share inferences and intelligence to regulatory bodies like RBI, IDRBT, CERT-In.

6.9.2.10 The bank shall deploy mechanisms to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web / internet gateway.

Related Procedure

- CBI ISMS-L2-12-Operations Security Procedure

6.9.3 Anti-Phishing

6.9.3.1 Mechanisms to manage events related to phishing/rouge applications should be implemented.

6.9.4 Vulnerability Assessment and Penetration Testing

6.9.4.1 The bank should periodically conduct vulnerability assessment and penetration testing (VA/PT) for all the critical systems.

6.9.4.2 Vulnerabilities identified should be remediated in a timely manner.

6.9.4.3 Penetration testing of public facing systems and critical applications should be carried out by professionally qualified teams.

6.9.4.4 Concerned Asset owners/team leaders should ensure that necessary remedial measures are implemented to close the findings detected by penetration testing.

6.9.4.5 VA/PT findings and follow up actions should be closely monitored by senior management as well as Information Security/ IT audit team.

6.9.4.6 The bank shall perform periodic red team exercises to test organizational readiness to identify and stop attacks.

6.9.4.7 The bank should periodically and actively participate in external cyber drills.

Related Procedure

- CBI-ISMS-L2-12-Operations Security Procedure

6.9.5 Patch/Vulnerability and Change Management

6.9.5.1 Updates and patches should be evaluated, prioritized and deployed. Consideration should be made of the risks associated with deployment of an update or patch.

6.9.5.2 The bank should establish processes to identify, track, manage and monitor the status of patches to operating system and application software in the bank"s network including data centres, disaster recovery centre, third party hosted sites and shared-infrastructure locations.

6.9.5.3 An implementation timeframe for each category of security patches shall be established to implement security patches in a timely manner.

6.9.5.4 Changes to bank"s applications should follow change management process to ensure that changes are sufficiently recorded and have been subject to appropriate approvals.

6.9.5.5 Requirements validation, coordination, testing and post-implementation arrangements should be appropriately undertaken for all changes to maintain integrity of the system.

6.9.5.6 The bank should periodically conduct vulnerability assessment and penetration testing exercises for critical internet facing web applications, servers & network components at the time of boarding the system, when there are significant changes and before the current valid penetration test expires.

6.9.5.7 The bank should periodically conduct application security testing for web applications at the time of boarding the system, when there are significant changes and before the current valid penetration test expires in environment closely resembling production environment.

6.9.5.8 Root cause of incident should be regularly tracked and vulnerabilities should be remediated by applying patches.

6.9.5.9 The bank should periodically evaluate the access device configurations and patch levels for ingress/ egress network connections with partner, vendor and service provider networks.

Related Procedure

- CBI-ISMS-L2-12.1-Application Version Change Control Procedure
- Patch Management Policy

2018

6.9.6 Audit Log Settings

6.9.6.1 The bank should implement and periodically validate settings for capturing appropriate logs/audit trails for all of each device, system software and application software.

6.9.6.2 Logs capture should include the following, at minimum:

6.9.6.3 System starting and finishing times

6.9.6.4 System errors or faults and corrective action taken

6.9.6.5 The name of the person/user-id making the log entry

6.9.6.6 The audit logs should be retained based on the record retention requirements

Related Procedure

- CBI ISMS-L2-9-Access Control Procedure

6.9.7 Maintenance, Monitoring and Analysis of Audit Logs

6.9.7.1 Logging should be enabled for critical devices, systems and application software.

6.9.7.2 Audit logs should uniquely identify users and their actions to assist in forensic auditing.

6.9.7.3 Stakeholders should be consulted for finalizing the scope, frequency and storage of log collection.

6.9.7.4 Bank should deploy a central repository for storing logs.

6.9.7.5 System and user activity logs should be monitored for anomalous behavior or activity.

6.9.7.6 Security logs are analyzed based on alerts generated from Security Incident and Event Management (SIEM) tool.

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

Related Procedure

- CBI ISMS-L2-9-Access Control Procedure
- CBI/ISMS-L-12-Operations Security Procedure.

7 Appendix 1 Wording

The following words have a specific meaning in the context of this document and subordinate documents.

Words	Meaning
„should"	It is mandatory to implement the action defined in the requirement, unless there is a business justification not to implement it, or it is currently a technological impossibility to implement it.
„should not"	The action defined in the requirement is prohibited, unless there is a business justification to allow it, or it is currently a technological impossibility to omit it.
„shall"	The action defined is not obligatory. The bank will try to implement it wherever feasible.

8 Appendix 2 Abbreviations

Abbreviation	Meaning
ASLC	Application Security Life Cycle
ATM	Automated Teller Machine
CBI	Central Bank of India
CCMP	Cyber Crisis Management Plan
CBV	Call Back Verification
CD	Compact Disk
CISO	Chief Information Security Office
DDOS	Distributed Denial of Service
DVD	Digital Versatile Disk
E-Mail	Electronic Mail
FRMS	Fraud Risk Management System
HR	Human Resource
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and communication technology
ID	Identifier
IS	Information Security
ISMS	Information Security Management System
IT	Information Technology
MBSS	Minimum baseline security standards
NDA	Non-Disclosure Agreement
OS	Operating Systems
OWASP	Open Web Application Security Project
PC	Personal Computer
PT	Penetration Testing
RBI	Reserve Bank of India
ROM	Read Only Memory
SDLC	Software Development Life Cycle
SMS	Short Message Services
SoC	Security Operation Centre
SIEM	Security Incident and Event Management
SSH	Secure Shell
SSL	Secure Sockets Layer
VA	Vulnerability Assessment

VBA	Visual Basics for Applications
USB	Universal Serial Bus
VPN	Virtual Private Network