Information Technology
&
Information Security Policy

Uttarakhand State Co-Operative Bank Limited

Haldwani, Uttarakhand

Effective Date: 03-06-2023

Reviewed on: 08-11-2025

Resolution Number: 01

Approved By: Administrator

THE UTTARAKHAND STATE CO-OPERATIVE BANK LIMITED
INFORMATION TECHNOLOGY & INFORMATION SECURITY POLICY

Document Definition: This document is designed to assist the Bank for Information Technology & Information Security Policy. The policy is designed in accordance to the NABARD Circular No. 33 dated 25thFebruary 2015 and Industry's Best Practices.

Board of Directors Meeting dated 08/11/2025 resolved that "The Uttarakhand State Co-operative Bank Limited" now being on the Core Banking Solution (CBS) platform provided by M/S. Wipro Limited, it is expedient to have a comprehensive Information Technology & Information Security Policy in order to safeguard Bank's Information System assets, maintain data Confidentiality, Integrity and Availability and to utilize resources efficiently.

Further Resolved that the following policy framework is hereby approved for implementation which will ensure protection for Bank's assets in accordance with the appropriate laws, regulations, and standards. All existing policies relating to personal, administration and other areas will apply equally in the computerized environment also.

THE UTTARAKHAND STATE CO-OPERATIVE BANK LIMITED
INFORMATION TECHNOLOGY & INFORMATION SECURITY POLICY

Contents

INTRODUCTION

1. Purpose

The purpose of this policy is to safeguard Bank's Information Technology (IT) and Information System (IS) assets, maintain data confidentiality, integrity and availability, to fulfill organizational goals effectively and utilize resources efficiently. This document provides the framework to ensure the protection of Bank's assets in accordance with appropriate standards, laws and regulations. All existing policies related to Personnel, Administration, Protection of confidential information and other areas apply equally to the computerized environment.

2. Scope

This policy applies to all the members of Board of Directors, Senior Management, Employees, Contractors, Vendors, and other Workers working for the Bank & their associates, including all personnel affiliated with third parties. This policy also applies to all applications and equipment that is owned or leased by the Bank.

3. General Use and Ownership

1. The Board of Directors has the responsibility for ensuring appropriate corporate policies, which set out the management responsibilities and the control practices for all the areas of information processing activities.
2. Senior Management is responsible for understanding risks to the bank to ensure that they are adequately addressed from a governance perspective.
3. While Bank's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the bank. Because of the need to protect bank's network, management

cannot guarantee the confidentiality of the information stored on any network device belonging to individual.

4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual areas are responsible for creating guidelines concerning personal use of Internet & Intranet systems. In the absence of such policies and if there is any uncertainty, employees should consult their supervisor or manager.
5. Any information that the information-owner considers sensitive or vulnerable should be password-protected in transit/storage.
6. Bank reserves the right to monitor and audit networks and systems on a periodic/ad-hoc basis to ensure compliance with this policy.

4. Unacceptable Use

The following activities are, in general, prohibited. However, employees may be exempted from these restrictions during their legitimate job responsibilities. Under no circumstances is an employee of the bank authorized to engage in any activity that is illegal under local, state, or regulator's prescription while utilizing bank owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by bank. Introduction of vulnerable/malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
2. Accessing confidential information like account password of which the employee is not an intended recipient and revealing to others or allowing use of our account by others.

3. Using the banks computing asset to actively engage in procuring on transmitting material that is in violation of 'sexual harassment' or 'hostile workplace' laws in the user's local jurisdiction.
4. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
5. Circumventing user authentication or security of any host, network or account.

5. Enforcement

Any violation of the policy by the employee should be deemed to be a breach of the service conditions or rules/regulations governing his/her conduct and the employee would be made liable to disciplinary action, up to and including termination of employment as per bank's management decision.

6. Policy Ratification

The entire Information Technology & Information Security Policy must be approved by the Members of the Board of Directors before it is implemented. As technology is dynamic, the policy needs an on- going review to keep pace with threats arising out of the new technology.

INFORMATION SECURITY POLICIES

1. Access Control policy and Procedures

Objective & Purpose

The purpose of this policy is to prevent unauthorized access to information systems and network systems. The Policy describes how access controls are applied by the bank, which covers all the stages where this policy should be applied.

Policy Statement

1. Bank must have scope for providing access to the all type of users, including bank staff, vendor, provider, etc. The scope for access control must include 1) Authorization to access any banks assets. 2) Type of authentication. 3) Remote access. 4) Provider and vendor's access. 5) Wireless access. 6) Direct network access. etc.
2. Bank must have password mechanism for every bank's asset like PCs, Servers, Networking devices, etc. Bank also must have access mechanism like biometric or proximity card to get entry in the critical areas.
3. Bank must provide user privileges to users according to their designation. It also includes the access to banks data.
4. Bank must revoke privileges after breaking the banks rule and regulations and revoke the privileges after user's task.
5. Bank shall keep record of every access to the bank's infrastructure.
6. To perform tasks, user may require access to various assets or data which may be above users' privileges, then banks must provide access and must revoke the access after completion of the task.
7. Sometimes user must perform task which are meant to do by other user, in that situation

bank must provide access and must revoke the access after roll completion.

8. Banks critical areas like server room, networking device access are only to those have privileges and have knowledge about them.
9. Bank must decide privilege level before providing or taking remote access. After completion of work bank must revoke extra privileges that are provided.
10. Bank must provide limited privileges to provider or vendor for access to banks assets. And bank must revoke the access if any rule breaking action found.
11. Bank must provide limited access through direct access through LAN. Access through LAN must revoke after time interval.
12. Bank must apply session management process for all type logical access for all applications, n/w devices, systems, etc. Session timeout must be up to 5 Min.
13. Password expiration limit should be 45 days. Failed login limit must be 3 times.
14. Global password policy should be applied in bank infrastructure or bank must create its own password policy.
15. Maker checker concept should be implemented in the bank infrastructure.

Procedure

1. Bank must decide what types of access and privileges to be provide for new user. New user must fill a form for access bank asset.
2. The users who are no longer required access to information systems and services must de-registration from the bank. All the access and privileges must revoke before de-registration.
3. User must fill out a form for CBS access and must give this form to user's immediate upper officer.
4. Bank must provide first login temporary password to all user for login which must be changed after first login.
5. Bank must check all users' rights time to time.

6. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exceptions

1. Exception to the policy will be handled on case-by-case basis and reviewed and approved by the CISO.
2. Any reason where access control policy cannot be able to implement must be record in detail with proper reasoning.

Roles & Responsibility

1. HR Department being responsible for registration and deregistration of user and total regarding process responsibility is completely goes to HR Department. All information should be check and validated before creation of user.
2. IS Officer being responsible for regular interval of making request list of scrapping for assets and submitted to CISO for proper approval. (Should access list be reviewed by IS officer for unused accounts and submitted to IS manager for deleting accounts, access.)
3. IS Manager being responsible for periodical review the scrapping request and take necessary action against that request. Change roll and change requirement for any user and its responsibility goes to IS Manager.
4. CISO being responsible for any kind of escalation.

2. Password Policy

Objective & Purpose

This policy is designed to protect the resources on the network by requiring strong password along with protection of these passwords and establishing a minimum time between changes to password.

Policy Statement

1. **Password Policy is applicable to following assets:**
    a. Servers
    b. Workstations/End Points
    c. Laptops
    d. Networking Devices (Details are available in Network Configuration Policy,Owned, Managed by Bank)
    e. CBS and Non-CBS Application
    f. DVR
    g. Confidential Documents and Files
    I. Mail and Messaging System (Details are available in Email Policy)
2. User must not disclose their password by any means.
3. System level password i.e., root, administrator, service account must be stored within in an encrypted format.
4. Privilege users should be provided with an alternate account with a password different to their standard accounts.
5. In case if password is compromised, immediate change in password should be done and should be informed to IT Team.
6. CBS & Non-CBS Password Policy Password of applications to be changed automatically in 30 days.
7. End Points, Servers Password for Servers and Workstations should be changed automatically in 90 days.
8. Other assets Password for other assets should be changed automatically in 90 days.
9. Other Password Policy Points Strong Password policy should be available with minimum 8 characters having Alphabet, Numeric, Special Characters, Upper and Lower case to be used.

10. Employees should be given training on Password Policy and use of Standard Password Policy through circulars, seminar etc. by bank.
11. Bank should ensure that Passwords must not be written down and left in a place where unauthorized access of password is possible.
12. Passwords must be completely unique and should not contain common name, dictionary words, default password etc. which may be easy to guess or crack.
13. Bank Employees shall use different passwords for all the applications, networking devices, workstation, servers, email etc.
14. Passwords must never be shared or revealed to anyone including Superior, Colleagues subordinate etc. which may lead to unauthorized use of password.
15. Sharing of password should be considered as serious disciplinary offence and will be dealt with accordingly.
16. Employees who have forgot password of CBS application, shall receive default password on mail by Superior/Branch Manager. The password shall be shared by Superior/Branch Manager to the employee personally.
17. Bank should ensure that, user should be blocked after inserting wrong password for three times i.e., Applications/ Servers/ N/w Devices/ Workstation.
18. Bank should ensure that all the passwords must be in encrypted format while it is at rest, transits, and processing.
19. The users of the bank shall ensure that password will not be save in the browser.

Procedures

1. Bank should assign IS Officer who shall create passwords for all the new IT assets which includes Severs/Workstation/Application/E-Mail/N/w Devices etc.
2. Once the password assigned by the IS Officer is handed over to the responsible user, the user must change the default password on immediate basis.

3. Bank should ensure that all the critical asset like ATM, networking devices, servers, applications, etc. password is available with higher responsible person, in case of IS Officer forgets the password and this password must keep in locker with sealed envelope.
4. If any IS Officer forgot the password for critical assets and which is available in sealed envelope, then proper authorization will be required from every regarding officer to open envelope. After opening that envelope, it must be back into locker with sealed and with regarding officer's acknowledgement letter and signed. And, proper logs should be maintained for this process.
5. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. Exception to the policy will be handled on case-by-case basis and reviewed and approved by the CISO.
2. Detailed reasoning shall be recorded for Exception to the policy.

Roles & Responsibility

1. It is user's responsibility that, to follow all the instructions provided by IT department which includes changing user's password after getting from IS Officer immediately.
2. IS Officer being responsible for regular base monitoring, review, and maintenance of all the records, logs, etc. and escalate in case of any emergency.
3. IS Manager being responsible for periodical review of all the records, logs, etc. and take necessary decision if required.
4. CISO is being responsible for any kind of escalation.

3. Antivirus Policy and Procedures

Objective & Purpose

The document is designed to reduce the likelihood of malware, or malicious code execution on the banks computing devices and network. The primary objective of this policy is to ensure Data, files, and resources can be protected by preventing such Viruses, malware, etc. in the network.

Policy Statement

1. Vendor should use Enterprise Antivirus Solution (licensed antivirus) in the Bank Network wherein appropriate controls are pushed from AV Server to all the Server or workstations.
2. Antivirus should be available on all the Servers, Systems, ATM machines, Passbook printing, Cheque Book printing, CDM etc.
3. Anti-virus should have the capability to manage all servers, endpoints centrally.
4. Only IS Officer/Vendor is authorized to make changes in the Anti-virus function.
5. Anti-Virus Server should remain active on 24*7*365 days and be installed at Bank DC wherein adequate cooling and Physical security is provided as per Industry's Best Practices.
6. **Antivirus Update:**

   Auto Update: Antivirus system should be updated on real time basis for the latest patches.

   Manual Update: If antivirus in the system cannot be able to update automatically then it must be updated manually and it is must be recorded.
7. **Scanning is Scheduled:** All the devices should be scanned on daily basis.
8. **Advance Signature:** Vendor should use advance Anti-Virus which works on the principle of Artificial Intelligence and behavior Monitoring etc. This advance signature solution provide protection against unknown threats in bank infrastructure.
9. Policy should be established in AV such that External Devices like USB, CD, External Hard disk etc. are not allowed on Bank Infrastructure.

10. IS Officer/Vendor having access to Anti-Virus console should address the user grievance within 1 hour.
11. IS Officer should review Anti-Virus policies on monthly basis and submitted to CISO for his review and necessary action, if required.
12. Alerts and notification are received to IS Officer on digital media i.e. Mail/SMS.
13. Any security alert and notification should be dealt on priority by IS Officer.
14. Anti-Virus should have capabilities of block unwanted website, automatic virus removal, safeguard from email scams, protect against ransom ware attack, key logger protection.
15. Anti-Virus should have capabilities to provide functionality of Data Leak Prevention on host for data at rest or moving.
16. In the event of Virus infection, a root cause analysis should be done by Bank/Vendor with help of External Experts.
17. Security Audit of AV system shall be conducted periodically by External Vendors.
18. All application before installation in the bank infrastructure must be scan by using AV for viruses, malwares etc.
19. Any vendor who wants to demonstrate anything in any type of storage device or over system will not allow to connect banks n/w or to insert storage device in banks system. Vendor should have to demonstrate on vendor's system.
20. The system which has an internet connection or USB allowed must be isolated form banks m/w. So, the chances of injecting viruses or malwares will be less.

Procedures

1. Bank should allocate dedicated IS Officer who would be responsible for log review, policy review/updating/changes/modification/deletion, grievance resolution on real time basis.
2. Change Management process should be followed in case of replacement of Anti-Virus and/or any vital changes made in the existing system.

3. Bank should impart adequate training to Users about AV functionality and actionable on any circumstances; if required.
4. Report on regular basis for alerts and notification to be prepared and submitted by IS Officer to CISO.
5. All files must be scanned before and after download from emails/ any other source.
6. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. A formal exception document should be approved by CISO.
2. Any Server or Workstation where AV is not present needs to be recorded in the Anti-Virus Exception file with detailed reasoning.

Roles & Responsibility

1. User is responsible to follow all the instructions provided by IT department including scanning before downloading, USB scanning, etc.It is user's responsibility, if anything found suspicious on their system must be reported to IT department immediately.
2. IS Officer being responsible for daily base monitoring, review and maintenance of all the records, logs, passwords, change management etc. and escalate in case of any emergency.
3. IS Manager being responsible for periodical review of all the records, logs, passwords, change management etc. and take necessary decision if required.
4. CISO being Responsible for any kind of escalation.

4. IT & IS Audit Policy and Procedures

Objective & Purpose

The objective of the IT & IS Internal & External Audit Policy is to ensure Integrity, Confidentiality & Availability of information and resources and to monitor all security measures are in conformance with Bank policy and Regulatory guidelines.

Policy Statement

1. IT Inspection of the branches should be carried out periodically **(once in a year)** by internal IT staff.
2. Bank should get the IS Audit carried out as per the NABARD guidelines by a qualified technical audit firm.
3. The frequency of IT audit should be annual. In addition, an information security review will be done when significant changes to the security implementation or IT environment occur.
4. Audit scope should be in accordance to NABARD circular:
   a. NB.DoS.HO.POL/3634/J-1/2014-15/33 dated 25th February 2015
   b. NB.DoS.Pol.HO/794/J-1/2019-20/134 dated 21st May 2019
   c. Industries Best Practice
5. The appointment of independent third parties for information security audits and IT Compliance reviews will be done with Management approval.
6. Responsibility will be assigned for all corrective actions and will be documented.
7. IS Audit should cover all the critical assets at Head Office and Branches, Data Centre and other critical locations.
8. IS Audit should be completed before Statutory Audit so that the comments of IS Audit report may be incorporated in Statutory Audit.
9. Manager IT should consolidate various reports of the audits carried out as per the audit plan. Key findings as a result of these will be presented to the Audit Committee.

10. The compliance of IS Audit to be furnished within one month from date of issuance of Audit Report.

Procedures

1. Selection is as per the Vendor Management Policy. Experience of Audit firm in the domain and qualifications of Auditors are the major indicators for selection purpose.
2. Few employees based on their experience are assigned role of Internal Audit from Bank IT Department.
3. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exceptions

1. A formal exception document should be approved by CISO.
2. Any reason where IT-IS policy cannot be able to implement, must be recorded in detail with proper reasoning.

Roles & Responsibility

1. IS Officer being responsible for consolidating all the audit queries and resolving/escalating such queries. Submitting compliance report to CISO for review purpose.
2. IS Manager being responsible for review and closure of compliances for the audit conducted.
3. CISO being responsible for any kind of escalation.

5. User Awareness & Training Policy & Procedures

Objective & Purpose

This policy specifies an Information Security Awareness & Training Program to inform and motivate all employees regarding their Information Risk, Security, Privacy and Related Obligations.

Looking at the dynamism, it is important to impart training to various departments, designation etc. so that they may use technology and security in alignment to Bank infrastructure.

Policy Statement

1. Bank should ensure that all employees achieve and maintain at least a basic level of understanding on security matters i.e., General Obligations under various Information Security Policy, guidelines, regulations, standard of ethics and acceptable behavior.
2. Additional training should be imparted to IT/IS Team with specific obligations towards Information Security.
3. Bank should ensure regular base user training according to the job requirement.
4. After completion of training, feedback shall be collected from participants who have attended the training program.
5. Bank shall strive to provide training to its employees on regular time frame.
   Bank shall ask Internal Team member or External Experts for training the users.
6. Bank shall send its employee for outdoor and specialized training conducted at NABARD, BERDS, OEM etc.
7. Bank should impart training to customer through Display over website, branch premises, tool kit, ATM centers etc. and personally by bank.
8. Bank should impart training to its Board Member on the subject which they are required to know as per Regulators guidelines.

9. Bank should have records of participants who have attended training which may be produced to Management, regulator whenever required.
10. Any new change in technology and process shall be imparted to employees before implementation of the same.
11. Induction training shall be provided to all the new employees.

Procedures

1. IT Department shall conduct regular training for CBS & other applications as a part of User Awareness & Training not less than three months. Bank IT Team should try and provide practical demonstration for the applications.
2. IT Department shall conduct training on Information Security as a part of the user awareness not less than three months.
3. IT Department shall identify External Experts and invite for imparting training to its users, in case Bank is unable to identify internal trainer.
4. Bank IT Team shall send its employee for outdoor and specialized training which may help the user to perform his or her duties in a better way.
5. This feedback shall help Bank to provide better and user-friendly training in the future. Also, the feedback shall give an insight about the areas to focus while giving training.
6. With increase in Cyber-attacks and threats in today's world, Bank shall educate its customers.
7. Bank has arranged for Customer Tips and presented the same on all the ATM rooms giving guidelines to customer about Do's and Don'ts while using ATM.
8. Users should immediately report any suspicious activity to IT Department i.e. File missing from the system, suspicious system activity etc.
9. Users shall be advised not to take any action against system failure, repairs by his own. Always the user should report the matter to Bank IS Officer.

10. Bank should ensure that all the users are given proper training to use Physical and Environmental controls available in the bank i.e. CCTV, Fire Extinguishers, Smoke Detector, Panic switch etc.
11. Bank should ask the users to drill the Physical and Environmental controls on regular intervals for Head Office, Branches and regional offices. The report shall be submitted by Users to Bank IS Officer for his records purpose.
12. The bank shall have a record of the awareness trainings that has been conducted in the bank.
13. Bank should have records of participants who have attended training which may be produced to Management, regulator whenever required.
14. The records must include: Training topic, date and time of training, location of training, Trainer Name, Internal/External, Participant Name, Designation, Signature etc.
15. Management shall review the training records and feedback form on a periodical basis and guide the IT Department to improvise, if required.
16. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. Exception to the policy will be handled on case-by-case basis and reviewed and approved by the CISO.
2. Detailed reasoning shall be recorded for Exception to the policy.

Roles & Responsibility

1. IS Officer being responsible for regular base monitoring, review, and maintenance of all the records, logs, etc. and escalate in case of any emergency.

2. IS Manager being responsible for periodical review of all the records, logs, etc. and take necessary decision if required.
3. CISO being responsible for any kind of escalation.

6. Problem and Incident management policy

Scope:

This document covers the Problem/Incident Response process for all identified problems and security incidents, with the intent to preserve confidentiality, integrity, and availability of Information and the equipment, devices or services containing or providing such Information.

Meaning of Problem management: Process of detecting, reporting, resolving the **Information Technology** related problems faced by the organization which ranges from day-to-day problems (e.g., Fault in working of printer) to bigger problems, but it would not include the events that has the potential to compromise the security of the organization.

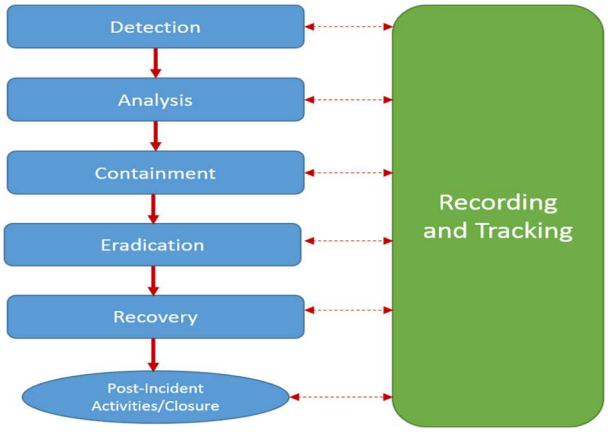
Meaning of Incident management: Process of detecting, reporting, assessing, responding to, dealing with, and learning **from Information Security** Incidents that occur in our organization.

Process:

The following activities will be covered in the process for Problem/Incident management: -

- Detection
- Analysis
- Containment
- Eradication
- Recovery

•Post-Incident Activities



The Problem/Incident Response process is considered complete once Information confidentiality, integrity, and/or availability are restored to normal and verification has occurred.

A. Detection:

1. In the detection phase the internal or external entity, identifies an event to determine that whether it belongs to Problem management or to Incident management process. It may be the result of a potential exploitation of a Security Vulnerability or a Security Weakness, or that may be the result of an innocent error or of any Hardware/software malfunctioning and immediately upon observation or notice of any suspected event, Personnel shall use reasonable efforts to promptly report such knowledge and/or suspicion to the Information Security Department/ Information Technology Department.

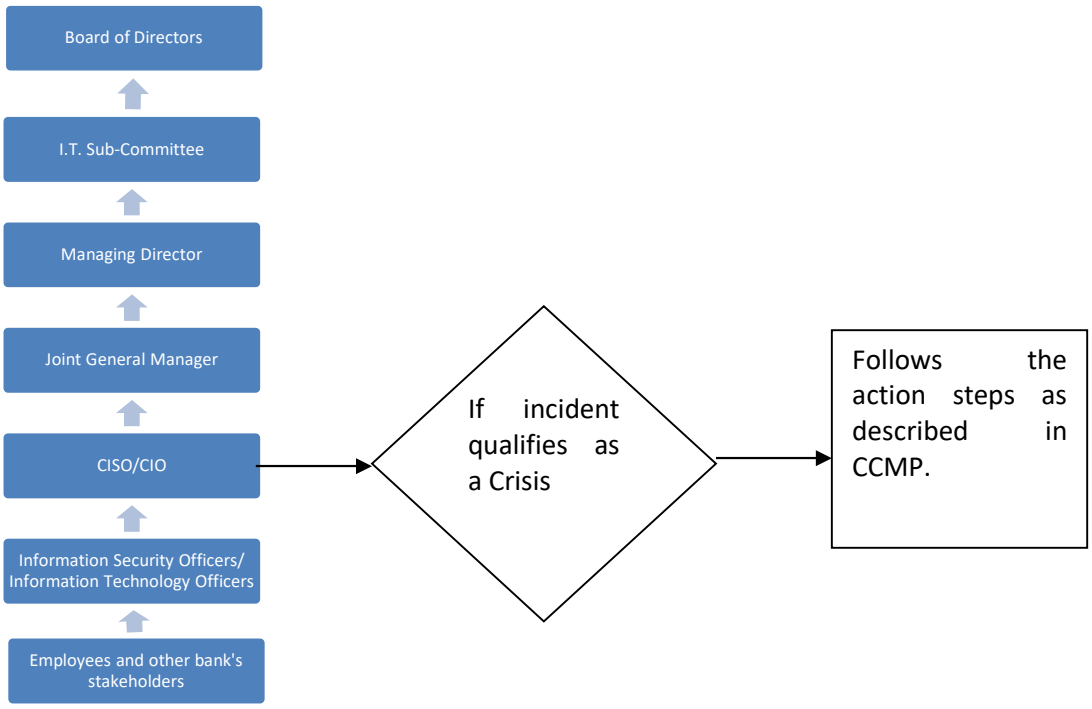
2. A Security Event may be discovered in many ways, including the following:
    - Observation of suspicious behavior or unusual occurrences;
    - Lapses in physical or procedural security;
    - Information coming into the possession of unauthorized Personnel or Third Parties.

- Information inappropriately exposed on a publicly facing website.

B. Analysis:

1.The initial response to detection of an event is typically the Analysis Phase. In this phase the person determines whether an event is an actual Security Incident or a Problem Incident. To determine if an event is a Security Incident/ Problem Incident the experience and subjective understanding of the person will come into effect.

2.Depending upon the severity of the incident the first respondent will escalate the incident as per the following escalation matrix:



C. Containment:

1. The Containment Phase mitigates the root cause of the Problem/Incident to prevent further damage or exposure. This phase attempts to limit the impact of a Problem/Incident prior to an eradication and recovery event. During this phase, the personnel may implement controls, as necessary, to limit the damage from a

Problem/Incident. If an Incident is determined to be caused by innocent error, the eradication phase may not be needed.

D. Eradication:

1. The Eradication Phase is the phase where vulnerabilities causing the Problem/Incident, and any associated compromises, are removed from the environment. An effective eradication for a targeted attack removes the attacker's access to the environment all at once, during a coordinated containment and eradication event. Although the specific actions taken during the Eradication Phase can vary depending on the Security Incident, the standard process for the Eradication Phase shall be as follows:

- Determine the symptoms and cause related to the affected system(s).
- Eliminate components of the Security Incident. This may include deleting malware, disabling breached user accounts, etc.
- Strengthen the controls surrounding the affected system(s), where possible (a risk assessment will be performed, if needed). This may include the following:
  - Strengthening network perimeter defenses.
  - Improving monitoring capabilities or scope.
  - Remediating any security issues within the affected system(s), such as removing unused services or implementing general host hardening techniques.
  - Conduct a vulnerability assessment to verify that all the holes/gaps that can be exploited have been addressed.

E. Recovery:

1. Although the specific actions taken during the Recovery Phase can vary depending on the identified Problem/Incident, the standard process to accomplish this shall be as follows:

- Installing patches.
- Rebuilding systems.
- Changing passwords.
- Restoring systems from clean backups.
- Replacing affected files with clean versions.

F. Post Incident Activities:

1.This activity involves continual education and awareness so that repeated Problem/incidents do not take place. It also includes steps to inform to any agency about the Problem/incident. This activity also involves Logging and documenting of the Problem/incident occurred and the steps taken to mitigate it. If the Problem/Incident is not severe then only logging of the same would suffice but if it is severe then proper and complete documentation of it is to be done. The severity of the event is based on the subjective judgement of the organization.

The Incident Management Register: The bank shall have the records for the incidents that has been occurred in the bank in the incident management register.

Roles & Responsibility

Bank's Responsibility:

1. The bank must use the escalation matrix for any security incident and CISO will decide if the incident qualifies as a cyber crisis.
2. Bank must perform Root Cause Analysis if any security incident occurs and eradicate the security issue and take appropriate measures make sure the security incident never happens again.

3. After Eradication, Recovery phase Bank must conduct a review of affected systems by industry experts verifying that the affected systems are now clean and all the gaps are patched which were used to exploit the vulnerability.

1. All Users are responsible to:

a) Report suspected information security incidents and weaknesses promptly so that appropriate action can be taken to minimize harm.

2. IT Officer is responsible for:

a) Monitoring the BANK systems, users, Information Technology (IT) infrastructure to identify suspected breaches.

b) Investigate into reported incidents and respond with appropriate action.

c) Maintenance of IS incident management process, and incident register which shall be available to the auditors at any point of time, all incident/weakness reported are recorded.

d) Is responsible for reporting, investigating, and taking appropriate action to address breaches of physical security and suspected attempts to gain unauthorized access to secure areas.

3. GM (IT)/CISO is responsible for:

a) Responding to incidents with appropriate actions

b) Responsible for reporting incidents observed on IT infrastructure to 2.like NABARD C-site Cell, CERT-IN, RBI.

4. CEO/MD is responsible for:

a) Is responsible for ensuring the availability of all required resources for incident management.

b) Ensuring staff have access to and understand the obligations under this policy at the time they are given access to bank systems.

c) Reporting breaches of this policy to various stakeholders i.e., regulators; customers; vendors etc.

Vendor's Responsibility:

1. Vendor must inform the bank as soon as possible, if any suspicious event/activity occurs.
2. Vendor is also obligated to follow the Cyber Crisis Management Policy put up by the Bank.
3. Vendor must perform Root Cause Analysis if any security incident occurs and eradicate the security issue and take appropriate measures make sure the security incident never happens again.
4. After Eradication, Recovery phase vendor must submit report to the bank submitted by industry experts verifying that the affected systems are now clean and all the gaps are patched which were used to exploit the vulnerability.

Glossary:

Security Event: An identified occurrence of a system, service or network state indicating a possible breach of information security policy, a possible exploitation of a Security Vulnerability or Security Weakness or a previously unknown situation that can be security relevant.

Security Incident: A single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security.

Crisis: An incident or problem or an event which has the severity or the potential to disrupt the organization and hamper the production environment of a considerable time span and may also bring down the reputation of the organization.

Problem: For the purpose of this Policy only, problem means any occurrence of an event which interrupts the functioning of Hardware, software, network, data, and other related IT resources but does not include events which can cause harm to the Confidentiality, Integrity, Availability of the IT resources.

7. Network Security Policy

Objective & Purpose

The objective of this policy is to ensure the security of the Bank Network and to do this the Bank will ensure the protection of network from unauthorized disclosure and accidental modification. The objective is also to ensure the accuracy and completeness of the Bank IT Asset.

Policy Statement

1. Bank should ensure that Network Architecture must be designed in a manner that ensures security traits i.e., Confidentiality, Integrity, and Availability in the Bank Infrastructure.
2. **Network Architecture Diagram:** Bank should ensure that Network Architecture Diagram is in place and should be in line with existing bank infrastructure. The network diagram should be reviewed and approved by CISO.

3. **Primary Connectivity:** Bank should use dedicated MPLS connectivity for Banking Operations. Any other Network connectivity like Wi-Fi and other medium are strictly prohibited.
4. **Secondary Connectivity:** As a backup, bank should ensure for secondary connectivity in the Bank Infrastructure. In case the primary MPLS connectivity goes down, the secondary connectivity should be switched ON automatically and can be put in use.
5. **Switch:** Vendor should use Core Manageable switch at Data Centre, which has the capability of controlling logical and physical access and logging.
6. **Firewall:** Bank should use Firewall in Bank network perimeter and all the outbound and inbound traffic would be routed through Firewall.
7. **Router:** Bank should use Router for packet forwarding between two networks.
8. **Zoning & Segmentation:** Bank should establish adequate zoning and segmentation for Bank Critical Assets likely ATM; RTGS/NEFT Systems, CTS Systems; Bank IT Systems, CBS Systems, Mail and Messaging Systems etc.
9. **Dematerialized Zone:** It should be implemented for public facing Applications/Servers.
10. **Default Username/Passwords:** The default username/passwords of all the network devices/systems should be changed after installation.
11. Bank IS Person should ensure that Password should be kept on encrypted mode.
12. Bank should use SSH for remote services. Also, Bank should restrict Telnet service on console.
13. Bank should ensure that all connections to external network and system via VPN have documented and approved by CISO.
14. Bank should ensure following security configuration for secure hardening of networking device:

    a. Network Time Protocol

    b. Console Session Timeout

    c. HTTPS session timeout

d. Filter rules both for inbound and outbound traffic

e. Auxiliary Port should be disabled etc.

15. Bank should implement appropriate measures for both Host based and Network Based Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) implementation.
16. Bank should establish Proxy Server for public facing services.
17. IS Officer should review Network Architecture Diagram and Network Devices Policies on periodical basis. The same shall be approved by CISO.
18. In the event of incident due to Network Security breach, a root cause analysis should be done by Bank with help of External Experts.
19. Security Audit of Network Diagram and Devices shall be conducted periodically by External Vendors.
20. Bank must use network monitoring tool for monitoring banks entire network, which inform which connectivity is currently down, band width uses, etc.
21. Bank do not allow any third party or personal devices to connect in bank network.
22. Bank and vendor must maintain inventory for networking devices which includes warranty, guarantee, serial no, subscription etc.
23. Data must be encrypted if it is at rest or encrypt channel when it is travel.
24. Remote access should be given via encrypted channel to anyone with proper permission of regarding authority.
25. Bank shall have the baseline configuration document for configuring the networking devices.
26. Bank shall conduct secure configuration audit for all networking devices for ensuring the configuration set up for networking devices.

Procedures

1. **Approval Process:** Any network device should only be deployed only after understanding of its design and configuration. On proper authentication and approval

from IS Officer and CISO, the network devices should be deployed in the Bank's Network. Any exception in existing policy/procedures needs to be recorded in the Network Security Exception file with detailed reasoning.

2. Any new policy establishment and/or changes in Network Infrastructure by Bank IS Officer or by external vendor should be a part of change management process.
3. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty

Policy Exception

1. A formal exception document should be approved by CISO.
2. Any exception in existing policy/procedures needs to be recorded in the Network Security Exception file with detailed reasoning.

Roles & Responsibility

1. IS Officer being responsible for periodical base monitoring, review of Networking Devices and maintenance of all the records, logs, change management etc. and escalate in case of any emergency
2. IS Manager being responsible for review of all the records, logs, change management etc. and take necessary decision, if required.
3. CISO being responsible for any kind of escalation.

8. Physical, Environmental and General Controls Policy

Objective & Purpose

The Objective is to prevent unauthorized physical access, damage to Bank's Information and Assets.

Policy Statement

1. Information processing facility must be protected by a physical security perimeter.
2. IS Officer must ensure appropriate controls are in place to establish secure areas.
3. Sensitive Information must be protected in any case.
4. **Physical controls at Branch level:**

   Following controls should be established and put in place at Branch level.

   a. CCTV

   b. Guards

   c. Visitor Register

   d. Networking Device Cabinet
5. **Physical controls in ATM:**

   Following controls should be established and put in place in ATM Room

   a. CCTV

   b. Guards
6. **Physical controls in Data Center:**

   Following controls should be established and put in place in Data Center managed by Vendor.

   a. CCTV

   b. Biometric

   c. Server Rack

   d. Visitor Register

   e. Networking Device Cabinet
7. **Physical controls in DR Set up:**

   Following controls should be established and put in place in Near DR Setup by Vendor.

   a. CCTV

   b. Biometric

   c. Server Rack

d. Visitor Register

e. Networking Device Cabinet

Environmental Control

1. **Environmental controls at Branch level:**

   Following controls should be established and put in place at Branch level.

   a. Smoke Detector

   b. Panic Switch

   c. Fire Extinguisher

2. **Environmental controls in ATM:**

   Following controls should be established and put in place in ATM Room.

   a. Smoke Detector

   b. Fire Extinguisher

   c. Proper Cooling System

3. **Environmental controls in Data Center at vendor site:**

   Following controls should be established and put in place in Data Center.

   a. Smoke Detector

   b. Fire-Extinguisher

   c. VesdaSystem (Temperature, Water Leakage, Fire Detection System, Rodent System, Alert is available via email)

   d. Proper Cooling System

   e. Food is not allowed in the Data Center

   f. Fire Doors Exit Available

   g. Power Supply is available

   h. Dry Pipe is using

   I. Raised Floor

   j. Toughened Glass (High in strength, More Secure compare to Ordinary Glass

4. **Environmental controls in Data Center at vendor site:**

   Following controls should be established and put in place in Data Center

   a. Smoke Detector

   b. Fire Extinguisher

   c. VesdaSystem (Temperature, Water Leakage, Fire Detection System, Rodent System, Alert is available via email)

   d. Proper Cooling System

   e. Food is not allowed in the Data Center

   f. Fire Doors Exit Available

   g. Power Supply is available

   h. Dry Pipe is using

   I. Raised Floor

   j. Toughened Glass (High in strength, More Secure compare to Ordinary Glass

5. Bank should ensure that CCTV is installed at Banks strategic and critical locations.
6. **Recording History:** Bank should ensure 90 days DVR recording which should be kept in record.
7. **Asset Movement Register:** A register indicating IT Asset movement should be maintained in the Bank premises wherein details for movement must be logged having minimum details i.e. Date; Time; Reason; User; Approving Authority; Signature (Asset moved by and branch officials). Prior approval of concerned IS Officer shall be taken for such asset movement.
8. Cabling should be properly concealed. Cables in ATM Centre should be underneath the floor.
9. Power and Telecommunication cabling carrying data must be protected from interception or damage.

10. **Tagging & Labelling:** Adequate tagging should be done for cables in Bank infrastructure. These tagging can be useful for understanding of the services run on which cables and during the time of emergency and contingency.
11. Equipment must be correctly maintained to help ensure integrity and availability of sensitive information and assets.
12. In the event of incident due to lapses in Physical, Environmental and General Controls, a root cause analysis should be done by Bank with help of External Experts.
13. Security Audit of Physical, Environmental and General controls shall be conducted periodically by External Vendors.
14. UPS/ generator must be available with the bank in case of any power failure to continue banks production. Proper ventilation must be present in UPS/ Generator room.
15. Bank must have blueprint for power and data cabling.
16. Bank must use MCB and ELCB for preventing sparking or fire outrage.

Procedures

1. **User Awareness:** Bank should provide the training to all the users for proper usage of environmental control.
2. **Drill Reports:** Drills of various physical & environmental control of assets shall be done on periodical basis. The reports of such drills should be shared with the IS Officer for his further action.
3. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. A formal exception document should be approved by CISO.
2. Any exception in existing policy/procedures needs to be recorded in the Physical & Environmental Controls Exception file with detailed reasoning.

Roles & Responsibility

1. IS Officer being responsible for periodical base monitoring, review of Physical, Environmental & General Controls and maintenance of all the records, logs, change management etc. and escalate in case of any emergency.
2. IS Manager being responsible for review of all the records, logs, change management etc. and take necessary decision, if required
3. CISO being responsible for any kind of escalation.

9. Information Asset Classification and Handling Policy

Purpose

All IT assets used by bank are owned or leased by bank. A large amount of company's internal, confidential & critical information is created and stored or supported by these IT assets and systems. Bank will ensure all feasible efforts to maintain appropriate access control and availability of these assets. This policy is developed for classification of the IT Assets and systems so that appropriate controls can be implemented based on the threat to the asset.

The purpose of this document is to provide guidance to Bank businesses on (a) classifying information generated or used by the Company; and (b) recommended ways to label, store, transmit, and dispose of such information, depending on its classification.

Policy Details

Scope

All IT assets and systems which includes but not limited to Desktops, Laptops, Servers and network components, software assets (including applications), power supply, UPS, HVAC (Heat, Ventilation, Air conditioning units), Fire detection and suppression systems.

This policy applies to employees, contract employees and consultants at Bank, including all personnel affiliated with any third parties. This policy applies to all information that is owned or leased by Bank

Policy Statement

Each IT asset of Bank handled by its users and / or administrators, and support staff will be classified and labeled either as highly critical or moderately critical or non-critical asset. Access control to these systems will adhere to the guidelines set in the access control policy.

Asset Classification

- **Highly Critical:**

  Information of the highest sensitivity, which, if mishandled may cause substantial damage to the bank's business / image e.g., merger/acquisition information, strategic business plans, customer transaction information, etc.

- **Moderately Critical:**

  Information, which, if mishandled, may cause moderate damage to the bank's business / image e.g., departmental budget plans, customer information, personnel information, internal memos, telephone books, organization charts etc.

- **Non-Critical:**

  Information, which, even if mishandled, may not cause damage to the bank's business / goodwill e.g., annual report, already published product information brochures, etc.

Asset Labeling and Handling

- The assets shall be classified and clearly labeled so that all users are aware of the ownership and classification of the asset.
- From the time when IT asset is acquired until it is destroyed or declassified, it must be labeled (marked) with a sensitivity designation.
- Information and its related IT assets shall be processed and stored strictly in accordance with the classification levels assigned to those assets.
- Access to the information assets shall be the responsibility of a designated owner or custodian.
- Exception: In exceptional cases asset labeling shall not physically possible for some items such as (small devices, Tube lights, smoke detectors etc.), in such cases asset inventory of such items shall be maintained in asset list.

Information Asset Classification

All information on the Bank Information Systems shall be classified based on its importance to its business and to its image. The classification of information may change over a period and necessary controls shall be applied.

Definitions

- **Information**: Any information, which has value, usefulness and association to bank.
- **Information Owner**: Any person or persons, individually or collectively responsible at Group Head levels for any subset of the data or the information on the Organizations Information Systems.

- **Information Custodian**: Any person or persons, individually or collectively responsible to perform regular administrative tasks on the information delegated by the information owner or Information Security Task Force.

Information ownership and accountability

The CISO shall designate a person or group of persons to be responsible for an asset. Such person or group of persons shall be the Asset owner. Ownership of the asset remains with the owner at any level however, different persons, processes shall be held accountable for compromising the confidentiality, integrity and / or availability of information, hence detective controls shall be in place wherever possible.

Classification of information

Information classification shall be classified based on confidentially, integrity and availability by their respective owners into any one of the following:

(a) Confidential

(b) Restricted

(c) Company Circulation

(d) Public

The above classifications are defined as follows:

(a) Confidential

This classification applies to the sensitive organizational or departmental information that is intended strictly for use within limited group of individuals within the department. Its unauthorized disclosure and / or access could seriously and adversely impact the organization and will have to be treated with care. This type of information

shall be handled using controlled access to address confidentiality.

(b) Restricted

This classification applies to sensitive business information that is intended strictly for use within the Group. This information shall be exempted from any disclosure and / or access rules or other applicable laws or regulations. Its unauthorized disclosure and / or access could seriously and adversely impact the Group and its stakeholders, its business partners, and / or its customers and will have to be treated with care. Access shall be granted only to group members or authorized individuals.

(c) Company Circulation

This classification applies to information that is intended for use within the Department. Its unauthorized disclosure could moderately impact the Organization and / or its employees.

(d) Public

This classification applies to all other information that does not clearly fit into any of the below three classifications. While it's unauthorized, disclosure probably may not be against the policy and it is not expected to seriously or adversely impact Organization, employees, and/or customers.

Roles and Responsibilities of Information Owners

The Information owner shall:

(a) Maintain an appropriate level of protection, physical and / or logical, for the information.

(b) Take prior approval of the CISO or Group Head before sharing information.

(c) Review the information classification periodically.

(d) Ensure availability of information at all times and circumstances.

(e) Periodic review of access control.

The Information custodian shall:

(a) Perform regular backup and data validity testing activities.

(b) Perform data restoration from backups periodically.

(c) Implement access control as defined by information owner.

(d) Perform regular administrative tasks.

Communication of Policy Details

This policy and relevant specific policies, procedures shall be published on Company's Intranet and communicated to employees and relevant external parties.

Periodical Review

- The information security policy shall be reviewed on yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
- The Information Security Forum would review this Policy, the compliance and implementation status, effectiveness of controls and their implementation, considering Internal Audit Reports, Incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements to Apex Committee.

Disciplinary Action

- Any non-compliance with these requirements shall constitute a security violation and shall be reported to management and shall result in short-term or permanent loss of access to computing systems. Serious violations may result in dismissal and/or civil or criminal prosecution.

- Any breach of this policy shall invite disciplinary action as defined in HR Security policy.

INFORMATION TECHNOLOGY POLICIES

1. Business Continuity Plan & Disaster Recovery Policy & Procedures

Objective & Purpose

In order to ensure continuity of business operations during business disruptions/ disasters on account of process disruptions, technology break down, power failure, natural calamities, fire, riots etc., the Bank shall put in place a well-defined board approved Policy. Business Continuity Policy demonstrates the Bank's commitment towards maintaining uninterrupted banking services, thereby enhancing customer satisfaction, quality of customer service, superior delivery standards besides assuring organizational performance improvement.

- A Disaster Recovery Site shall be in place replicating the Data Centre (Production Site). During above mentioned crisis, bank shall operate on DR site.
- Bank CBS is on ASP model hence DC and DR managed by WIPRO Pvt Limited.
- Bank also maintain DC for AUA-KUA services.
- The proper arrangements shall be made by the ASP Vendor for DR site.
- Disaster Recovery is the process of rebuilding the operation or infrastructure after the disaster has occurred.
- Business continuity plan includes planning for disaster recovery. Disaster might occur anytime, so the bank must be prepared.
- The Business Continuity Plan shall cover the occurrence of following events:
    - Equipment failure (such as hard disk crash)
    - Disruption of power supply
    - Disruption in network connectivity

- Application failure or corruption of database
- Human error, sabotages, or strike
- Malicious Software (Viruses, Worms, Trojan horses) attack

- Hacking or other Internet attacks
- Social unrest or terrorist attacks
- Fire
- Natural disasters (Flood, Earthquake, Hurricanes etc.)

The underlying purpose of business continuity planning is the speedy resumption of business operations, hence, it is essential to consider entire organization, not just the information systems processing services, while developing a plan. The BCP Project shall be initiated and formally approved and committed by the Management.

Applicability:

This policy applies to all departments, functions, systems, applications, and personnel within the bank. It encompasses all critical business processes and technology assets that are essential for the continued operation and service delivery of the bank. This policy is mandatory for all employees, contractors, and third-party vendors who are involved in bank's operations.

Policy Statement

1. The Bank endeavors to render critical banking services to all its customers, within shortest possible time, in the event of any business disruptions/disaster.
2. To ensure safeguards and well-being of people within Bank's premises.
3. It regularly maintains and updates various Business Continuity documents for its critical functions.
4. To minimize or prevent business/ financial losses on account of disruption/ disaster.

5. To ensure compliance to NABARD guidelines on BCP and follow best industry practices.
6. To enhance Bank's reputation and brand value.
7. Bank is providing various Banking solution to its customers. The below are the mentioned application which help in serving customer better.
    a. CBS Application
    b. RTGS/NEFT
    c. IMPS
    d. CTS
    e. ATM/POS/ECOM
    f. AEPS
    g. Mobile Banking(View Only)
8. Bank shall acquire DR Drill reports from vendor once in six months to ensure the functionality of DC-DR arrangement and to comply with NABARD Guidelines.
9. A report shall be submitted by Bank IT Officer after approval from IT HEAD to the Management about DR Drill. The report shall be kept in records for Regulatory & Management review.
10. The Bank is subjected to regulation by the NABARD. As per regulatory requirement, the Bank reports instances of major failures faced by the Bank, customer segment/ services impacted due to failures and corrective steps taken to avoid such failures in future.
11. The Bank shall update its Policy whenever there is a material change to its operations, structure, business, or location. In addition, the BCP of various functions shall be reviewed annually to incorporate changes in its operations, structure, business, or locations.
12. Once it is understood that Bank has met with a crisis, CEO/CISO/MD will declare to internal, external, and regulatory stakeholders.

13. In the event of incident, a root cause analysis should be done by Bank with help of External Experts.
14. Bank shall acquire Security audit report of data center and disaster recovery from the vendor to ensure that information hosted in their premises is safe from physical and environmental hazards.

Procedures

1. Once it is understood that Bank has met with a crisis, CEO/CISO/MD will declare to internal, external, and regulatory stakeholders.
2. Identifying the Root Cause Analysis and mitigating the same.
3. Documentation of the whole crisis and assuring such kind of crisis do not happen in future.
4. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.
5. Bank shall acquire BCP/DRP plan of vendor to ensure that adequate measures has been taken to continue the business operations in case of disaster.
6. ASP vendor and Bank shall follow the below mentioned points to achieve effective business continuity.

<u>At Head Office</u>

Requisites for BCP:

- Organization Chart;
- Network Architecture (Refer Network Diagram – available with IT department);
- Risk Assessment
- Business Impact Analysis
- Network Devices configuration Backup

- Staff Contact List
- Vendor Contact List

Network:

- Bank shall arrange all critical devices in high availability mode to continue their business operations.
- Bank has arranged Dual connectivity (Primary and Secondary Connectivity) for both branch and head office so that can continue their business operations if one connectivity gets down bank can continue their operations on other network.
- Secondary link connectivity is checked on daily basis.
- Bank shall take configuration backup of network devices to restore device in case of failure.

Data Backup

- Bank shall take backup of critical systems on periodical basis. And restoration activity of backup shall be conducted to ensure that backup data is complete and accurate can help in case of unavailability of data.

Power Backup

- Bank shall arrange adequate power backup for systems running at head office.

At Vendor Premises

Server:

ASP vendor shall conduct Cluster Fail over testing of Database Servers (Synchronization of software version in DC and DR done on monthly basis / as and when changes are implemented.

Data Backup

- ASP vendor shall take backup of data on daily basis, either full back up or incremental backup and critical servers and services on a separate backup server on a periodical basis to ensure the continuity of the critical operations.
- Backup server shall be arranged in different LAN segment.

Alternative Site

ASP vendor shall set alternative DR to ensure the continuity of the business.

DB Maintenance:

- DC – DR (Hot Site): ASP vendor shall carry out the Data mirroring activity with a time lag of (15 Minutes)
- Maintenance of DB tables done at defined frequency as per DBA process.

Redundancy:

- ASP vendor shall carryout DR takeover and testing of integrity for minimum 3 branches, bimonthly.
- ASP vendor shall carry out daily back up of data & periodic restoration at DR Site.

DC-DR Security Audits

ASP vendor shall conduct security audit of DC and DR premises to ensure that all DC and DR operations, controls are running effectively.

DR Drill Activity

- Vendor shall carry out DR drill activity once in six months as mandated by NABARD and shall share the DR drill report to banks representative.

- ASP vendor providing services like IMPS, ATM and other critical services shall maintain alternative DR setup to continue the payment services in case of disaster. And shall conduct DR drill of the services once in six months to ensure the continuity.

For Branches

Power

- For Continuity of Power/ Electricity bank has arranged UPS and Generator set available at every branch and it is tested on periodical basis.
- Preventive maintenance is carried out for UPS and Generator on regular basis.

Network

- Bank has arranged Dual connectivity (Primary and Secondary Connectivity) for both branch and head office so that can continue their business operations if one connectivity gets down bank can continue their operations on other network.
- Secondary link connectivity is checked on monthly basis.
- For any network related issues branch users shall inform or lodge a complaint to the head office.

Contact Lists in case of emergency

- Branch users shall be aware staff contact list in case of emergency.
- Bank users shall of contact list of all AMC vendors.

Issues with Application Software Failure

1. Identify the Nature of failure: whether there are errors in a particular area or corruption of code.
2. Notify the concerned authorities.
3. Consider the actions to be taken to recover the same. -recovery from backup.

4. Consider immediate steps to be taken if required – Communicate with software vendor.
5. Calculate estimated time required to recover, from the action emanated from the above step.
6. Notify the IT Department and the concerned users.
7. Follow the actions as directed by the authorities.
8. On completion of the same, report to the concerned authorities.
9. Notify the concerned users.

Issues with Network Failure

1. Identify the Nature of failure: whether the router is working properly or not.
2. Contact the representatives belong to network team.
3. Follow instructions guided by them.
4. If issued the does not get solved, lodge a complaint to the head office.

Responsibility

1. IT Officer being responsible for coordinating mock drill, receiving documents from vendor, and getting it reviewed by the CEO/CISO/MD. IT officer must know if any incident happened then how much time will it take to come back on track and how to recover the situation.
2. IT Manager being responsible for the overall BCP/DR process.
3. CEO/CISO/Department Head being responsible for any kind of escalation.
4. IT department shall address the issues lodged by branch users pertaining to system/service unavailability.

2. Internet Usage Policy & Procedures

Objective & Purpose

An Internet Usage policy provides employees with rules and guidelines about the appropriate use of company equipment, network for Internet access. Guidelines are in place for Bank users to use such Internet facility in an efficient, effective, lawful, and ethical manner.

This policy is intended to implement adequate security and access control measures to ensure that the Internet access or browsing facility provided by the Bank is used for appropriate official & business purposes only.

Since the nature of work demands, use of internet for business purpose is inevitable. Internet browsing consumes a significant amount of employee time as well as other resources. It involves serious security risks in terms of virus attacks, hacking, denial of service, etc. which have a potential of bringing the entire business to standstill. The implementation policy of internet usage is therefore very critical for the business.

Applicability:

This Policy applies to all employees, contractors, third-party vendors, and authorized users who access the internet using bank's network or computing resources. The policy is applicable to all devices, including desktops, laptops, mobile devices, and any other equipment connected to the bank's network.

Policy Statement

1. Bank should allow internet only through Firewall wherein adequate restriction on internet can be done. Users can use Internet as per the requirement of the job role.
2. Access to the Internet should be strictly provided for Bank's official purposes only. Bank does not permit its users to use internet for personal and non-banking purposes.

3. Internet access shall be provided by the IT department after they receive an authorized and justified request (URF) from a HR department.
4. The Users are required to submit a request for Access to Internet with justification to their HOD/ Branch Head. The HOD shall recommend the request & forward it to HRD Department for final approval. HRD shall approve /reject the request & forward the same to the IT department or to the HOD.
5. HRD shall review the access periodically and inform IT Dept. to add/delete/curtail access for the users on the basis of their changed role or transfer.
6. Users shall be identified and authenticated at the gateway before allowing access to the Internet facility. They shall be responsible for all browsing and access activities from their user IDs.
7. **Following Website categories should be strictly blocked in Bank environment:**
    a. Pornography
    b. Social Networking Sites
    c. Gaming Sites
    d. Hacking Sites
    e. Advertisement and Spyware
    f. News and Entertainment
    g. Proxy Sites
    h. E-Commerce Sites
8. **Internet Authentication:** Users should only be given access to internet facility on user authentication with special time period.
9. **Internet Access:** Internet access in Bank network should be available only via Bank infrastructure. Users should not connect to the Internet on devices in Bank's network via external services.
10. **Internet Restriction:** Access to the internet is limited to a pre-approved list of whitelisted systems, websites and URLs that are deemed safe, relevant, and necessary for business-related tasks.

11. Wi-Fi / Hotspot should strictly be prohibited in Bank Infrastructure.
12. **Points that should be considered by employees while using Internet for making payment to vendor and others:**

    a. Details of credit card/debit card/digital payment i.e., NEFT and RTGS should be submitted on a secured Web Page.

    b. Such details should never be send on email.

    c. Public Wi-Fi should be strictly prohibited while making payment online.

    d. Password should be changed regularly and should follow strong password policy.
13. All devices connected to the Internet must be equipped with the latest versions of anti-virus software, which has been approved by Bank.
14. **Internet Restriction on Servers:**

    a. Internet should not be allowed for Internal Server.

    b. Internet should be allowed on requirement basis for Public Facing Server.
15. **Training & Development:** Users should be provided adequate training for the usage of Internet.
16. **Periodical Firewall Logs Review:** Firewall logs would be reviewed on periodical basis by the Bank IT Officer and submitted for review to AGM IT.
17. In the event of incident due to Internet Usage, a root cause analysis should be done by Bank with help of External Experts.
18. Security Audit of Internet Usage (Firewall Review) shall be conducted periodically by External Vendors.
19. **User Responsibility:**

    a. Should not open social networking sites.

    b. Should use internet in accordance to Data Protection Act and IT Act.

    c. Should not violate other people's privacy.

    d. Should not use internet for personal interest which will be considered unlawful and strict action against the same will be taken by Management.

e. Should not be used to transmit unsolicited commercial or advertising material.

Procedures

1. **Internet Access Process:** Internet Access request form is received from user to IT Officer. The form will have approvals of Manager, AGM Dept Head, HEAD IT.
2. **Temporary Internet Access to employee/auditor/third party vendors etc.:** Temporary Access to Internet will be allowed only on approval of AGM IT.

   Once the task is completed, IT Officer should ensure to terminate the temporary Internet access provided to user.
3. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. A formal exception document should be approved by AGM IT.
2. Any exception in existing policy/procedures needs to be recorded in the Internet Usage Exception file with detailed reasoning.

Roles & Responsibility

1. IT Officer being responsible for periodical base monitoring, review of Firewall and maintenance of all the records, logs, change management etc. and escalate in case of any emergency.
2. IT Manager being responsible for review of all the records, logs, change management etc. and take necessary decision, if required.
3. AGM IT being responsible for any kind of escalation.
4. Branch manager will be responsible for any incident at branch level.

3. E-Mail Policy

Objective & Purpose

In today's banking scenario all important communications are done through Mail & Messaging System. It is important that proper guidelines are in place for Bank users to use such E-mail facility in an efficient, effective, lawful, and ethical manner.

This policy is intended to protect confidentiality and integrity of electronic messages and minimize the risk of misuse and damage to the security of Bank's image, information, and information systems. It is majorly set to indemnify the Bank from any wrong doings or intentions by the users using the facility.

Applicability:

This policy is applicable to all employees and authorized users who have access to bank's email systems or use email services on behalf of the bank. The policy applies to all email communications conducted using the bank's official email accounts, regardless of the device or platform used.

Policy Statement

1. Bank is using email services for Internal and External communication.
2. Internal communication is limited to Bank employees and used for sharing of common circular, official communication etc. Mail server is hosted in Bank Data Center and managed by Bank IT Officer.
3. Bank can avail "Delegated Admin Console" service from Mail Service Provider. Using the console, the authorized IT Officer can create/delete/change the password of User ID and policy settings and functions under respective Bank domain without routing the request through Mail Service Provider.

4. **Training & Development:** Employees are given training on Phishing attack and appropriate use of email ID through circulars, seminar etc.
5. **Admin Rights:** Access to admin rights is given to only IT Officer.
6. All users accessing the email services should have their separate email IDs.
7. All users accessing the email services should use strong and secure password for security of their email account.
8. User should ensure that emails are kept confidential. Mail Service Provider & Bank IT Officer shall take all possible precautions in maintaining privacy.
9. Official e-mail IDs should be opened only in Bank's infrastructure.
10. Email should be used only for Business operations and not for personal work.
11. **Two-Step Verification:** Two-step verification should be enabled for additional level of security.
12. Bank IT Officer should take all necessary steps to secure Mail services by implementing latest functionality i.e., DKIM, SPF, DMARC.
13. The bank shall enable the appropriate security features to email solution and email servers such as anti-malware, anti-phishing, file uploading and downloading limit, etc.
14. **Device Approval Function:** Any new device getting attached to existing email services, should be approved from IT Officer with proper justification.
15. **Back Up Email Configuration:** Back up email archival and retention facility should be enabled. Back up of emails of two years to be maintained by Bank IT Officer.
16. Auto Saving password in the Email services shall not be permitted for security purpose.
17. **Users Responsibility:**
    a. Should not transmit by email any file attachments which are known to be infected with a virus.
    b. Should not open email file attachment have received from unsolicited and unreliable sources.
    c. All email attachment received should be virus scanned.

d. Should be responsible for the contents of his/her emails.
e. Email of employees are the property of Bank and it reserves rights to examine the same at any point of time.
f. Email shall not be used for sharing of offensive/disruptive message.
g. Blanket forwarding of email messages is prohibited. Transmission/re-transmission of chain messages are strictly prohibited.
h. User can not add bcc in their email, while sending email in from/ To section in any case.
i. User must use sober language in the bank email.

18. Mail Service Provider shall provide the email service based on the adequate Service Level Agreement.
19. **Personal Email:** Personal emails are strictly prohibited. Proper authorization and permissions are required for any individual to use personal email in Bank Network.
20. In the event of email incident, a root cause analysis should be done by Bank with help of External Experts.
21. Security Audit of Mail & Messaging system shall be conducted periodically by External Vendors.
22. User must use authorized mailing system for sending and receiving mails.

Procedures

1. **Email Creation Request:** E-mail creation request is received from user to IT Officer. The form will have approvals of AGM IT.
2. **Sharing of Credentials:** Once User ID and Password is created, then login details are shared to the Branch Manager vide mail which further is shared with the staff.
3. In case of Higher Authority email creation is requested, MD approval must be taken.
4. **Sharing of login details:** The login details of users are shared with his/her Branch Manager/Superior vide mail.

5. **Mail & Messaging access on Individual Mobile Phones:** A request is received from user to access E-Mail on Mobile phone with approval from his Superior with proper justification for the same. Only after proper due diligence by IT Officer, AGM IT gives approval for the same.
6. **Sharing of Circular related to Security to users:** Circulars on regular basis are shared to Email users in relation to security measures to be adopted by Users while using Email facility.
7. In case, if IT Officer is on leave for longer period, he/she should share the credentials with the superior or any other deputed person.
8. **Termination/Retirement/Exit:** IT Officer should receive hard copy from Human Resource Department for Termination/Retirement/Exit letter of the user. Accordingly, the administration disables the login of the user.
9. **Bulk sharing of email:** A common group shall be created for Branches to share bulk email by IT Officer.
10. Bank should use two step authentications i.e. First Step is to apply Password and second step is to generate OTP on registered mobile number only.
11. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. A formal exception document should be approved by AGM IT.
2. Any exception in existing policy/procedures needs to be recorded in the Mail & Messaging Exception file with detailed reasoning

Roles & Responsibility

- IT officer shall be responsible for implementation of this policy across the organization. He shall be assisted by Asst. Manager - IT Security.
    1. IT Officer being responsible for regular base monitoring, review and maintenance of all the records, logs, etc. and escalate in case of any emergency.
    2. IT Manager being responsible for periodical review of all the records, logs, etc. and take necessary decision if required.
    3. AGM IT being responsible for any kind of escalation.
    4. Branch Managers and HO Head (Location heads) shall be responsible to follow the policy and in act in line for their respective location.

4. Logging & Monitoring Policy & Procedures

Objective & Purpose

To ensure that records are managed and controlled effectively and at best value commensurate with legal, operational and information needs.

Logging

The Log & Audit Trail Policy provides a framework for Logging & Auditing Operating System events, Application Events, Database Events in the Local Area Network, and the Network events of the bank's IT infrastructure.

Monitoring

The purpose of the Security Monitoring Policy is to ensure that information security and technology security controls are in place and effective. One of the benefits of security monitoring is the early identification of security issues or new security vulnerabilities. This early

identification can help to prevent security incidents or to at least minimize the potential impact of such incidents.

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective.

Applicability:

This policy applies to all systems, networks, applications, and digital assets owned, operated, or managed by bank as well as third party vendors.

Policy Statement

1. Bank should maintain logs of logical access for following assets:
    a. Servers
    b. Critical End Points including where CBS is operational
    c. Networking Devices
    d. Network Monitoring Tool
    e. Critical Applications
2. **Bank should maintain logs of physical access for following assets:**
    a. Biometric Devices for physical access of Data Centre and Near DR.
    b. Third party visitor register for accessing Bank Information Assets at Bank DC, Head Office, Branches.
    c. Records should be maintained for accessing N/w rack and Branch server room etc.
3. System usage would be reviewed and monitored to ensure that unauthorized system activities are detected in a timely manner.
4. The level of reviewing and monitoring of the system would be determined based on the criticality of the system.

5. A centralized log monitoring solution should be implemented to record any information security events.
6. All Administrative activities shall be logged to ensure accountability and effective management.
7. The bank shall define the appropriate retention period for the logs.
8. System logs will be enabled to identify a record system logs and unauthorized activity. Logging shall be enabled to capture audit trails of an event for all the critical devices including application server, network device and security device.
9. Security event recorded in logs must be enough to establish individual accountability for action performed and be able to support the investigation for suspected violation at a minimum following information shall be captured:
    a. User ID/Identity of the source
    b. Date and time stamp of the event
    c. Severity
    d. Description of the Event
    e. Affected System/Resource
    f. Outcome/result of the event
9. Adequate controls shall be implemented to ensure that log files are not altered while copying for secondary logs required for analysis, audit trail etc.
10. Bank should use information asset register to monitor and understand what collection of records and information we hold and note each document retention period.
11. **Logs for following categories should be maintained:**
    a. Create
    b. Update
    c. Delete
    d. Read

Procedures

1. Logs of all the Networking devices should be stored on Syslog server.
2. Logs of Network Monitoring Tools should be stored in Bank.
3. Logs of Critical End Points & Servers should be stored in Bank.
4. Logs of Biometric devices should be stored in the application provided by the vendor.
5. Logs of Anti-Virus and Email should be stored on dedicated server.
6. All the logs should be monitored by IT Officer on real time basis and action to be initiated in case of any discrepancy.
7. All the logs should be reviewed by IT Officer on periodical basis and reports shall be submitted to AGM IT for further review.
8. In case of any incident, the above-mentioned logs should be timely available for all the critical assets.
9. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.
10. Alert shall be generated for any modifications or changes to the log settings, configuration to validate the log settings.

Policy Exception

1. Exception to the policy will be handled on case-by-case basis and reviewed and approved by the AGM IT.
2. Detailed reasoning shall be recorded for Exception to the policy.

Roles & Responsibility

1. IT Officer being responsible for regular base monitoring, review and maintenance of all the records, logs, etc. and escalate in case of any emergency.

2. IT Manager being responsible for periodical review of all the records, logs, etc. and take necessary decision if required.
3. AGM IT being responsible for any kind of escalation.
4. Branch Managers and HO Head (Location heads) shall be responsible to follow the policy and in act in line for their respective location.

5. Update, Patch & Change Management

Objective & Purpose

The Change Management policy is in place to control changes to all critical and non-critical IT infrastructures and resources that underpin the day to day operations of the bank.

The Patch Management policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to Operating system, firmware, productivity application and utilities.

This policy is designed to

1. Ensure Users face minimum inconvenience during change process.
2. Ensure that exposures such as data loss, change of contents, business disruption are kept to the minimum during the change process.

Applicability:

This policy applies to all technology assets, systems, applications, and devices utilized within bank's infrastructure. This encompasses all hardware, software, and network components that contribute to the bank's IT environment.

Policy Statement

1. All supported and managed servers and endpoints must be accurately listed in the centralized patch management solution.
2. All Microsoft and Non-Microsoft patches including firmware updates will be downloaded only from the authorized system vendor or designated authorized partner.
3. Each patch source and its integrity must be verified through full anti-virus scan upon download prior to being made available for deployment.
4. Before application of all Microsoft and Non-Microsoft patches; it should be tested on UAT environment before deployment in the production environment.
5. A back out plan that allows safe restoration of system to the pre-patch stage must be devised prior to any patch roll out if the patch has unforeseen effects.
6. New servers, workstation, third party standard applications and network equipment will be patched to the most recent patch release before coming on to the bank network in order to reduce the risk.
7. Bank should immediately update patch which are Critical and High in nature and requires immediate action based on advisory from CERT In, RBI, NABARD, NPCI, Microsoft, Third Party Vendor etc.
8. Before implementation of Patch on Live Environment; Bank IT Department should take prior approval of AGM IT.
9. Logs should be maintained by the IT Officer for Patches installed.
10. Bank IT Officer should review the logs on quarterly basis. The logs should be approved by AGM IT.
11. The addition; modification or removal of approved; supported or baseline hardware; network; software; application; environment; system or associated documentation.
12. Before application of any changes; it should be tested whether it is compatible with Bank existing Infrastructure.
13. Logs should be maintained by the concerned official for Patch installation.

14. Bank should take backup before applying any patch, update or any change in the infrastructure.
15. Any updating in database must be done by database administrator at vendor site with prior permission from respective authority.

Procedures

1. **Systems Patches:** Bank should adopt the measures to automatically apply Patches on host whether being Microsoft or Non-Microsoft.
2. Bank should adopt centralized patch management solution which will managed by IT Officer and pushed from Server to Servers and Workstations in the Network.
3. CBS and Non-CBS Application patches shall be received from Vendor over the mail.
4. CBS and Non-CBS Application patch shall be approved by IT Manager and AGM IT.
5. Before deploying the patches in production environment, patches should be test on UAT Server.
6. Once the patch is running smoothly on UAT Server, the patch would be deployed on production environment.
7. Network patches/firmware shall be received from Vendor/Online Service Provider.
8. Network patches/firmware shall be approved by IT Manager and AGM IT.
9. Before deploying the patches in banking hours, patches should be test during non-banking hours.
10. Once the patch is running smoothly during non-banking hours, the patch would be deployed during banking hours.
11. Any change in the established environment whether in terms of software, infrastructure, hardware & peripherals should be documented and approved from Higher authority.
12. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. Any servers or workstations that do not comply with policy must have an approved exception recorded in the Patch Management exceptions file detailing the reason for the exception and the steps taken to mitigate the risk.
2. System will only have exception to the policy if scheduled updates or patches are deemed likely to cause major disruption to the system, resident software or service functionality or if it is deemed to be a bespoke critical system for which updates or patches are not available.

Roles & Responsibility

1. IT Officer being responsible for regular base monitoring, review and maintenance of all the records, logs, change management etc. and escalate in case of any emergency.
2. IT Manager being responsible for periodical review of all the records, logs, change management etc. and take necessary decision if required.
3. AGM IT being responsible for any kind of escalation.
4. Branch manager is responsible for to check authorized H/W and S/W which is installed by an IT team/ vendor at branch.

6. Asset Classification & Management

Objective & Purpose

To establish a process for security, classifying and handling bank Information Assets based on its level of sensitivity, value and criticality to the bank.

All the IT Assets shall be protected against misuse, theft, damage, destruction and disasters due to natural calamities like flood, fire, earthquake, attacks etc.

This purpose is to achieve and maintain the required level of protection and operating standards for the Information assets, applications, processing facilities of the organization.

Applicability

- This policy is applicable to all the employees of the bank.
- Physical assets, shall include -
  - Hardware assets like servers, PCs, active networking devices.
  - Software assets, which include various software applications and data-deemed necessary for archival.
  - Hard copy documents.
  - Employees and 3rd party contract personnel.
  - Other infrastructure assets which form a part of the processing facilities.

Policy Statement

1. Bank should define the Responsibility for ensuring that Information Assets have a security classification authorized by the Information System Owner.
2. Bank should maintain the proper inventory and identify the information asset in accordance with information asset and security classification.
3. Bank should have performed a risk assessment and consider the vulnerabilities that are attributed to each Information Asset.
4. Bank should ensure that all the confidential data must be stored in encrypted mode.
5. Bank should ensure that IT team take the backup at regular interval.
6. Bank should have performed a risk assessment audit for all the Assets in bank infrastructure and identify and maintained the inventory according to asset severity.
7. Bank should have the need-to-know principle requires that Information Assets should only be available to those who need to use or access the Information Asset to do their work.

8. Bank should maintain confidentiality and integrity of classified Information Assets a strict audit logging process is to form part of the Security Classified Information Asset Register. This audit log must be carefully designed to ensure it can provide a 'trail of evidence' which can be used to investigate inappropriate or illegal access.
9. Bank should ensure that all the Employs have knowledge about the importance of assets. Also bank IT Team provide the awareness circular at regular interval for all the Employees.
10. Bank must ensure that insurance for every IT asset is taken.
11. Regular interval of time bank must check and review all assets.
12. If bank assets moved from one place to another then travelling record must be maintained. Also, proper labeling on the device and place on which assets will be recites must be clean.
13. A dead stock register must be maintained for assets. And depreciation value must be calculated properly and maintained in the dead stock register.

Procedures

1. The purpose of Information Security is to protect the confidentiality, integrity and availability of Information Assets. The classification of Information helps to determine what baseline Security Controls are appropriate for safeguarding that Information. Bank should have ensured that all the minimum-security controls are available for all the Information Assets.
2. Bank should calculate their risks for IT assets in regular interval of time.
3. Bank should have proper authorization process to provide access to its critical assets.
4. Proper procedure with proper authorization must be taken before purchase new assets or replacement of old assets. For this process record should be maintained.
5. A proper procedure must follow before reselling of banks assets with proper authorization from every regarding officer.

6. **Following points must be included in inventory register:**

1) Asset numbering
2) Asset description
3) vendor
4) brand
5) configuration
6) purchase date
7) warranty info
8) location of asset
9) license type and no
10) Maintenance schedule
11) insurance details

7. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exceptions

1. Exception to the policy will be handled on case by case basis and reviewed and approved by the AGM IT.
2. Any reason where Asset Classification & Management Policy cannot be able to implement must be recorded in detail with proper reasoning.

Roles and Responsibility

1. User being responsible to inform anything happened with banks asset to the proper responsible officer.
2. IT Officer being responsible for regular interval of making request list of scrapping for assets and submitted to AGM IT for proper approval.

3. IT Manager being responsible for periodical review the scrapping request and take necessary action against that request.
4. AGM IT being responsible for any kind of escalation.
5. All the users shall be responsible for appropriate and secured use of IT Assets
6. Operational level responsibility lies with IT Manager and All Asst. Manager with respect to assets maintained by them.
7. Branch manager shall be responsible for all the assets installed in their respective branches.

7. Capacity Management Policy

Objective & Purpose

The Objective is to make available IT resources that the Business requires efficiently in a cost-effective manner.

To correctly monitor the performance of the existing or future bank system, to forecast their evolution and identify possible bottlenecks.

Applicability

This policy is applicable to all employees of the bank.

Policy Statement

1. The Capacity Management process shall identify Capacity requirements based on business requirements, usage trends, sizing of new service, vendor need etc.
2. All documentation related to Capacity Management must adhere to established standards for consistency and clarity.
3. The bank shall arrange where in Critical Systems wherein important parameters i.e., CPU utilization, Memory utilization is performed on real-time basis.

4. Capacity of critical systems should be checked periodically to meet current and future business need.
5. Bank should make arrangement to ensure for optimal performance, end throughput or load on Server of IT resources.
6. Bank should make arrangement wherein load balancing and stress testing evaluation can be reviewed periodically and in case of any problem identified, adequate action can be taken.
7. Bank should decide where Storage allocation can be done virtually on real-time basis to prevent the circumstances of contingency.
8. Understanding the demand on the service and future for workload growth.
9. Producing regular management reports that includes current usage or resources, trend and forecast.
10. In the event of failure in Capacity Management, a root cause analysis should be done by Bank with help of External Experts.
11. Security Audit of Capacity Management shall be conducted periodically by External Vendors.
12. The bank shall provide training and awareness programs to ensure that all employees are well-informed about the Capacity Management Policy and its procedures.

Procedures

1. Monitoring and reviewing of storage capacity of Servers by IT Officer.
2. Shifting of storage from one server to another on real-time basis, once the storage capacity of existing server is almost full.
3. Manual logs should be maintained for 6 months by IT Officer for the above-mentioned activity. These logs are to be reviewed by AGM IT on quarterly basis.
4. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

5. Training sessions on Capacity Management shall be conducted annually for all bank employees involved in IT resource management.

Policy Exception

1. A formal exception document should be approved by AGM IT.
2. Any exception in Capacity Management, needs to be recorded in the Capacity Management Exception file with detailed reasoning.

Roles & Responsibility

1. All the employees are required to follow the instructions issued by the IT Department with respect to the policy.
2. IT Officer being responsible for daily base monitoring, review and maintenance of all the records, log, etc. and escalate in case of any emergency.
3. IT Manager being responsible for periodical review of all the records, logs etc. and take necessary decision if required.
4. AGM IT being responsible for any kind of escalation.
5. System administrators are responsibility for the day-to-day management of the systems, identification and solving of current problems and performance tuning.

8. Network Administration Policy

Objective & Purpose

The Network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.

Applicability

This policy is applicable to all employees of the bank.

Policy Statement

1. IT Officer should ensure Network Availability and effective Network Performance.
2. IT Officer should install, maintain and update Networking Devices i.e. software and hardware.
3. Bank should have a dedicated IT Officer who will coordinate with the vendor to resolve Hardware related issues on real time basis i.e. Systems failure, Networking devices failure etc.
4. The IT Officer should also coordinate and take care of cabling issue in the bank infrastructure on real time basis.
5. The performance of the Network should be monitored on real-time basis.
6. Install standard monitoring system at Data Centre for daily monitoring and log generation for Network downtime etc.
7. For any scheduled downtime, notify all users sufficiently in advance.
8. Monitor and inform the employees for the status of the network in case of real-time downtime.
9. Responsible for effective installation of Networking equipment and reviewing smooth functioning of the same.
10. The configuration of the network impacts directly on its performance and affects its stability and Information Security.
11. The design and configuration of Network Architecture must be guided & verified by IT Officer and approved by AGM IT.
12. In the event of Network Failure, a root cause analysis should be done by Bank with help of External Experts.
13. Security Audit of Network shall be conducted periodically by External Auditor.

14. If an employee detects a network-related issue or suspects a security breach, they must report it immediately to the IT Officer.

Procedures

1. Bank shall maintain an up-to-do/centralised inventory of authorised devices connected to bank's network (within/outside banks premises) and related network devices in the banks network.
2. Any issue related to Hardware/Cabling in the Branch should be informed by Employee to the IT Officer. The IT Officer shall ask the Vendor to visit Branch for resolution of issue.
3. If there is a minor fault in the Hardware/Cabling at Branch level, the vendor should visit the branch and resolve the issue.
4. After resolution of the above issue, the Employee shall submit a compliance report to the IT Officer for his record purpose.
5. If there is a major fault in the Hardware/Cabling at Branch level, the vendor should bring the asset to the Head Office and repair the same. Once the asset is repaired, the IT Officer along with Vendor shall take and re-install the Hardware at the Branch.
6. A compliance report shall be prepared by Vendor for all major faults and shared to IT Officer for his records.
7. IT Officer should have a complete record keeping for all the faults addressed by the Employee/Vendor and submit the report to AGM IT for his review purpose on periodical basis.
8. Bank should ensure that IT Officer shall provide advance notification to all the users in case of scheduled downtime in the Bank network.
9. Bank should ensure that IT Officer shall monitor and inform and update about the real time downtime of the network to the employees/vendor.

10. Bank should ensure that IT Officer shall the resolve the faults reported by Employees. A ticket is generated to track the status of fault and ensure that faults are being handled correctly and timely.
11. For any significant network disruption or breach, the bank shall notify the appropriate authorities, regulatory bodies, and affected parties as required by applicable laws and regulations.
12. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. A formal exception document should be approved by AGM IT.
2. Any exception in existing Network needs to be recorded in the Network Administration Exception file with detailed reasoning.

Roles & Responsibility

1. All the employees are required to follow the instructions issued by the IT Department with respect to the policy.
2. IT Officer being responsible for daily base monitoring, review and maintenance of all the records, logs, hardware details etc. and escalate in case of any emergency.
3. IT Manager being responsible for periodical review of all the records, logs, hardware details etc. and take necessary decision, if required.
4. AGM IT responsible for any kind of escalation.

9. System Administration Policy

Objective & Purpose

To ensure the security, reliability and privacy of the bank Servers and Workstations. Overall responsibility, management and upkeep of servers and workstation.

Applicability

This policy is applicable to all employees of the bank.

Policy Statement

1. System administrator should provide access to the user on the need-to-know basis and access provided shall be revoked once work gets done.
2. System administrator shall maintain system user profile register.
3. The system configuration of the workstation and server should be based on the system load.
4. The IT Officer shall be responsible for installation of Group Policy i.e. Software settings, Windows settings, Administrative Templates for Computer Configuration and User Configuration based on Industry's Best Practices.
5. An IT Officer shall be responsible for activities of deploying new systems, record keeping, reviewing and escalation, if required.
6. An IT Officer shall install applications/data/records on workstation based on job profile.
7. IT Officer should centrally manage, monitor, create, issue, deactivate the user credentials with adequate restriction for the Users.
8. IT Officer should provide storage space in Server and workstation based on the Capacity Management Plan.

9. IT Officer should ensure that all the servers and workstations are fulfilling the requirement for adequate licensing for Operating System.
10. IT Officer should update server and workstation as soon as new version of Application Software is available.
11. IT officer should arrange spare hardware in case of irreparable workstation so that Bank's business operations are not hampered.
12. IT Officer should take back up of files and folders for critical systems
13. IT Officer should compulsorily update patch as per OEM release on workstation and servers.
14. IT Officer shall conduct training on latest technology, security in the Workstations to the employees.
15. Changes and modification in Inventory shall be communicated by the IT Officer to the person who is managing inventory on periodical basis.
16. To make sure remove/prevent the spread of viruses and other unauthorized software in the workstation.
17. In the event of Server and Workstation Failure, a root cause analysis should be done by Bank with help of External Experts.
18. Security Audit of Workstation shall be conducted periodically by External Vendors.
19. IT Officer shall be responsible for closure of VAPT findings of Server and Workstation. The status shall be prepared by him and should be reviewed by AGM IT.
20. Immediate action should be taken to remediate the vulnerability as identify/reported by OEM, CERT IN, Regulators etc.
21. Scheduled backups must be taken then the information must be copied away to a disk and be kept off-site in case it is needed and for the tapes to be re used.
22. The Systems Administrator must submit to the CISO to sign a schedule of all monthly backups done on the systems and quarterly tested backups after every quarter.

Procedures

1. Any deployment of new server and workstation in the existing Bank Infrastructure should have a proper approval process.
2. A proper approval chain should be in place for new deployment. Based on the requirement and approval from AGM IT, new system is deployed to Branch/Head Office.
3. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.
4. The user account must not be deleted for a period of five years, in case later there's information requested from that account. This is also because the username holds audit trails that may be needed at some stage.
5. The bank shall implement a method for assessing and validating user access rights on a regular basis to ensure that they adhere to the principle of least privilege.

Policy Exception

1. A formal exception document should be approved by AGM IT.
2. Any exception in existing workstation needs to be recorded in the System Administration Exception file with detailed reasoning.

Roles & Responsibility

1. All the employees are required to follow the instructions issued by the IT Department with respect to the policy.
2. IT Officer being responsible for daily base monitoring, review and maintenance of all the records, logs, hardware details etc. and escalate in case of any emergency.
3. IT Manager being responsible for periodical review of all the records, logs, hardware details etc. and take necessary decision if required.

4. AGM IT being responsible for any kind of escalation.
5. Upon receiving communication from HR informing the retired and/or resigned employees, the systems administrator must disable the employee, ensuring that the account cannot be used / accessible.

10. IT Disposal Policy and Procedures

Objective & Purpose

- The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by bank.
- To define the responsibilities of individuals for the secure disposal of Bank IT assets.
- To provide advice on the appropriate methods of destruction of physical media.
- To ensure sensitive information assets stored via the IT equipment is sufficiently backed up, copied and/or removed prior to being disposed of.
- To ensure that chain of custody is maintained for disposal/destruction of IT Assets.

Applicability

This policy is applicable to all employees and vendor associated with disposing of IT assets of the bank.

Policy Statements

1. IT assets like PC, Laptops, Servers, Storage devices, printers, scanners, software's etc. must have a tag which helps to identify assets EOL.
2. It must contain Equipment that stores sensitive data, which is no longer needed or has reached "end of life", must be securely deleted.

3. This policy on disposal covers all data or information held by the bank whether held digitally or electronically on IT equipment or as manual records held on paper or in hard copy.
4. All data and files must be removed properly like overwriting each disk sector of the device by using commercially available disk cleaning program, because only deleting data is not enough, recovery tools can able to recover all deleted data.
5. It is very important to remove all software licenses including OS before destruction of storage devices.
6. It is very important that to ensure any sensitive data is removed before IT equipment is redistributed.
7. It is very important that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal.
8. It is very important to stick scrap sticker on IT assets which are being disposed.
9. IT devices that have been used for sensitive work and cannot be protected from external threats must be disposed immediately.
10. IT devices that have NOT been used for sensitive work and CAN be protected from external threats must be disposed by creating schedule.
11. In bank the old IT assets or is due for replacement by a newer model, proper action must be taken by bank IT team and make sure that bank getting fair price for old IT assets against the replacement of that assets.

Procedures

1. It must be done after IT assets stop getting services from provider.
2. scrapping process for assets
    - Remove the hardware from the systems and disposed physically.
    - Sanitizing the OS for complete removal of software's.
    - Overwriting each disk sector of the device by using commercially available disk cleaning program, after deletion of data from storage devices.

- Use Shredder machine to dispose physical data.

3. It is very easy to identify which IT assets are disposed and which are being disposed.
4. It is depending on whether sensitive data is being stored in the device or not. Then it is disposed under urgent or non-urgent disposal.
5. Bank should have documentation which includes entire assets, reasons, time stamps and approval.
6. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.
7. User May need to fill IT Disposal Form prior to disposal of IT asset.
8. All IT equipment that is identified for disposal should be accompanied by an equipment disposal verification and entry included in asset register.
9. All such equipment should be processed by a registered and approved contractor to securely remove any personal data
10. When agreeing a contract with a professional equipment disposal service, the management of the bank should obtain a clear evidence of sufficient data security arrangements, including a written statement regarding confidentiality, destruction methods and indemnity if the contractor fail to adequately destroy
11. IT equipment should not leave the organization premises unless a chain of custody is established relating to the data contained within the device, this means establishing who is responsible for sensitive contained in them.
12. Successful deletion and destruction must be evidenced and certification must be obtained and recorded at all times.
13. The bank shall have process to maintain the record of disposed IT assets with proper necessary details in the register.

Policy Exceptions

1. Exception to the policy will be handled on case-by-case basis and reviewed and approved by the AGM IT.
2. Any reason where IT disposal policy cannot be able to implement must be record in detail with proper reasoning.

Roles & Responsibility

1. All the employees are required to provide details of IT assets which have become non-operational to IT Department for carrying out the disposal activity with respect to the policy.
2. IT Officer being responsible for regular interval of making request list of scrapping for assets and submitted to AGM IT for proper approval.
3. IT Manager being responsible for periodical review the scrapping request and take necessary action against that request.
4. AGM IT being responsible for any kind of escalation.

11. Financial Service Policy

Objective & Purpose

Financial services regulation should contribute to an environment that protects consumers, promotes market integrity, and supports investment and growth.

Applicability

This policy is applicable to all employees of the bank.

Policy Statements

1. Types of services

1.1 Internet Banking: If bank have Internet banking, then, bank must provide all possible security to IB such as conduct VAPT on regular interval of time. Bank must have to investigate how many IB customers handled by IB server, so service remains continues.

1.2 Mobile Banking: If bank have Mobile banking, then, bank must provide all possible security to Mobile Banking such as conduct VAPT on regular interval of time. Bank must have to investigate how many IB customers handled by IB server, so service remains continues.

1.3 ATM services: If bank have ATM services, then bank must ensure that ATM should remain in service 24*7. And, ATM OS must update and should receive updated patched on regular interval of time. Also, guard should be available at the ATM, privacy should be maintained within ATM room.

1.3.1 ATM Cards: Bank should ensure that customer should activate their ATM card from visiting bank or from Internet banking. Bank must ensure that customer must not receive already activated card.

1.4 Cheque: Bank must use and provide MICR cheques Also keep customers cheques securely for banking process.

Procedures

1. Bank must have a proper procedure to create its well financial assets list.
2. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exceptions

1. Exception to the policy will be handled on case-by-case basis and reviewed and approved by the AGM IT.
2. Any reason where Financial Service Policy cannot be implemented must be recorded in detail with proper reasoning.

Roles & Responsibility

1. IT Officer being responsible for monitoring, review, and maintenance of all the records, logs etc. and escalate in case of any emergency.
2. Respective departments have to resolve customer complaints whenever complaints get logged in to the log book.
3. IT Manager being responsible for periodical review of all the records, logs etc. and take necessary decision if required.
4. AGM IT being responsible for any kind of escalation.

12. Backup and Restoration Policy & Procedures

Objective & Purpose

The objective of this policy is to define formal requirement for IT continuity, Backup and Recovery in order to prevent or mitigate the risk of IT disruption or disaster and allow for an efficient recovery of IT services and data in a timely manner.

Back up shall be taken for all data comprising mainly of applications, configurations and transactional data created by the applications by the respective administrators as per the Backup Procedure. Back up shall be done on regular basis. The back-ups shall be tested for recovery at regular intervals.

Applicability

This policy is applicable to all the employees of the bank.

Policy Statement

1. Tape drives, cleaning tapes and other backup media must be maintained in accordance to OEM Guidelines.
2. Frequency of back up for all critical and important data shall be identified by the asset owner.
3. Restoration of Backup data should be tested periodically wherein major parameters i.e., financial indicators likely GL balances; Profit and Losses etc. for the cutoff date should match with actual. In case of any difference/discrepancy should be immediately reported by IT Officer to AGM IT.
4. **Back Up:**

   a. Vendor should ensure to take full backup of Database on external device on daily basis.

   b. Vendor should ensure to take real time backup when Bank is operating on DR site.
5. In the event of incident due to lapses in Backup & Restoration, a root cause analysis should be done by Bank and vendor with help of External Experts.
6. Security Audit of Backup & Restoration shall be conducted periodically by External Vendors.
7. Bank shall take offline backup of critical data of every critical system every month on external Hard Drive as well.
8. Bank should maintain proper inventory for backup devices which includes Sr. No. and proper labeling.

Procedures

1. **Data backup:** Vendor should ensure data replication in DR on real time basis to avoid data loss in case of any contingency for all the Bank processes likely CBS; RTGS / NEFT; IMPS; ATM; Antivirus; Mail and Messaging; Critical Systems etc.
2. Vendor should ensure manual Data Backup for all the Bank processes as stated in 3.13.3/1 on daily basis. Vendor is responsible for taking manual backups of the Bank Database at vendor site.
3. Bank shall be responsible for taking backup of the data/devices/critical systems present at bank.
4. Restoration of Data Backup should be periodically tested, not less than three months, to ensure availability of Backup data.
5. The bank shall maintain the backup register to keep a track of back up done in the bank.
6. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. A formal exception document should be approved by AGM IT.
2. Any exception in existing policy/procedures needs to be recorded in the Backup and Restoration Exception file with detailed reasoning.

Roles & Responsibility

1. IT Officer being responsible for periodical base monitoring, review of Backup & Restoration of all the records, logs, change management etc. and escalate in case of any emergency.

2. IT Manager being responsible for review of all the records, logs, change management etc. and take necessary decision, if required.
3. AGM IT being responsible for any kind of escalation.
4. Vendor is responsible for backup of data present stored at Vendor site.
5. Branch manager is responsible for branch level daily backup of critical data.

13. Database Administration Policy

Objective & Purpose

To establish uniform data standards that ensures consistency, comparability, accuracy, and integrity of Database.

Applicability

This policy is applicable to all the employees of the bank and vendor who is managing the Database of the bank.

Policy Statement

1. **Ensuring integrity of production data:** controls for unauthorized access, adequate validation procedures.
2. **Ensuring security and privacy of data:** controls for unauthorized access, safeguards against physical harm to the systems (e.g., Accidental erasures, physical deterioration of storage media etc.).
3. **Encryption:** The vendor shall implement appropriate encryption methodology to encrypt the database of the bank and the same shall be verified by the bank on regular basis to prevent the unauthorized access to the database.

4. Vendor shall be responsible for addition/deletion/modification of database, record keeping, reviewing, and escalating, if required.
5. Vendor ensure Data Backup for all the Bank processes on daily basis and it should be taken on external devices.
6. CBS vendor should be responsible for ensuring that the Database is not corrupted, for which following action should be in place:

    - Split the database.
    - Keep your device drivers updated.
    - Keep your device scanning from Viruses.

7. Taking periodic backup of database and archival of data for six months.
8. Only authorized person shall have Read and Write Access of Database and shall be responsible for assigning the rights to Users/Vendors.
9. CBS vendor shall be responsible for troubleshooting of the problem.
10. CBS vendor shall be responsible for performance and tuning of the database.
11. In case of any incident/operational issue, CBS vendor is responsible for adequate resumption of Business Operations as per policy of BCP/DR.
12. CBS vendor must check table indexing and table size allocation on regular interval of time and make changes if required.
13. CBS vendor must review database if database is updated or any kind of changes.

Procedures

1. Extraction of proper reasoning for any modification in Database structure shall be done by CBS and other application vendor.
2. CBS vendor shall take approval from respective authorities for changes in Data Manipulation Language and Database Structure.

3. CBS vendor shall be responsible for modification of Database Structure (Tuples and Rows) modify the database structure as per the requirement.
4. CBS vendor must act against the responsible/ accountable person if any incident is happened and that person found guilty.

Policy Exception

1. A formal exception document should be approved by respective authority at the vendor site.
2. Any exception in existing Database needs to be recorded in the Database Administration Exception file with detailed reasoning.

Roles & Responsibility

1. CBS vendor shall be responsible for periodical review of all the records, logs, database details etc. and take necessary decision if required and to review CBS application development periodically.
2. CBS vendor shall be responsible for any kind of escalation and to implement this policy and its proper working at CBS vendor environment.

14. Software Acquisition, Development, Maintenance Policy

Objective & Purpose

Standardizing the development approach and coding techniques for critical systems will ensure their maintainability, security, protection against cyber-attacks and accessibility.

Applicability

This policy is applicable to the IT employees of the bank and vendor.

This policy is applicable to each user who uses CBS application for any type of banking operations.

This policy also extends to external software development vendors with whom the bank has engaged for applications that are utilized by the bank.

Policy Statement

1. Bank should ensure from vendor that vendor is conducting source code review audit of Internal application on periodical basis by IT professionals.
2. Any new patches/module/functionality changes to be deployed in the production environment only after successful testing on UAT environment.
3. Bank should ensure that application developer deployed by the vendor shall follow the OWASP Top 10 for securing the application.
4. Bank should use valid SSL Certificate for the critical applications.
5. Bank should ensure that Software Development Life Cycle models (SDLC) is followed by the vendor. The application should be working on the specify design selected in SDLC Model i.e., Waterfall, V Model etc.
6. Any change in the established technology whether in terms of software, applications, database should be properly documented and approved.
7. In the event of Software Failure, a root cause analysis should be done by vendor with help of External Experts.
8. Security Audit of Software shall be conducted periodically by External Vendors.
9. The bank shall acquire the certificate or report from application vendor for conducting security audit on periodic basis.
10. Vendor shall be responsible for closure of VAPT findings of Software on priority basis and vendor shall maintain the record for closed and open vulnerabilities.
11. The bank shall acquire the findings and closure status of the vulnerabilities found from vendor.

12. Bank must ensure that modules from CBS application must be created according to bank need.

Procedures

1. Logs should be maintained for 6 months by the vendor for all the changes made in the existing software. These logs are to be reviewed on quarterly basis.
2. Bank must ensure that banks employee must get training for CBS application in regular time interval.
3. Bank must act against the responsible/ accountable person if any incident is happened and that person found guilty.
4. **System Acquisition–For systems purchased by the organization:**
    - Bank shall follow/refer vendor management policy for all kind of software purchases.
    - Bank shall conduct security assessment of vendor prior entering into the contract
    - Processes like acceptance criteria shall be considered, which will give assurances that security requirements are met.
    - Bank shall review and evaluate previous vendor contractual agreements for security protections. Helpful documents:
    - Rules for the development of software and systems should be established and applied to developments within the organization. Secure development policy is used to ensure that development environments are themselves secure and that the processes for developing and implementing systems and system changes encourage the use of secure coding and development practices. Such policies will include showing how security needs to be considered at all stages of the development lifecycle from design through to live implementation. Specific coding languages and development tools have different vulnerabilities and require different “hardening” techniques accordingly and it is important that these are identified and agreed upon and developers are made aware of their responsibilities to follow them.

Policy Exception

1. A formal exception document should be approved by AGM IT.
2. Any exception in existing Software Development needs to be recorded in the Software Exception file with detailed reasoning

Roles & Responsibility

1. IT Officer/Vendor being responsible for monitoring, review, and maintenance of all the records, logs etc. and escalate in case of any emergency.
2. IT Manager being responsible for periodical review of all the records, logs etc. and take necessary decision if required.
3. AGM IT being responsible for any kind of escalation.

15. UIDAI/Aadhaar related Policy:

The Following portion of the document added to the IS Policy illustrates the Policy of the bank related to UIDAI/Aadhaar.

Uttarakhand State Co-Operative Bank Ltd. will comply with all Information Security Policy and Procedures addressing the security aspects of Aadhaar as defined under the Aadhaar Act Regulations and specifications.

Certain Specific Processes/Policies are defined below:

I. Bank will take the consent of Aadhaar Card Holder for Authentication and shall save the consent forms with the consent details for a period of at least 7 Years. Similarly, the logs regarding Authentication will be saved for 2 years Online and 5 years Archived.

II. For any given Aadhaar number holder, whose identity information was collected, the bank will be able to demonstrate that consent was taken and disclosure of information was made whenever required for any Regulatory requirement.

III. Aadhaar card holder will be intimated when the request for NPCI mapping of account number has been initiated by Uttarakhand State Co-Operative Bank Ltd. via SMS/Email

in 24 Hours.

IV. Uttarakhand State Co-Operative Bank Ltd. will Whitelist any application (Web/ Android/ iOS or any other client application) in public domain with Uttarakhand State Co-Operative Bank's name, application name, logo and URL etc.

V. Uttarakhand State Co-Operative Bank Ltd. shall be fully responsible for the misuse and illegal sharing of the license key in production or pre-production environment of UIDAI. Uttarakhand State Co-Operative Bank Ltd. shall not allow any other agency to perform authentication by sharing its license key. Uttarakhand State Co-Operative Bank Ltd. shall not forward authentication request using PID block captured by unaudited application using their license key. For every sub-AUA if any, a separate license key shall be used.

VI. Uttarakhand State Co-Operative Bank Ltd. understands that in case, Authority notices misuse or illegal sharing of license key by the AUA / KUA / sub-AUA, Authority shall terminate the license of the AUA / KUA and other actions including criminal prosecution shall be taken against AUA / KUA as well as the sub AUA and other entities as per Aadhaar Act and its Regulations.

VII. Uttarakhand State Co-Operative Bank Ltd. shall not perform any test transactions on UIDAI's production environment. Any test transaction will be performed on UIDAI's pre-production environment only.

VIII. In all authentication applications deployed by Uttarakhand State Co-Operative Bank Ltd. and sub-AUA, name of Uttarakhand State Co-Operative Bank Ltd. shall be clearly displayed to the Aadhaar number holder.

IX. Uttarakhand State Co-Operative Bank Ltd. shall ensure that it has provisions for periodic reviews and assessments of its systems, infrastructure, etc., by a UIDAI empanelled or CERT-In empanelled agency to ensure compliance with Aadhaar Act, Regulations and specifications on annual basis or as defined by UIDAI.

X. As a part of the Exception handling process if fingerprint is not working at all then alternate option of iris or OTP will be provided for Aadhaar Authentication.

XI. Uttarakhand State Co-Operative Bank will comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016 in case it wants to surrender its UIDAI License keys.

XII. Uttarakhand State Co-Operative Bank Ltd. will ensure that Team working on Aadhaar based applications development is aptly qualified (Graduate is Minimum requirement).

XIII. Uttarakhand State Co-Operative Bank will comply with all the requirements of UIDAI Circular No. 06 of 2018, K- 11020/217/2018-UIDAI (Auth-I), dated 04th June 2018

(Implementation of Virtual ID, UID Token and Limited KYC) by implementing the latest Authentication API 2.5, EKYC API 2.5 and OTP Request API 2.5 for VID and UID Token.

XIV. Uttarakhand State Co-Operative Bank will comply with all the circulars, notices, mandates issued by UIDAI from time to time.

As an AUA, Uttarakhand State Co-Operative Bank understands and will always follow any of the following Do's and Don'ts related to UIDAI/Aadhaar Applicable to it as stipulated by UIDAI:

Do's:

1. Read Aadhaar Act, 2016 and its Regulations carefully and ensure compliance of all the provisions of the Aadhaar Act, 2016 and its Regulations.
2. Ensure that everyone involved in Aadhaar related work is well conversant with provisions of Aadhaar Act, 2017 and its Regulations as well as processes, policies specifications, guidelines, circular etc issued by UIDAI from time to time.
3. Create internal awareness about consequences of breaches of data as per Aadhaar Act, 2016.
4. Follow the information security guidelines of UIDAI as released from time to time.
5. Full Aadhaar number display must be controlled only for the Aadhaar holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
6. Verify that all data capture point and information dissemination points (website, report etc) should comply with UIDAI's security requirements.
7. If agency is storing Aadhaar number in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using HSMs. If simple spreadsheets are used, it must be password protected and securely stored.
8. Access controls to data must be in place to make sure Aadhaar number along with personally identifiable demographic data is protected.
9. For Aadhaar number look up in database, either encrypt the input and then look up the record or use hashing to create Aadhaar number-based index.
10. Regular audit must be conducted to ensure Aadhaar number and linked data is protected.
11. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.

12. An individual in the organization must be made responsible for protecting Aadhaar linked personal data. That person should be in charge of the security of system, access control, audit, etc.
13. Identify and prevent any potential data breach or publication of personal data.
14. Ensure swift action on any breach personal data.
15. Ensure no Aadhaar data is displayed or disclosed to external agencies or unauthorized persons.
16. Informed consent - Aadhaar holder should clearly be made aware of the usage, the data being collected, and its usage. Aadhaar holder consent should be taken either on paper or electronically.
17. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure all Aadhaar holders are able to use it effectively.
18. Multi-factor for high security - When doing high value transactions, multifactor authentication must be considered.
19. Create Exception handling mechanism on following lines
20. It is expected that a small percentage of Aadhaar holders will not be able to do biometric authentication. It is necessary that a well-defined exception handling mechanism be put in place to ensure inclusion.
21. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.
22. If the scheme is family based (like PDS system), anyone in the family must be able to authenticate to avail the benefit. This ensures that even if one person is unable to do any fingerprint authentication, someone else in the family is able to authenticate. This reduces the error rate significantly.
23. If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card or PIN or other means.
24. All authentication usage must follow with notifications/receipts of transactions.
25. All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, sms, physical-center, etc.).
26. Get all the applications using Aadhaar audited & certified for its data security by appropriate authority such as STQC/CERT-IN.
27. Use only STQC/UIDAI certified biometric devices for Aadhaar

authentication.

Dont's:

1. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc. Publication of Aadhaar details is punishable under Aadhaar act.
2. Do not store biometric information of Aadhaar holders collected for authentication.
3. Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones or tablets or any other devices.
4. Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other certificate/document. Aadhaar number if required to be printed, Aadhaar number should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed.
5. Do not capture/store/use Aadhaar data without consent of the resident as per Aadhaar act. The purpose of use of Aadhaar information needs to be disclosed to the resident.
6. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.
7. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room
8. Do not permit any unauthorized people to access stored Aadhaar data

Do not share Authentication license key with any other entity.

16. Risk Management Policy

Objective & Purpose

The purpose of this policy is to establish a systematic approach to identify, assess, treat, and monitor risks to the bank's information assets, ensuring residual risk is within acceptable limits and aligned with business objectives.

Policy Statement

Bank shall adopt a formal risk management methodology in line with ISO 27005 and NIST SP 800-30.

All information assets, systems, and services shall undergo risk assessment at least annually or when significant changes occur.

Risks shall be classified as Low, Medium, High, or Critical based on impact and likelihood.

Risk treatment options shall include: mitigate, transfer, avoid, or accept.

A Risk Register shall be maintained by the IS Officer and reviewed by the CISO quarterly.

Residual risk acceptance shall be documented and approved by Senior Management.

Procedures

1. Identify threats, vulnerabilities, and impacts on assets.
2. Assess likelihood and impact using a risk matrix.
3. Document results in Risk Register.
4. Implement mitigation measures with clear ownership and timelines.
5. Report to Board of Directors on risk posture quarterly.

Policy Exceptions

Exceptions shall be documented with justification and approved by the CISO.

Roles & Responsibility

IT Manager: Perform risk assessments, maintain risk register.

AGM: Review assessments and mitigation plans.

CISO: Approve risk treatment, escalate critical risks to Management.

17. Cryptography Policy

Objective & Purpose

To ensure consistent and effective use of cryptography to protect confidentiality, integrity, and authenticity of information.

Policy Statement

Bank shall use only strong, industry-accepted cryptographic algorithms (AES-256, RSA-3072/4096, SHA-256 or higher, ECC curves P-256 or above).

Encryption must be applied for data at rest, data in transit, and sensitive data in processing.

Key management practices must ensure secure generation, storage, distribution, rotation, and destruction of cryptographic keys.

Default or vendor-provided keys must not be used in production.

Digital signatures and certificates must be obtained from trusted Certificate Authorities (CAs).

All cryptographic implementations must comply with RBI, CERT-IN, and ISO standards.

Procedures

Maintain a Key Management Register.

Rotate encryption keys annually or upon suspected compromise.

Use Hardware Security Modules (HSM) or equivalent secure key storage.

Document approval for all cryptographic use cases.

Policy Exceptions

Exceptions must be formally approved by the CISO and documented with risk justification.

Roles & Responsibility

IT Manager: Implement encryption controls.

AGM: Validate secure key management.

CISO: Ensure compliance with standards and approve exceptions.

18. Vulnerability Management Policy

Objective & Purpose

To identify, assess, prioritize, and remediate vulnerabilities to minimize the risk of exploitation.

Policy Statement

Vulnerability scans (internal and external) must be conducted quarterly, and after major system changes.

Critical vulnerabilities must be remediated within 15 days, High within 30 days, Medium within 60 days, and Low within 90 days.

Vulnerability scanning tools must be updated with latest signatures.

Reports must be reviewed by IS Officer and submitted to CISO.

Procedures

1. Perform automated scans using approved tools.
2. Conduct penetration testing annually and after major upgrades.
3. Track remediation progress in Vulnerability Register.
4. Verify closure of vulnerabilities by re-scanning.
5. Report status to Audit Committee.

Policy Exceptions

Any exception due to business impact must be recorded with compensating controls and approved by the CISO.

Roles & Responsibility

IT Manager: Conduct scans, validate remediation.

AGM: Review scan results, track remediation.

CISO: Approve exceptions, report to Board.

19. Privacy & PII Handling Policy

Objective & Purpose

To safeguard Personally Identifiable Information (PII) in compliance with privacy laws, regulations, and ISO27701.

Policy Statement

The Bank shall appoint a Data Protection Officer (DPO).

A PII Processing Register shall be maintained to track collection, use, storage, and disposal of PII.

Consent from customers must be obtained prior to processing their PII.

Data Subject Rights (access, correction, deletion, portability) must be honored within regulatory timelines.

Privacy Impact Assessments (PIA/DPIA) shall be conducted for new projects handling sensitive PII.

Third-party contracts must include privacy clauses ensuring secure handling of PII.

Procedures

Collect only necessary PII for business operations.

Encrypt PII in storage and transit.

Define retention periods and securely dispose expired data.

Respond to Data Subject Requests (DSRs) within 30 days.

Review and approve PIAs before deployment of new systems.

Policy Exceptions

Any exception to handling of PII must be approved by the DPO and CISO with documented justification.

Roles & Responsibility

All Employees: Protect PII and follow handling procedures.

IT Manager: Ensure secure storage and transmission.

DPO: Oversee compliance with privacy requirements.

CISO: Monitor overall privacy governance.

20. Cloud Security Policy

Objective & Purpose

To ensure the security, compliance, and resilience of data, applications, and services hosted in cloud environments.

Policy Statement

Cloud vendors must undergo security assessment before onboarding.

Data residency and sovereignty requirements must be documented and approved by CISO.

Bank shall define responsibilities under the shared responsibility model with each provider.

Multi-tenancy risks must be addressed through encryption and tenant isolation.

Upon contract termination, bank must retrieve all data and ensure secure deletion by vendor.

Continuous monitoring must be implemented for cloud services.

Procedures

Perform Cloud Risk Assessment before adoption.

Document Data Location and Processing Agreements.

Implement Cloud Access Security Broker (CASB) for monitoring.

Maintain exit plan for vendor lock-in scenarios.

Review vendor audit reports annually (SOC 2, ISO27017/18).

Policy Exceptions

Exceptions must be approved by CISO and documented with risk mitigation.

Roles & Responsibility

IT Manager: Manage vendor coordination.

AGM: Validate controls and compliance.

CISO: Approve vendor selection, review annual security reports.

21. Metrics & Reporting Policy

Objective & Purpose

To establish measurable indicators for cybersecurity effectiveness and ensure management oversight.

Policy Statement

Bank shall define Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) for cybersecurity.

Metrics shall include patch compliance %, incident response time, % of closed audit findings, number of unresolved critical vulnerabilities, and user awareness training completion.

Reports shall be generated monthly and submitted to the CISO.

Quarterly dashboards shall be presented to Senior Management and the Board.

Procedures

Collect data from monitoring tools, incident logs, training systems.

Prepare KPI/KRI dashboard.

Review and update metrics annually based on evolving threats and business objectives.

Policy Exceptions

Any missing metrics must be justified and approved by CISO.

Roles & Responsibility

IT Manager: Collect and validate raw data.

AGM: Consolidate and analyze metrics.

CISO: Report to Board, define new metrics as needed.

****