MBANK
The Muslim Co-operative Bank Ltd. Pune

# The Muslim Co-Operative Bank Ltd.

# Information Security Management System Policy

## Document Control

| Reference Number | Version | Release Date | Document Classification |
|---|---|---|---|
| PL-01 | 1.0 | 31/08/2021 | 1. Yearly Review. |
| | 2.0 | 18/10/2022 | 2. Created detailed policies for all IS and Cyber Security Requirements |

## Table of contents

# 1. Introduction

The Information Security Policy provides an integrated set of protection measures that must be uniformly applied across The Muslim Co-operative Bank Ltd. to ensure a secured operating environment for its business operations.

Customer Information, organizational information, supporting IT systems, processes and people that are generating, storing and retrieving information are important assets of Bank. The availability, integrity and confidentiality of information are essential in building and maintaining our competitive edge, cash flow, profitability, legal compliance and respected bank image.

As a result, the Information Security Management System (ISMS) Framework is constructed inline and according to ISO/IEC27001:2013 standards. The policbany will detail the following:

- The objective of Information Security.
- Identify all elements that constitute Information Security.
- Specify the various categories of Information Assets, equipment, services and processes subject to this policy.
- Indicate the responsibilities of the various roles in which all users of Bank computing services may function.
- Identify appropriate levels of security through other policies and procedures with reference to ISO/IEC27001:2013 standards.

# 2. Purpose

The purpose of this document is to demonstrate Bank's Top Management commitment with respect to the ISMS by ensuring that its scope and objectives are established, are compatible with the strategic direction of the Bank and to ensure the integration of the ISMS requirements into Bank 's Information Services and processes.

The purpose of this document is also to define the context, scope and boundaries of the Information Security Management System (ISO 27001:2013) implementation.

# 3. Definitions

| | |
|---|---|
| **Appropriate Use** | Appropriate Use means the behavior and conduct of Users when using the IT Infrastructure as laid down by the Bank. |
| **Authorized Equipment** | Authorized Equipment means devices that are allowed to access Information Assets such as desktops, laptops and other mobile devices authorized for use by the Bank. |
| **Availability** | Availability means ensuring that authorized Users have access to Information Assets and associated assets when required. |
| **Change Management** | Change Management means the definition and implementation of procedures and/or technologies to effect a Change. |
| **Bank Services on Personal Devices** | Applications and underlying data that have been authorized by the Bank to be accessed or used from Personal Devices. |
| **Confidentiality** | Confidentiality means ensuring that Information Assets are accessible only to those who are authorized to have access. |
| **Bank / Bank** | The Muslim Co-operative Bank Ltd. the organisation.<br>This excludes subsidiaries and associated companies where Bank does not manage its Information Technology. |
| **Information Assets** | Information Asset means information relating to Bank's business held in electronic format by the Bank as well as any specific building, equipment, communication channel, repository and medium used in connection with capturing, processing, transmitting and storing such information - whether these are owned, leased, hired or rented. |
| **Information Owner** | Information Owner means a named person (usually the head of a function) who is nominated to be responsible for the Information Asset. An Information Owner may delegate responsibility for implementing controls such as Information Asset classification and access management but will retain accountability for the Information Asset. If the named Information Owner is unavailable, then the responsibility will be temporarily entrusted to a more senior person within the function. |
| **Integrity** | Integrity means safeguarding the accuracy and completeness of Information Assets and processing methods. |
| **Least Access** | Least Access means the minimum access that can be granted in order that a User may properly and effectively perform the duties specified for the role. |
| **Mobile Device** | Mobile Device means any portable computing device installed with corporate standard software, supplied to a User by the Bank for use in connection with the Bank business. Mobile Device allows a User to connect to the IT Infrastructure from the office, home or whilst traveling. Mobile Devices include laptops, tablet PCs and handheld computers (Blackberry, Pocket PCs, smartphones, PDAs, etc). |
| **Policy** | Policy means a written statement of direction of the agreed best way to achieve the security goals relating to the Information Assets of the Bank. |

| | |
|---|---|
| **Procedure** | Procedure means a set of actions that has been accepted as the official way of proceeding with something within the Bank |
| **Sensitive Information** | Sensitive Information means any information that is classified as confidational or designated for restricted access. |
| **Third Party** | An external entity with whom the Bank has, or, where the context permits, intends to have, a contractual relationship. This also includes any employees, contractors, subcontractors or agents (authorised employees) whose services are used by the Third Party to meet their contractual obligations to Bank. |
| **User** | User means any person or organisation (excluding customers), who operates or interacts directly or indirectly with the bank Infrastructure and / or has access by any means to any Information Assets.<br>Internal users include persons classified as bank staff or contractors employed directly by or retained by the Bank.<br>External users include suppliers, business partners, vendors, Third Party service providers their employees and their agents who interact with any Information Asset. |
| **User ID** | User ID is the credential which identifies a User during login into the Bank's IT Infrastructure. User is provided access to the Information Assets through this User ID. A User ID can be a combination of any alphabets or numbers. |

# 4. Context of the Organization

## 4.1. Understanding the Organisation and its Context

The Muslim Co-operative Bank Ltd. Is co op Bank and providing banking services.

- The organisation provides Banking related services.
- As such Information Technology helps the Bank to enhance its activities and functions.
- The Top Management ( BOD) shall define the Bank's information risk appetite.

## 4.2. The Needs and Expectations of Interested Parties

### 4.2.1. General

The ISMS in place to minimize the risks to the Information Assets and thereby reduce the impact on Bank's business operations.

### 4.2.2. Internal Parties

- Top Management requires all Information Assets to be handled and processed in a secure manner.
- Employees expect the bank to secure their data and provide a secure work environment.

### 4.2.3. External Parties

- Customers expect bank to have a secure workplace and work practices thereby ensuring that they are not vulnerable to security attacks/breaches from bank.

### 4.2.4. Legal and Regulatory Requirements

- Bank must ensure that it complies with the relevant laws of The Republic of India, especially the RBI regulations.

# 5. Scope of ISMS

The following is in the scope of the ISMS:

- Banking Services provided for customers through Head Office and Branch Offices.
- The following locations
  - The Muslim Co-operative Bank Ltd –Admin office pune

    Branches- Pune(13),Ahmed Nagar, Baramati, Solapur, Junnar, Nasik, Bhiwandi, Shreerampur & Lonawala.

# 6. Objective of the ISMS

Bank has set the below objectives of establishing the ISMS:

1. The management of the security of its information.
2. The responsibilities of various teams in securing the information.
3. Comply with business, legal, regulatory requirements pertaining to information security.
4. Continually strengthen and improve the overall capabilities of the ISMS.

To implement the above, Bank through, ISO/IEC 27001:2013 standard, will:

1. Ensure all risks rated as ‘High’ are mitigated within six months. Risks rated as ‘Caution’ and ‘Medium’ are mitigated within a year.
2. Ensure all employees and contract staff undertake the information security awareness training at least once every year.
3. Ensure all information security incidents are recorded and addressed with appropriate corrective actions. 95% of such incidents must be addressed within their agreed service level durations.
4. Ensure all information systems are assessed for vulnerabilities at least once a year. ‘High’ risk vulnerabilities must be addressed within 2 months of it being reported. All other vulnerabilities must be addressed within 9 months of them being reported.
5. Apply relevant vendor-provided security hotfixes and bug fixes within 3 months of their release.
6. Assess compliance to ISMS, through audits at least once a year.
7. Ensure all information security policies and procedures are reviewed once a year.

# 7. Information Security Policies

At Bank considering the security requirements, Information Security policies have been framed based on a series of security principles. All the Information Security policies and their need have been addressed below:

## 7.1. Asset Management

Information Assets must be accounted for and have a nominated asset owner.

Owners must be identified and catalogued for all Information Assets and the responsibility for maintenance of appropriated controls must be assigned.

The implementation of specific controls may be delegated by the owner as appropriate but the owner remains accountable for the proper protection of the assets.

**Asset Inventory**

Bank Information Assets must be listed in an asset register. Each asset must be clearly identified individually and (if appropriate) collectively in combination with other assets to form an identifiable Information asset.

The Asset inventory must include all information necessary in order to recover from a disaster or abe able to trace and asset. The register must contain the following information as a minimum:
Identification (Item code on all the assets)

- Description
- Asset Type
- Owner
- Custodian
- User
- Inventory holder
- Location/Zone
- Asset classification (based on criticality)
- Warranty details

**Return of Assets**

The termination process should be formalized to include the return of all previously issued software, corporate documents, and equipment.

Other organizational assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also need to be returned.

In cases where an employee, contractor or third-party user purchases the organization’s equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.

In cases where an employee, contractor or third-party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

**Removal of assets**

Equipment, information or software should not be taken off-site without prior authorization.

Employees, contractors and third-party users who have authority to permit off-site removal of assets should be clearly identified.

Time limits for equipment removal should be set and returns checked for compliance.

Where necessary and appropriate, equipment should be recorded as being removed off-site and recorded when returned.

Spot checks, undertaken to detect unauthorized removal of property, may also be performed to detect unauthorized recording devices, weapons, etc., and prevent their entry into the datacentre premises.

Such spot checks should be carried out in accordance with relevant legislation and regulations.

Individuals should be made aware is spot checks are carried out, and the checks should only be performed with authorization appropriate for the legal and regulatory requirements.

Ref: Asset Management Policy
Removable Media Policy

## 7.2. Information Classification and Handling

Information must be classified by its Information Owner as per the Information Classification as described in the document control procedure.

The classification of the information is done on the basis of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modifications.

Owners of the information assets must be accountable for their classification.

Owners must be responsible for the review of the asset classification at least once a year or before any major change involving the respective asset.

The level of protection for the information and asset must be depending on the analysis based on confidentiality, integrity and availability for the asset and information that is being considered.

The classification of information and assets must be done throughout their life-cycle.

The following classification applies to the information and information processing and storing assets:

| Classification Title | Description | Examples |
|---|---|---|
| **Confidential** | If this information is leaked outside Bank, it will result in major financial and/or image loss.<br>Compromise of this information will result in statutory, legal non- compliance.<br>Information to be shared with few named individuals only (on need to know basis). | Legal contracts<br>Client communication<br>Client information<br>PII data<br>System passwords / administrative passwords etc.<br>Audit reports,<br>Budget plans, review, expenditure reports<br>Agreements<br>Risk assessment and risk treatment register,<br>Security incident register, |

| | | |
|---|---|---|
| | | Backup data |
| **Internal** | If this information is leaked outside Bank, it will result in moderate financial and/or image loss<br>Information to be shared only within Bank. | Strategy documents and plans<br>Policies and procedures<br>Configuration databases<br>Internal mails and memos<br>Training material<br>Attendance records<br>Newsletters |
| **Public** | Non availability will have no effect if this information is leaked outside Bank, it will result in no loss.<br>Information can be shared with public. | Authorized Information published through official press release<br>All public information<br>Information released on bank's website |

Information retention must be done in accordance with applicable law, regulations and contractual requirements.

All information must be labelled and handled as per Information Classification, Labelling and Handling controls as described in the ISMS Controls Manual document.

The information labelling must cover non-electronic media (Ex: physical documents) and electronic media (e.g: Emails, CDROM, Tapes, Word Documents, Excel, PPTs). The physical labelling format must be easily distinguishable and readable.

All information for disposal must be approved and recorded.

After the retention period is complete, the content from the tape and disk must be erased before reusing or disposing the media.

Any critical information contained in media and sensitive documents must be stored in fireproof and locked cabinet.

Devices containing Sensitive Information must be physically destroyed when no longer required.

Procedures for handling and storage of Sensitive Information must be established in order to protect it from unauthorized disclosure or misuse.

All media device being transported must be protected from unauthorized access, misuse or corruption.

Users must be made aware of protecting the exchange of Sensitive Information during voice and video communications.

Sensitive documents stored in soft copy format must be adequately safeguarded by the information owner through methods like password protection or encryption as deemed appropriate.

All documents from external origin should also be classified.

If Sensitive Information is lost, disclosed to unauthorized parties, suspected of being lost or disclosed to unauthorized parties, its owner must be notified, and a security incident report must be initiated immediately.

Users must share the Sensitive Information through discussions and electronic means only with personnel who are authorized to use the information by Information Owner.

Information Owner must be responsible for safeguarding information by exercising appropriate controls.

Ref: Information Classification policy

## 7.3. Acceptable Use

This Policy has been prepared and implemented to ensure that all the users and staff at Bank are aware of their responsibilities towards the IT Resources of Bank. This Policy details the end-users aware of their responsibilities and the acceptable use of the IT Resources of Bank.

Ref: Acceptable IT Usage Policy

## 7.4. Access Control

Data must have sufficient granularity to allow the appropriate authorized access. Access to Information Assets must be on a 'least access' principle based on a 'need to know' basis. The Access Control Policy addresses this need.

Ref: Access Control Policy

## 7.5. Password Security

Users must strictly adhere to the password policy as described below. The following policy must be considered as the minimum baseline password policy for implementation across all IT infrastructure and applications in Bank.

**Users must:**

- Change their systems, admins and server-level passwords (e.g. root, enable, administrator, application administration accounts, etc.) at least every 45 days.
- Change their normal user accounts' password (e.g. Webmail, Active Directory / Workgroup, etc.) at least every 90 days.
- Not share their user ID and password with anyone else. Confidentiality of passwords must be maintained.
- Set a password with a minimum of 8 characters.
- Set strong passwords. A strong password has a combination of all of the below:
    - Lower case
    - Upper case
    - Numbers
    - Special characters.
- Not set weak or easily guessable passwords (for example do not set passwords such as Yourname@123 or Bank@123).

**Account Lockout:**

- Account lockout occurs in an event of 3 continuous failure login attempts.
- System Lockout: if system is not in use for more than 600 seconds, system will be locked out. User must enter his/her account password to unlock the system.

Ref: Password Policy

## 7.6. Change Management

Changes to information technology facilities and systems should be controlled in order to ensure that changes made to a production component are applied in a secure and consistent manner.

All Changes must be reviewed and approved by the relevant stakeholders before implementation.

Ref: Change Management Policy

## 7.7. Network Security

Appropriate controls must be established to ensure the security of data in private and public networks, and the protection of connected services from unauthorized access. Bank Solutions' Network infrastructure needs to be protected from unauthorized access.

A range of security controls is required in computer networks to protect these environments. Considering the above, the network security policy has been framed for Bank .

Ref: Network Security Policy
Design and Implementation of Security in Systems and Networks Policy

## 7.8. Backup & Recovery

In order to safeguard information and computing resources from various business and environmental threats, systems and procedures have been developed for backup of all business data, related application systems and operating systems software on a scheduled basis and in a standardized manner across Bank.

The backup and recovery procedures must be automated wherever possible using the system features and be monitored regularly.

The backup data must be periodically tested for integrity by following process of restoration.

Ref: Backup Policy

## 7.9. Physical & Environmental security

To prevent unauthorized physical access, damage and interference to the organisation's premises and information, critical or Sensitive Information processing facilities must be housed in a secure area, protected by secure parameters, with appropriate entry controls.

Ref: Physical -Environmental Security Procedure

## 7.10. Mobile Device

Adherence by all Users authorized for accessing and managing information including email through handheld devices.

Usage of any type of mobile devices like laptops, smart phones, any mobile device with an embedded operating system enabling remote connectivity/storage/ synchronization features.

Users must be solely accountable for the loss of information from the handheld devices, in case of a theft or loss of device.

Users must take due care of mobile devices against theft of devices.

Users must necessarily use a power-on password in their Mobile device as the first level protection measure.

Users should store information which is confidential/very confidential or covered by a privacy or regulatory act, in an encrypted manner ONLY, as per official needs.

Any handheld devices issued by bank should be used for official purposes and should be loaded with approved software only.

Ref: Mobile device Security Policy

## 7.11. Telecommuting / Remote Access

Telecommuters (employees working outside Bank  workplaces connecting to Bank or to Client networks using Bank assets) must configure their remote working environment to ensure compliance with Bank and Clients security standards.

Remote access to Bank IT resources from public network must be allowed only after successful identification and authentication of users.

Remote access to intranet applications must be provided only through secured communication channels such as SSL or IPSEC.

Access to critical applications in the intranet must be granted only with 2 factor authentications.

In case of user separation from Bank's services, user credentials must be deleted (to be disabled in the case of SecurID tokens) on the last day of user promptly by the respective Personnel (IT/Project head).

VPN access to Bank’s resources must be authenticated by the Active Directory.

User Authentication for establishing VPN session must be encrypted.

Remote access logs must be maintained for a period of 45 days on file server and then backed up for 3 months on secondary storage.

Deny access logs on remote access service must be monitored by Network/ Security Operations staff for taking appropriate Preventive actions.

Adequate care must be taken by mobile users when mobile computing facilities are used in public places, meeting rooms and other unprotected areas.

Remote access users must not extend access to Bank Intranet resources to others such as friends or family in any form.

Remote Access through VPN to administer critical IT resources must be activated after evaluation of risk with 2 factor authentications.

Dial-out/Dial-in connectivity from/to the Bank backbone as well as the restricted network must be allowed ONLY with written approval from the Network Operations Manager/Security Operations Manager.

User must not simultaneously connect the desktop/laptop to any two types of networks in any form. For example, Users must refrain from connecting Bank's LAN and Internet using dial-in or VPN or through any other form of connectivity, simultaneously.

Ref: Remote User Access Policy

## 7.12. Log Management

Bank must maintain secure log for infrastructure assets with appropriate controls and segregation of duties.

Logs must contain sufficient information to establish occurred event(s), sources of event(s), outcomes of the event(s) and their corresponding timestamp(s).

IT Systems logs must be retained for 30 days online and archived for 90 days or as per applicable legal and contractual obligations. Physical access logs must be available for 90 days and CCTV records must be retained for 30 days.

Logs pertaining to security incidents must be retained for minimum of 1 year or as per applicable legal and contractual requirements.

Bank reserves the right to perform lawful monitoring of systems, networks and communications.

Ref: IT Operations, Network Security Monitoring Procedure

## 7.13. Application Security

Software applications must be developed in accordance with industry best practices and adhere to guidelines for developing the secure web.

Security assessment must be conducted before moving code to production.

Development, testing and production environments must be segregated.
Ref: Secure Development Procedure

## 7.14. Anti-Malware

All the workstations and servers that are in Bank network must be installed with legit antivirus software..

Proactive protection or Real-time protection must be enabled in all the machines and should be scheduled (from the server side) to perform virus scans at regular intervals.

Virus definition updates must be configured in the antivirus Client to occur on a daily basis.

Firewall/Router must be configured to block certain ports which are liable for any malicious network attacks. It is not advised to open ports in Firewall unless it is required and the port should be secured with other firewall rules.

Antivirus server must be checked regularly for any threats detected & clients must be monitored on a regular basis from the antivirus server for any threats or issues with the Proactive Threat protection.

If end user receives any virus alert or suspects any unexpected errors probably related to malicious activity, it should be immediately brought to the notice of IT Support who then have to inspect the issue and terminate a possible virus activity immediately without delay.

Any intentional activity to create or distribute a malicious code inside the organization is strictly prohibited.

As a proactive measure, USB mass storage support must be disabled in all the workstations to avoid unnecessary intrusion from outside.

Any data which is brought from outside the organization to Bank must be scanned with the Virus scanner.

In order to avoid any security holes in the operating system which leads to a virus attack, security patches must be applied to the operating systems.

IT Support team is responsible to keep track of the software updates (versions) or patches provided by the Antivirus vendor and enable it in each and every machine in the organization on a timely basis.

Ref: Malware protection Policy

## 7.15. Third Party / Supplier Security

Outsourcing of any service must go through risk assessment.
Prior to outsourcing, suppliers must undergo security, privacy and continuity due diligence.
Suppliers must be contractually bound to adhere to security and privacy requirements.
Suppliers and Third Party (including Customers) remote access must only be provided after approval by Head of Information Security.

Ref: Supplier and Third Party security policy

## 7.16. Security Incident Management

Security incidents must be reported through the incident reporting system (Helpdesk)/ incident management process or procedure.

Security incident response must include categorization, containment, remediation, analysis and reporting to management.

Users must be made aware of procedures for reporting a Security incident.

Timely notifications must be sent to the required stake holders based on applicable regulatory and contractual requirement.

All incidents must be categorized based on the severity, type and suitable corrective actions initiated based on this severity.

Security incidents must be analysed, and corrective actions taken to minimize recurrence of an incident.

Security incidents requiring forensic investigations must be conducted by the Chief Information Security Officer (CISO) or person authorized by the CISO.

Periodic report on the security incidents must be presented to the management.

Specific disciplinary actions must be initiated to address security incidents.

Ref: Incident Management Procedure
Incident Management Policy

## 7.17. Business Continuity and Disaster Recovery

Business continuity procedure(s) must incorporate security requirements.

The Business Critical facilities and IT infrastructure must have built-in redundancy for security controls.

Business Continuity Plan (BCP) must be developed and maintained by the respective owner predefined in the BCP plan.

Ref: -Business continuity Policy
Business Impact Analysis Policy

## 7.18. IT communications and Operations Management

Purchase and installation of IT equipment must be approved by the IT department.

Purchase and installation of software for IT equipment must be approved by the IT department.

The IT department should ensure documentation of the IT systems according to Bank standards.
Changes in IT systems should only be implemented if well-founded from a business and security standpoint.

The IT department should have emergency procedures in order to minimize the effect of unsuccessful changes to the IT systems.

Operational procedures should be documented. Documentation must be updated following all substantial changes.

Ref: IT Operations, Network Security Monitoring Procedure

## 7.19. Patch Management

The information related to patches must be obtained from authorized and genuine sources such as but not limited to supplier mailing lists/websites, Security Alert announcements/bulletins like SANS & CERT and Virus bulletins.

The criticality of patches must be defined based on risk ranking either by the vendors and/or by the Bank (network) team.

Bank must carry out an assessment to understand the impact of vulnerabilities to Bank’s IT environment.

Patches must be tested in the test environment before actual implementation in the production environment by the system owners. Exceptions to this requirement must be recorded and maintained in case, testing is not feasible.

Patches must be implemented by the system owners at the earliest to all the vulnerable systems after assessment for applicability in Bank’s IT environment. Critical patches must be installed within 30 days of release by the software vendor.

Patch implementation information must be announced to the intended audience before the implementation in the production environment by the system owners.

Change and Release management procedures must be followed for patch deployment.

Patch implementation steps must be monitored on a periodic basis and patch completion records must be archived for future reference with relevant details.

Suitable tools and technologies must be utilized for carrying out patch management in the multi-vendor environment.

Security incident management procedure must be adhered, for potential security issues observed in the patch management.

Appropriate and authorized scanning mechanisms must be deployed to report the status of patch implementation in the IT systems and applications on daily or need basis.

Ref: IT Operations, Network Security Monitoring Procedure

## 7.20. Media Disposal

All disposal of removable media drives should be done in caution so as to ensure that no information gets transferred to unauthorized users by any means.

All information to be erased from equipment prior to disposal or reuse. All media to be disposed off securely and safely when no longer required.

Formal procedures for the secure disposal of media should minimize the risk of sensitive information leakage to unauthorized persons.

Media containing sensitive information should be stored and disposed of securely and safely, e.g. by shredding, or erased of data for use by another application within the organization.

Procedures should be in place to identify the items that might require secure disposal.

It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items.

Disposal of sensitive items should be logged where possible in order to maintain an audit trail.

All information for disposal must be approved and recorded.

After the retention period is complete, the content from the tape and disk must be erased before reusing or disposing the media.

Any critical information contained in media and sensitive documents must be stored in fire proof and locked cabinet.
Sensitive documents which are no longer required must be destroyed as per the Information Classification, Labelling and Handling procedure by Information owner.

Devices containing sensitive information must be physically destroyed when no longer required.

Procedures for handling and storage of sensitive information must be established in order to protect it from unauthorized disclosure or misuse.

All Media device being transported must be protected from unauthorized access, misuse or corruption.

Users must be made aware of protecting the exchange of sensitive information during voice and video communications.

Information owner must be responsible for safeguarding information by exercising appropriate controls.

Ref: Asset Disposal and Destruction Policy

## 7.21. Clean and Clear Desk

Employees should take note that any documents/removable media left unattended on desk or public areas are prone to security and fire hazards.

Copier or fax machines should be located in secure areas and due precaution should be taken while using these equipment's for confidential data handling.

Employees should ensure that confidential documents/ removable media are not left unattended on work desks, conference rooms, in the copiers or public areas.

Fax messages received should not be left on the machine for long time and should be collected immediately.

Confidential information when printed should be cleared from the printer immediately by the concerned employee.

Only required copies should be printed and bulk printing should be avoided.

Filing of papers should be prompted to avoid loss of confidential information.

Individuals should keep cabinets/side tables under lock and key all the time.

Confidential papers when not required anymore should be shredded by individual employee immediately.

Confidential data in the removable media should be immediately deleted when not required any more. In case of read only media (eg: CD/DVD) should be destroyed.

Facilities Management team should provide dustbins to employees to facilitate disposal of waste paper.

Wherever paper is placed for reusability (such as for writing pads), care should be taken so that confidential information such as copies of sensitive mails, financial and sales data are not lost or exposed to unauthorized person.

It is Facilities Management team's responsibility to dispose shredded and other waste paper.

Screens must be locked by the user when away from their workstation, irrespective of the amount of time spent away from the unattended workstation.

Workstation must be locked out when there is no activity for a pre-determined period of time and must be password protected for reactivation.

Ref: Clear Desk, Clear Screen Policy

## 7.22. Internal Audits

Bank must conduct internal audits at planned intervals to provide information on whether the information security management system:

1. conforms to
   a. the organization's own requirements for its information security management system; and
   b. the requirements of this International Standard;
2. is effectively implemented and maintained.
3. Bank must:
   a. plan, establish, implement and maintain an audit programme(s), including the frequency, methods,
   b. responsibilities, planning requirements and reporting. The audit programme(s) must take into
   c. consideration the importance of the processes concerned and the results of previous audits;
   d. define the audit criteria and scope for each audit;
   e. select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
   f. ensure that the results of the audits are reported to relevant management; and
   g. retain documented information as evidence of the audit programme(s) and the audit results.

   Ref: Internal and External Audit Policy

## 7.23. Removable Media Security

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Bank and to reduce the risk of acquiring malware infections on computers operated by Bank.

The Bank will ensure the controlled use of removable media devices to store and transfer information by all Employees who have access to information, information systems and IT equipment for the purposes of conducting official bank business. It is Bank Policy to prohibit the use of all removable media devices unless a valid business case for its use is provided.

Ref: Removable Media Policy

## 7.24. Electronic Mail Security

The purpose of the policy is to minimize the risk associated with Internet and email services and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

This policy applies to all email communications carried out through the Bank's IT systems. It is also applicable to all email communications carried out for conducting Bank IT Solutions business.

Ref: Electronic Mail Policy

## 7.25. Information Transfer

Due to the nature of its business, Bank transfers a lot of information across its internal and external network (with their customers). This policy aims to inform staff on best practices when securely transferring information. This should result in a reduced risk of unauthorized disclosure of such information that could lead to a breach of confidentiality. The policy requires staff to consider the various methods available to transfer information and to ensure that security provisions are applied to every selection.

The policy also identifies the risks when transferring personal information and requires staff to consider these in line with legislation.

Ref: Information Transfer Policy

## 7.26. Encryption Security

The purpose of this policy is to define how encryption is to be used throughout Bank's in order to reduce the likelihood of information leakage or unauthorized access to Bank's information. Encryption provides strong additional protection for particularly sensitive data (including personal data as defined under the Data Protection Act) or where data is held on less secure devices (e.g. laptops, smart devices, Removable storage devices) or transmitted over untrusted networks (including the internet).

Ref: Encryption Security Policy

## 7.27. Segregation of duties Policy

The purpose of this policy is to safeguard organization systems and information through appropriate segregation (separation) of technological duties, roles and environments.
Segregation of duties is an internal control to reduce the risk of accidental or deliberate system misuse, to identify problems, and to ensure that no single person can completely compromise information systems resources. It ensures that a concentration of responsibilities does not occur in one person or activity that will allow accidental or deliberate errors to go undetected.

Ref: Segregation of duties Policy

## 7.28. Privacy

Objective The purpose of this policy is to maintain the privacy of and protect the personal information of employees, contractors, vendors, interns, associates, customers and business partners of Bank and ensure compliance with laws and regulations applicable (refer to Annexure A 'Data Privacy Annexures' document) to Bank.
Ref: Privacy Policy

## 7.29. Customer Protection

The Bank may collect different information about you in different situations. Bank only collects Confidential Information about you through lawful means and to administer your account and conduct the business of providing you with quality products and services. Except as expressly provided for in this Policy, we do not share personal information with other persons or organizations for their marketing purposes, nor will we intentionally disclose your personal information to third parties unless.

Ref: Customer Protection Policy

## 7.30. Capacity management

The purpose of this process is to establish a Capacity Management process for the Bank. adoption and implementation of this process provide a structured method to ensure that the required capacity exists within the IT environment so that IT Services meet business requirements as documented in Service Level Agreements, and that this is provided in a cost-effective and timely manner. The Capacity process can be triggered by many other processes. In the normal course of business, each service has a pre-determined capacity review cycle (usually annually, to coincide with the budget cycle), and the process executes according to that cycle.

Ref: Capacity management policy

## 7.31. Personnel Security

The purpose of this policy is to reduce the risks of human actions that involve the fraudulent, malicious, irresponsible or erroneous misuse of technological systems.
These policies apply to all permanent and relevant contract and 3rd party staff. They must however be considered in the context of, and subject to, current HR policy and employment terms and conditions.

Ref: Personnel Security Policy

## 7.32. ATM Security

The purpose of this document is to define a security policy for Bank . This comprehensive policy is intended to cover all aspects of information security relating to Bank ATM machines including: installation, maintenance, and operation ATM machines and network, employee responsibilities, ramifications for customers, and the security of ATM transactions.

Ref: ATM Security Policy

## 7.33. Mobile Banking Policy

The purpose of this Mobile Banking Policy Template is to address the ability of a bank, credit union, fintech company, or other type of financial institution to offer its customers mobile financial services (MFS) through mobile devices via its mobile banking delivery channel.

Ref: Mobile Banking Policy

### 7.34. RTGS AND NEFT POLICY

"RTGS/NEFT Fund Transfer Application" means an unconditional instruction issued by the Customer in writing to Bank , in form, manner and substance as Bank may prescribe or require, to effect a funds transfer for a certain sum of money expressed in Indian rupees, to the designated account of a designated beneficiary in India with a scheduled bank, that shall be effected by debiting the Account of the Customer.

Ref:RTGS NEFT Policy

## 8. MANAGEMENT REVIEW

Top management must review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review must include consideration of:

1. the status of actions from previous management reviews;
2. changes in external and internal issues that are relevant to the information security management system;
3. feedback on the information security performance, including trends in:
    a. nonconformities and corrective actions;
    b. monitoring and measurement results;
    c. audit results; and
    d. fulfilment of information security objectives;
4. feedback from interested parties;
5. results of risk assessment and status of risk treatment plan; and
6. opportunities for continual improvement.

The outputs of the management review must include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization must retain documented information as evidence of the results of management reviews.

# 9. Roles & Responsibilities

## 9.1. Bank Executive Management (Top Management)

The Top Management has the following responsibilities:

- Endorse the Bank's ISMS.
- Support the enforcement of approved Policies through IT, Human Resources, Finance, IT and Business Operations, Internal Audit, and Legal departments.
- Provide appropriate and adequate infrastructure, processes and resources in order to facilitate implementation of the Bank's Information Security Policies, Standards, Procedures and Guidelines.

## 9.2. Information Security

- Information Security team must facilitate the formulation/updating of all relevant documents in line with this policy.
- Information Security must create awareness amongst users regarding compliance with this policy.
- Information Security must regularly assess different components of the IT Infrastructure and Applications to measure the effectiveness of a stated control or group of controls and to ensure that the component is compliant with published policies and standards.
- Information Security must maintain an adequate and up to date repository of all exceptions approved.
- Information Security must manage Information Security Incidents as per the incident management process.
- Information Security must facilitate the identification, assessment and mitigation of Informaiton Security risks.

## 9.3. Information Security Steering Committee

Information Security Steering Committee (ISSC) is a cross-functional group and constitutes representatives from HR, Information Security, Finance and Internal IT departments. ISSC will be chaired by the a representative appointed by the Top Management has the following responsibility.

1. Formulate, review and keep the ISMS updated.
2. Communicate all policies and procedures to Users.

3. Prioritize focus areas and drive an initiative to implement and measure compliance of the ISMS wherever verifiable, using various testing methodologies/tools and provide recommendations for ensuring compliance.
4. Report policy compliance on an annual basis to relevant stakeholders.

### 9.4. Users

- Users are responsible for maintaining the security of Information Assets they have access to.
- Users must complete the Information Security course available under the intranet portal. Users are required to repeat the course at least once a year.
- Users handling payment card (credit, debit, prepaid, stored value, gift or chip) transactions (of any sort) on behalf of the Bank must successfully complete the course before they start these card activities. Such Users are required to repeat the course at least once a year.

## 10. Compliance

All Users and Third Parties are required to comply with this Policy. The violation must be notified to the Head of Information Security.

## 11. Exceptions to the Policy

Exceptions to this Policy must be documented and formally approved by the IT Manager. Policy exceptions must contain the following:

- Description of the exception.
- A reasonable explanation for why the policy exception is required.
- Any risks created by the policy exception.
- Compensatory controls (if any) to address the risks.
- Evidence of approval by the IT Manager.

## 12. Inquiries

Inquiries regarding this policy should be directed to the Head of Information Security.

## 13. Amendments

- The Policy would be amended as and when required.

- The policy must be reviewed and updated at least once a year to ensure its applicability in addressing the current requirements of the Bank.

*** End of Document ***