THE MAHAVEER CO-OP. BANK LTD., BELAGAVI

I.S. MANAGEMENT POLICY

POLICIES FOR THE FY
2026-27
https://mahaveerbank.bank.in

The Mahaveer Co-op. Bank Ltd.,
1157, Shree Renuka Towers,
Anantshayan Galli,
Belagavi-590002
Phone : 0831-2407120/2407121/4212236

Information Security Management Policy 2026-27

Approved by the Board of Directors at its meeting held on 23/6/2026, vide Resolution No. 11.

Information Security Management Policy

Purpose:
To establish a comprehensive Information Security Management framework for safeguarding the confidentiality, integrity, and availability of the Bank's information assets, ensuring protection against unauthorized access, disclosure, alteration, and destruction, and to ensure compliance with applicable regulatory and statutory requirements.

Scope:
This policy applies to all information assets, IT systems, applications, employees, directors, contractual staff, and third-party service providers across all branches and offices of the Bank.

Policy:

- The Bank shall adopt a risk-based Information Security Management approach to identify, assess, and mitigate information security risks.
- The framework shall be aligned with RBI Cyber Security guidelines and other applicable regulatory requirements.
- Periodic information security risk assessments, vulnerability assessments, and security reviews shall be conducted to ensure effectiveness of controls.

1. Data Backup

Purpose:
To ensure that the Bank's data is securely backed up and can be reliably restored in the event of system failure, data loss, or disaster, thereby maintaining data availability, accuracy, and continuity of operations. It also aims to minimize downtime, prevent loss of critical information, and support smooth functioning of banking services during unexpected disruptions.

Scope:
This policy applies to all critical data, databases, applications, and IT systems of the Bank, including data stored at branches, data centers, and disaster recovery (DR) sites.

Policy:

- The Bank shall implement a structured backup mechanism, including daily incremental backups and periodic full backups of all critical systems and data.

THE MAHAVEER CO-OP. BANK LTD. BELAGAVI

- Backup data shall be securely stored at an offsite location and/or Disaster Recovery (DR) site to ensure redundancy and business continuity.
- All backup data shall be encrypted and protected against unauthorized access, alteration, or loss.
- Periodic testing of backup restoration shall be conducted to ensure data integrity and recovery readiness.
- Backup retention periods shall be defined in line with regulatory, legal, and business requirements.

Email Security

Purpose:
To ensure the secure and appropriate use of the Bank's email systems and to protect against threats such as phishing, malware, spam, data leakage, and unauthorized access, thereby safeguarding sensitive information and maintaining the integrity of communication.

Scope:
This policy applies to all employees, directors, contractual staff, and authorized users who access or use the Bank's official email systems, whether from office premises or remote locations.

Policy:

- The Bank shall deploy secure email infrastructure with controls such as spam filtering, anti-virus, anti-phishing, and malware protection mechanisms.
- Official email accounts shall be used strictly for authorized business communication. Use of personal email IDs for official purposes is strictly prohibited.
- Transmission of confidential or sensitive information through email shall be protected using encryption or other approved security controls.
- Users shall exercise caution while opening emails, attachments, or links, especially from unknown or unverified sources.
- Auto-forwarding of official emails to external email accounts shall be disabled or allowed only with proper authorization.
- Email attachments shall be scanned automatically, and high-risk file types may be blocked.
- The Bank reserves the right to monitor, log, and review email usage for security, audit, and compliance purposes.
- Phishing attempts, suspicious emails, or security incidents must be reported immediately to the IT Department.
- Email retention and archival shall be maintained in accordance with regulatory and legal requirements.

Network Security

Purpose:
To ensure the security, reliability, and integrity of the Bank's network infrastructure by protecting it from unauthorized access, cyber threats, and disruptions, thereby ensuring safe and continuous banking operations.

Scope:
This policy applies to all network infrastructure, including routers, switches, firewalls, communication links, wireless networks, and all systems connected to the Bank's internal and external networks across branches and offices.

Policy:

- The Bank shall implement layered network security controls, including firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and secure gateways.
- Network segmentation shall be enforced to separate critical systems, internal networks, and external/public-facing systems.
- Secure communication protocols shall be used for data transmission, and unsecured services shall be disabled.
- Remote access to the Bank's network shall be permitted only through secure VPN with strong authentication mechanisms.
- Wireless networks, if used, shall be secured with strong encryption and access controls.
- Regular Vulnerability Assessment and Penetration Testing (VAPT) shall be conducted to identify and mitigate network vulnerabilities.
- Network devices shall be securely configured, and default passwords/settings shall be changed.
- Continuous monitoring of network traffic and logs shall be carried out to detect suspicious activities.
- Unauthorized devices shall not be allowed to connect to the Bank's network.

Antivirus Policy

Purpose

- To protect the Bank's IT systems from **viruses, malware, ransomware, and cyber threats**
- To ensure **secure and uninterrupted banking operations**
- To comply with RBI cyber security guidelines

Scope

- Applicable to:
  - All desktops, servers, laptops
  - All endpoint devices connected to Bank network
  - All devices and users accessing the bank's systems and resources

Policy

- All systems shall have **licensed antivirus software installed**.
- Antivirus software shall be **updated regularly with latest virus definitions.**
- **Real-time protection** shall be enabled on all systems.
- Full system scans shall be performed **periodically**.
- Unauthorized software installation shall be **restricted.**
- USB and removable media shall be **scanned before use**.
- Systems shall be protected against **malware, ransomware, and spyware threats.**
- Antivirus alerts and logs shall be **monitored regularly**.
- Infected systems shall be **immediately isolated and cleaned**.
- Only authorized IT personnel shall manage antivirus settings.
- Antivirus software shall not be disabled by users.
- All endpoint devices shall comply with **security configuration standards**.
- Policy compliance shall be **reviewed periodically**.

Patch Management Policy

Purpose

To ensure that all systems and software in the Bank are regularly updated with the latest security patches to protect against vulnerabilities, cyber threats, and system failures.

Scope

This policy applies to:

- All desktops, laptops, and servers
- All software, applications, and operating systems
- All branches and Head Office

Policy

- All systems must be **regularly updated with latest security patches and updates**.
- Patch management shall be handled **only by the IT Head or authorized IT personnel**.
- **Automatic updates should be enabled** wherever possible.
- Critical security patches must be **applied on priority without delay**.
- Patches should be **tested (if required)** before applying to critical systems like servers/CBS.
- All updates and patches must be **properly recorded and documented**.
- Systems that are not updated regularly shall be **identified and corrected immediately**.
- Unsupported or outdated software/systems should be **upgraded or removed**.
- Endpoint management/patch management tools (if available) should be used for **centralized control**.
- Patch status should be **monitored regularly** to ensure compliance.
- Any patch-related issues or failures must be **reported to IT immediately**.

Software Installation Policy

Purpose:

The purpose of this policy is to ensure that only authorized, licensed, and secure software is installed on the Bank's systems. This helps in protecting the Bank's IT infrastructure from security threats, malware, data breaches, and ensures compliance with regulatory (RBI) guidelines.

Scope

This policy is applicable to:

- All employees, staff, and users of the Bank
- All IT assets including desktops, laptops, servers, and other devices connected to the Bank's network
- All software, applications, tools, and utilities installed or used within the Bank

Policy

- All software installations must be based on business requirements.
- Only the IT Head or authorized personnel shall have the rights to install or authorize the installation of any software.

- Administrative privileges (admin password) shall be strictly restricted. Only authorized personnel having access to admin credentials are permitted to install or approve installation of software.
- End-users are strictly prohibited from installing, downloading, or using any unauthorized software or applications.
- Only genuine, licensed, and approved software shall be installed and used in the Bank.
- All installed software must be recorded and maintained in the Software Inventory Register.
- Unauthorized or unlicensed software, if detected, shall be removed immediately and reported to management.
- Periodic checks, monitoring, and audits shall be conducted by the IT Department to ensure compliance with this policy.
- Any violation of this policy shall be treated as a security breach and may attract disciplinary action.

Environmental Monitoring & Data Centre Monitoring Policy

Purpose

The purpose of this policy is to establish a framework for monitoring and maintaining appropriate environmental conditions within the Bank's Data Centre and Server Rooms to ensure the **continuous, secure, and reliable operation of IT systems and Core Banking infrastructure**.

This policy aims to:

- Prevent system failures due to adverse environmental conditions
- Protect IT assets from damage caused by temperature, humidity, fire, power issues, or water leakage
- Ensure business continuity and minimize operational disruptions
- Comply with RBI guidelines on cyber security and IT infrastructure management

Scope

This policy applies to:

- All Data Centres, Server Rooms, and Network Rooms of the Bank
- All IT equipment including servers, storage devices, network devices, and power systems
- All employees, IT staff, and third-party vendors responsible for managing or accessing the Bank's IT infrastructure

Policy

3.1 Environmental Controls

- The Bank shall maintain appropriate environmental conditions in all Data Centre/Server Rooms:
  - Temperature: **18°C to 24°C**
  - Humidity: **40% to 60%**
- Adequate air-conditioning systems shall be installed and operated on a **24x7 basis**

3.2 Power Management

- All critical IT systems shall be supported by **Uninterruptible Power Supply (UPS)** systems
- Backup power through generators/inverters shall be ensured
- Voltage fluctuations and power irregularities shall be monitored and controlled

3.3 Fire Detection and Suppression

- Data Centre/Server Rooms shall be equipped with:
  - Smoke detectors and fire alarms
  - Fire extinguishers (preferably CO_2 type)
- Fire safety equipment shall be periodically tested and maintained

3.4 Water Leakage Protection

- IT infrastructure shall be positioned to avoid exposure to water leakage
- Preventive measures shall be taken to avoid seepage, flooding, or accidental water exposure

3.5 Monitoring Mechanism

- Environmental parameters such as temperature, humidity, and power shall be **continuously monitored** through manual checks or automated systems
- Alerts (SMS/email) shall be configured for abnormal conditions, wherever feasible

3.6 Physical Security

- Access to Data Centre/Server Rooms shall be **restricted to authorized personnel only**
- CCTV surveillance shall be implemented wherever feasible

3.7 Housekeeping and Maintenance

- Server rooms shall be maintained in a **clean and dust-free condition**
- No food, liquids, or unauthorized materials shall be allowed inside
- Periodic maintenance of AC, UPS, and other infrastructure shall be carried out

3.8 Incident Management

- Any deviation from prescribed environmental conditions shall be treated as an incident
- Immediate corrective action shall be taken to prevent system damage
- Major incidents shall be reported to management as per incident reporting procedures

3.9 Compliance and Audit

- The policy shall be reviewed periodically and updated as required
- Compliance shall be verified through internal/external audits

Wireless Security Policy

Purpose

The purpose of this policy is to ensure the **secure deployment, configuration, and usage of wireless networks (Wi-Fi)** within the Bank to prevent unauthorized access, data breaches, and cyber threats.

This policy aims to:

- Protect sensitive banking data transmitted over wireless networks
- Prevent unauthorized access to internal systems
- Ensure compliance with RBI cyber security guidelines

Scope

This policy applies to:

- All wireless networks (Wi-Fi) deployed within the Bank
- All access points, wireless controllers, and related devices
- All employees, vendors, and users accessing Bank Wi-Fi

Policy

- All wireless networks shall use **WPA2/WPA3 encryption** with strong passwords.
- Default SSID names and credentials shall be changed.
- Separate Wi-Fi networks shall be maintained for internal and guest users.
- Guest networks shall be isolated from core banking systems.
- Access shall be restricted to authorized users/devices only.
- Wireless access logs shall be maintained and monitored.
- Only approved access points shall be used; rogue devices shall be removed.
- Firmware updates and security patches shall be applied regularly.
- Sharing of Wi-Fi credentials and use of unauthorized hotspots is prohibited.
- Policy compliance shall be reviewed periodically.

Network Security Policy

Purpose

The purpose of this policy is to establish a framework for **protecting the Bank's network infrastructure** from cyber threats, unauthorized access, and data breaches.

This ensures:

- Confidentiality, integrity, and availability of information
- Secure operation of banking systems
- Compliance with RBI and regulatory requirements

Scope

This policy applies to:

- All network infrastructure (LAN, WAN, Internet, VPN)
- All network devices such as routers, switches, firewalls, IDS/IPS
- All employees, vendors, and third parties accessing the Bank's network

Policy

- Network access shall be restricted to authorized users with role-based controls.
- Firewalls shall be implemented to allow only necessary traffic.

- Critical systems shall be segregated using VLANs or equivalent controls.
- Default configurations shall be changed and unused services disabled.
- Network activities shall be continuously monitored and logged.
- All network devices shall be regularly updated with security patches.
- IDS/IPS shall be implemented to detect and prevent intrusions.
- Remote access shall be allowed only through secure VPN with MFA.
- Security incidents shall be reported and handled promptly.
- Third-party access shall be controlled, approved, and monitored.
- Regular audits and policy reviews shall be conducted.

Network Device Configuration Policy

Purpose

To ensure that all network devices (routers, switches, etc.) are configured securely to protect the Bank's network from unauthorized access, cyber threats, and misuse.

Scope

This policy applies to:

- All network devices used in the Bank (routers, switches, firewalls, Wi-Fi devices)
- All branches and Head Office
- All personnel responsible for managing network devices

Policy

- All network devices must be **configured only by the IT Head or authorized IT personnel**.
- Default usernames and passwords must be **changed immediately** and strong passwords must be used.
- Administrative access to network devices must be **restricted and controlled**.
- Only **required services and ports** should be enabled; unused ports must be disabled.
- Network should be **segregated** (e.g., separate network/VLAN for banking systems and internet PCs).
- Firewall must be properly configured to **allow only authorized traffic and block unauthorized access**.
- Remote access to network devices, if required, must be **secure and approved**.
- Configuration changes must be **approved and properly documented**.

- Regular **backup of device configuration** must be taken and stored securely.
- Logs should be **enabled and monitored regularly** for any suspicious activity.
- Firmware/updates of network devices must be **kept up to date**.
- Physical access to network devices must be **restricted to authorized personnel only**.

Customer Awareness Policy / Communication Plan

Purpose

The purpose of this policy is to ensure that customers of **The Mahaveer Co-operative Bank Ltd., Belagavi** are adequately informed and educated about safe banking practices, digital banking risks, cyber security threats, fraud prevention, and their rights and responsibilities. This policy aims to promote **secure banking behavior**, reduce fraud incidents, and enhance customer confidence in banking services in line with **RBI guidelines**.

Scope

This policy applies to:

- All customers of the bank (depositors, borrowers, digital banking users)
- All delivery channels including **branch banking, ATM services, internet/mobile banking**
- All communication modes such as **SMS, email, website, notices, social media, and campaigns**
- All bank staff responsible for customer interaction and awareness activities

Policy

- The Bank shall maintain a Customer Awareness & Cyber Security section on its website.
- The Bank shall conduct regular customer awareness programs on safe banking and cyber security.
- Awareness shall be shared through SMS, email, website, and branch notices.
- Communication shall be simple and in English and local languages.
- The Bank shall issue timely alerts on frauds and cyber threats.
- Customers shall be advised not to share OTP, PIN, or passwords.
- Customers shall be advised to report suspicious transactions immediately.
- Branch staff shall educate customers during regular interactions.
- The Bank shall maintain records of awareness programs and communications.
- The policy shall be reviewed annually or as per RBI guidelines.

Remote Access & RDP Control Policy

Purpose

To ensure that remote access to the bank's systems is secure and to prevent unauthorized use of Remote Desktop Protocol (RDP).

Scope

This policy applies to:

- All employees of the bank
- IT administrators
- Vendors and third-party service providers
- All systems, servers, and devices connected to the bank network

Policy

- Remote access and RDP shall be **disabled by default** on all systems.
- It shall be enabled **only with prior approval** from the IT Department / Information Security Officer.
- Access must be **need-based and time-bound**.
- Remote access shall be allowed **only through secure VPN**.
- **Direct RDP access over the internet is strictly prohibited**.
- Strong passwords and **Multi-Factor Authentication (MFA)** must be used.
- Access shall be given only to **authorized users** (least privilege).
- All remote access activities shall be **logged and monitored**.
- Vendor access shall be **temporary and supervised**.
- Any suspicious activity must be **reported immediately**.

Vendor SLA Review Policy / SOP

Purpose

To ensure that vendor SLAs are regularly reviewed and monitored for **service quality, performance, and compliance** with RBI outsourcing guidelines.

Scope

Applicable to all **vendors/service providers** engaged by the Bank for outsourced services.

SOP / Policy Guidelines (Point-wise)

- The Bank shall execute **formal SLAs** with all vendors defining roles, responsibilities, and service levels.
- SLAs shall include key parameters such as:
  - Service uptime and availability
  - Turnaround Time (TAT)
  - Penalty clauses
  - Data security and confidentiality
  - Grievance redressal
- The Bank shall review vendor SLAs at the following frequency:
  - **Critical Vendors (CBS, IT, Network, ATM, etc.): Quarterly review**
  - **Other Vendors: Half-yearly review**
- Vendor performance shall be **monitored continuously** against SLA parameters.
- Any **service failure or SLA deviation** shall be recorded and corrective action shall be taken.
- The Bank shall maintain a **Vendor Performance Review Register** for audit purposes.
- Non-performance or repeated issues shall be **escalated to higher management**.
- The Bank may **impose penalties or take action** as per SLA terms in case of non-compliance.
- Vendors shall comply with **RBI guidelines, data security, and regulatory requirements**.
- Vendors shall provide support during **audit, inspection, and regulatory review**.
- All SLA reviews shall be **documented and approved by the competent authority**.

Reconciliation Policy / SOP

Purpose

To ensure timely and accurate reconciliation of all transactions and accounts to detect discrepancies, prevent fraud, and maintain financial integrity as per RBI guidelines.

Scope

Applicable to all **bank transactions and accounts**, including CBS, ATM, NEFT/RTGS/IMPS, clearing, suspense accounts, and vendor-related transactions.

SOP / Policy Guidelines (Point-wise)

- The Bank shall carry out **reconciliation of all transactions and accounts on a daily basis (Mandatory)**.
- All entries in **CBS, ATM transactions, interbank transactions, and suspense accounts** shall be reconciled **at the end of each working day**.
- **Unreconciled entries**, if any, shall be tracked in a separate register and regularly followed up.
- The Bank shall maintain **reconciliation reports and supporting documents** for audit and inspection.
- The Bank undertakes **daily reconciliation of all transactions on a mandatory basis**.
- For **UPI/IMPS and RTGS/NEFT transactions (through HDFC Bank)**, reconciliation is carried out on a **day-to-day basis**.
- For **ATM and CTS transactions (through IDBI Bank)**, reconciliation is also performed **daily**.
- The Bank conducts **monthly reconciliation with all partner banks**, and the same is **verified and signed by one of the Directors**.
- **CBS reconciliation** is carried out by the **respective Branch Heads** on a regular basis.
- The **overall reconciliation and monitoring** is performed by the **Head Office Branch Manager (HO BM)**.
- All reconciliation records are **properly maintained and preserved** for audit and regulatory compliance.

Browser Security Configuration Policy

Purpose

The purpose of this policy is to ensure secure usage of web browsers within the Bank by minimizing risks related to malware, phishing attacks, data leakage, and unauthorized access while accessing internet-based applications.

Scope

This policy applies to:

- All employees and users of the Bank
- All devices (desktops, laptops, etc.) used to access the internet
- All web browsers installed on Bank systems

Policy

- Only **approved browsers** should be used in the Bank.
- Browser settings will be **controlled by the IT Department**.

- Browsers must be **regularly updated** to the latest version.
- Staff should **not install any extensions/add-ons** without IT approval.
- **Unsafe websites and pop-ups will be blocked**.
- Staff should **not visit unknown or suspicious websites**.
- Downloading files from unknown websites is **not allowed**.
- **Saving passwords in the browser is not allowed**.
- Security features like **phishing protection must be ON**.
- Internet usage may be **restricted by firewall or security system**.
- Any suspicious activity should be **reported to IT immediately**.

Internet Usage Policy

Purpose

To ensure safe and secure use of the internet in the Bank and to protect systems and data from cyber threats.

Scope

This policy applies to:

- All Bank employees
- All systems and devices with internet access

Policy

- Internet access shall be provided **only for official work purposes**.
- Access to **social media, entertainment, and non-business websites** should be restricted.
- Users must **not visit suspicious or unknown websites**.
- Downloading files, software, or data from untrusted sources is **strictly prohibited**.
- Important banking systems (like CBS, RTGS/NEFT, etc.) should **not be used for general internet browsing**.
- **A separate standalone computer (Internet PC)** shall be used for internet browsing, email, and downloading files.
- This standalone system should **not be connected to critical banking systems or internal network**.
- Data transfer from the internet PC to Bank systems must be done **only after proper virus scanning and IT approval**.

- All internet activity may be **monitored and controlled by the IT Department**.
- Security controls like **firewall, antivirus, and web filtering** must be enabled.
- Any suspicious activity or cyber incident must be **reported to IT immediately**.

Desktop & Laptop Management

Purpose:
To ensure secure configuration, controlled usage, and effective management of desktops and laptops, thereby safeguarding the Bank's information assets from unauthorized access, data leakage, malware, and operational risks.

Scope:
This policy applies to all desktops, laptops, and endpoint devices owned, leased, or used for official purposes by employees, contractual staff, and authorized users across all branches and offices of the Bank.

Policy:

- All desktops and laptops shall be configured as per approved security standards prior to deployment.
- Endpoint protection solutions (antivirus/EDR) shall be installed, regularly updated, and monitored.
- Installation of unauthorized or unlicensed software is strictly prohibited.
- Systems shall be secured with strong passwords and auto screen-lock after a defined period of inactivity.
- Data stored on laptops and portable devices shall be encrypted, especially when used outside Bank premises.
- Regular updates, patches, and security configurations shall be applied to all systems.
- Use of USB ports and external storage devices shall be restricted and controlled.
- Users shall not store sensitive data locally unless explicitly authorized.
- Loss or theft of any device must be reported immediately to the IT Department.

Clean Desk Policy:

- Employees shall ensure that no sensitive or confidential information (documents, printouts, and storage media) is left unattended on desks.
- All important documents shall be securely stored in locked drawers/cabinets when not in use.

- Computer screens shall be locked when unattended.
- At the end of the working day, desks shall be cleared of all sensitive information to prevent unauthorized access.

Operating System (OS)

Purpose:

The purpose of this policy is to ensure that all operating systems used by the Bank are securely configured and regularly updated. It aims to protect systems and data from unauthorized access, malware, and other security threats. The policy also ensures stability and proper functioning of IT systems across the Bank, reduces risks arising from vulnerabilities and outdated software, and supports safe and reliable banking operations through secure system management.

Scope:

This policy applies to all operating systems installed on servers, desktops, laptops, and other IT systems used across the Bank. It covers systems used at branches, offices, and data centers, including those accessed remotely or used outside the Bank premises. The policy is applicable to all employees, IT staff, and authorized users, and includes all devices connected to the Bank's network.

Policy:

- All operating systems shall be installed and configured as per approved security standards before use.
- Default accounts, passwords, and unnecessary services shall be disabled or removed.
- Regular security updates and patches shall be applied in a timely manner.
- Access to system settings and administrative privileges shall be restricted to authorized IT personnel only.
- Anti-virus and other security tools shall be installed, updated, and active at all times.
- Systems shall be monitored regularly, and logs shall be maintained to detect any unusual or unauthorized activity.
- Only licensed and approved operating systems shall be used within the Bank.
- Users shall not make any unauthorized changes to system configurations.

Database Security

Purpose:

The purpose of this policy is to ensure that all databases of the Bank are securely managed and

protected from unauthorized access, data leakage, and cyber threats. It aims to safeguard sensitive customer and financial data, maintain data accuracy and integrity, and ensure that database systems function reliably. The policy also helps in reducing risks related to data breaches and supports compliance with regulatory requirements.

Scope:
This policy applies to all databases used by the Bank, including those supporting core banking, applications, and other IT systems. It covers databases located at data centers, branches, and disaster recovery sites. The policy is applicable to all employees, database administrators, IT staff, and authorized users who access or manage database systems.

Policy:

- Access to databases shall be restricted to authorized users based on roles and responsibilities.
- Strong authentication and password controls shall be implemented.
- Sensitive data shall be encrypted at rest and during transmission.
- Regular database backups shall be taken and tested.
- Database activities and logs shall be monitored for any suspicious or unauthorized actions.
- Security patches and updates shall be applied regularly.
- Default settings and unnecessary services shall be disabled.

IT Asset Management

Purpose:
The purpose of this policy is to ensure proper identification, tracking, and management of all IT assets of the Bank throughout their lifecycle. It aims to safeguard assets from loss, theft, misuse, or unauthorized access, ensure accountability, and support efficient utilization of IT resources. The policy also helps in maintaining accurate records and ensuring compliance with audit and regulatory requirements.

Scope:
This policy applies to all IT assets of the Bank, including hardware (such as desktops, laptops, servers, network devices), software, and other technology resources used across branches, offices, and data centers. It covers assets owned, leased, or used for official purposes and is applicable to all employees, IT staff, and authorized users handling such assets.

Policy:

- All IT assets shall be recorded in a centralized asset register with unique identification.
- Assets shall be properly tagged, tracked, and periodically verified.

- Allocation and movement of assets shall be documented and approved.
- Only authorized and licensed software shall be installed on systems.
- Regular maintenance and updates of assets shall be carried out.
- End-of-life assets shall be disposed of securely as per defined procedures.
- Any loss, damage, or misuse of assets shall be reported immediately.

Data Retention & Disposal

Purpose:
The purpose of this policy is to ensure that the Bank's data is retained for an appropriate period as per business, legal, and regulatory requirements, and disposed of securely when no longer required. It aims to protect sensitive information from unauthorized access, prevent data leakage, and ensure efficient storage management while maintaining compliance with applicable laws and RBI guidelines.

Scope:
This policy applies to all data and records of the Bank, including physical and electronic data, maintained across branches, offices, data centers, and disaster recovery sites. It covers all employees, IT staff, and authorized users responsible for handling, storing, and disposing of such data.

Policy:

- Data shall be retained only for the period specified under regulatory, legal, and business requirements.
- A defined data retention schedule shall be maintained and followed.
- Sensitive and confidential data shall be stored securely during the retention period.
- Data that is no longer required shall be disposed of in a secure manner to prevent unauthorized access or recovery.
- Electronic data shall be permanently deleted using secure methods, and physical records shall be shredded or destroyed.
- Proper records of data disposal shall be maintained for audit purposes.
- Backup data shall also follow defined retention and disposal guidelines.

Removable Media / USB Control Policy

Purpose

- To protect bank systems and data from unauthorized access and data leakage
- To prevent malware infections through USB/removable devices

- To ensure secure and controlled use of removable media in bank environment

Scope

- Applies to all bank employees, IT staff, and vendors
- Covers all systems, laptops, desktops, servers, and network devices
- Includes all removable media such as USB drives, external hard disks, CDs, memory cards

Policy

- USB and removable media access shall be **blocked by default on all systems**
- Access shall be allowed only with **prior approval from IT Department / Information Security Officer**
- Usage must be **need-based, time-bound, and properly documented**
- Only **approved and registered devices** shall be permitted
- All devices must be **scanned for malware before use**
- Data transfer shall follow **least privilege principle (only required data)**
- All USB usage must be **logged and monitored through security tools**
- Personal or unapproved USB devices are **strictly prohibited**
- Sensitive or customer data must not be copied without authorization
- Secure deletion of data must be done using **IT-approved tools (not simple delete/format)**
- Physical destruction shall be done for unusable or retired devices
- Vendor access shall be **temporary and supervised only**
- Any violation must be **reported immediately to IT / Information Security Officer**

Vendor / Outsourcing Management

Purpose:

The purpose of this policy is to ensure that all vendors and outsourced service providers engaged by the Bank are managed securely and do not pose risks to the Bank's information systems and data. It aims to protect the Bank from operational, security, and compliance risks arising from third-party arrangements and to ensure adherence to regulatory requirements, including RBI guidelines.

Scope:

This policy applies to all third-party vendors, service providers, and outsourcing arrangements involving

IT systems, data processing, and other critical services of the Bank. It covers all departments and employees involved in vendor selection, engagement, and management across branches and offices.

Policy:

- Vendors shall be selected based on proper due diligence, including security and risk assessment.
- All vendor engagements shall be governed by formal agreements with defined roles, responsibilities, and security requirements.
- Appropriate confidentiality and data protection clauses shall be included in all contracts.
- Access to the Bank's systems and data shall be provided to vendors only on a need-to-know and authorized basis.
- Vendor activities shall be monitored and reviewed periodically for performance and security compliance.
- Critical vendors shall be subject to periodic audits and risk assessments.
- Any data shared with vendors shall be protected and used only for authorized purposes.
- Vendor access shall be revoked immediately upon completion or termination of the contract.

Business Continuity & Disaster Recovery (BCP & DR)

Purpose:
The purpose of this policy is to ensure the Bank can maintain critical operations and recover promptly in the event of a disruption, disaster, or cyber incident. It aims to minimize downtime, protect data and systems, and ensure uninterrupted banking services for customers, while complying with regulatory and RBI guidelines.

Scope:
This policy applies to all critical banking operations, IT systems, applications, data, and infrastructure across branches, offices, data centers, and disaster recovery sites. It covers all employees, IT staff, and vendors involved in business continuity and disaster recovery processes.

Policy:

- The Bank shall maintain a documented Business Continuity Plan (BCP) and Disaster Recovery (DR) plan covering all critical operations.
- A designated DR site shall be maintained with infrastructure, applications, and data replicated as per defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

- Periodic testing and simulation of BCP and DR plans shall be conducted to ensure readiness and effectiveness.
- Employees shall be trained on BCP & DR procedures and emergency response protocols.
- Critical processes, IT systems, and applications shall be prioritized for recovery in case of disruption.
- Vendors supporting critical operations shall be included in BCP & DR planning and testing.
- Incident reporting and escalation procedures shall be clearly defined and followed.

Password Policy

Purpose:
The purpose of this policy is to ensure the creation, use, and management of strong passwords to protect the Bank's systems, applications, and sensitive data from unauthorized access. It aims to maintain confidentiality, integrity, and security of information assets while reducing the risk of security breaches.

Scope:
This policy applies to all employees, contractors, and authorized users who access the Bank's IT systems, applications, and network resources, including desktops, laptops, servers, and online banking platforms.

Policy:

- All users must create strong, unique passwords that meet defined complexity requirements (e.g., a mix of uppercase, lowercase, numbers, and special characters).
- Passwords must be changed periodically, as per the Bank's defined schedule.
- Sharing of passwords or use of another user's credentials is strictly prohibited.
- Default system passwords must be changed immediately upon installation or deployment.
- Passwords must not be written down, stored in unsecured files, or shared over email.
- Multi-factor authentication (MFA) shall be implemented wherever applicable to enhance security.
- Accounts shall be automatically locked after a defined number of failed login attempts.
- All network devices, systems, and applications must have their default usernames and passwords changed immediately at the time of installation or first use.
- Use of factory default credentials is strictly prohibited under any circumstances.

Privileged Access Management (PAM) Policy

Purpose

- To control and secure privileged (admin) access to bank systems
- To prevent unauthorized access, misuse, and security risks

Scope

- Applies to all employees with admin/privileged access
- Covers IT administrators, system users, and vendors
- Applicable to all systems, servers, applications, and network devices

Policy

- Privileged access shall be **restricted and not granted by default**
- Access shall be provided only on **need basis and with approval**
- Access shall be **time-bound and documented**
- Users must have **separate admin and normal user accounts**
- **Sharing of admin credentials is strictly prohibited**
- Strong passwords and **MFA must be used**
- All privileged activities shall be **logged and monitored**
- Access rights shall be **reviewed periodically**
- Access shall be **revoked immediately when not required**
- Vendor access shall be **temporary and supervised**
- Any suspicious activity must be **reported immediately**

Access Control Policy

Purpose:
The purpose of this policy is to ensure that access to the Bank's systems, applications, and data is granted only to authorized personnel, based on their role and responsibilities. It aims to prevent unauthorized access, protect sensitive information, and maintain the confidentiality, integrity, and availability of the Bank's information assets.

Scope:
This policy applies to all employees, contractors, vendors, and authorized users who require access to

the Bank's IT systems, applications, network resources, and data across branches, offices, data centers, and remote locations.

Policy:

- Access to all systems and applications shall be provided on a **need-to-know** and **role-based** basis.
- All users must have unique login credentials; shared accounts are prohibited.
- Privileged or administrative access shall be restricted, monitored, and approved by senior management.
- Access rights shall be reviewed periodically to ensure they remain appropriate.
- Temporary access for projects or third parties shall have defined expiry and monitoring.
- Multi-factor authentication (MFA) shall be used wherever feasible to strengthen access security.
- All access activities shall be logged and monitored for suspicious or unauthorized activity.
- Immediate revocation of access shall be done upon employee exit, role change, or contract termination.

Roles & Responsibilities – Information Security Policies

1. Board of Directors / Senior Management:

- Approve all IT and Information Security policies, including BCP/DR, Access Control, and Data Security policies.
- Provide overall governance and oversight of IT risk management, cyber security, and regulatory compliance.
- Ensure adequate resources are allocated for IT security, disaster recovery, and employee training.
- Review periodic reports on IT security incidents, audits, and policy compliance.

2. IT Committee / Risk & IT Steering Committee:

- Monitor implementation of IT and information security policies.
- Review risk assessments, IT audits, vulnerability scans, and compliance reports.
- Recommend improvements to IT processes, policies, and disaster recovery plans.

3. Chief Information Security Officer (CISO) / IT Head:

- Implement, maintain, and enforce IT and information security policies across the Bank.
- Oversee security of desktops, laptops, servers, databases, network, and applications.
- Approve privileged access, monitor user activities, and enforce access control policies.
- Ensure regular data backup, retention, and secure disposal practices are followed.
- Coordinate Business Continuity & Disaster Recovery (BCP/DR) planning, testing, and reporting.
- Ensure compliance with RBI guidelines, statutory, and regulatory requirements.
- Oversee vendor and outsourcing security compliance and monitor third-party access.
- Manage IT asset inventory, lifecycle, and secure disposal.
- Conduct periodic awareness programs and training for staff on IT and security policies.

4. IT Department / System & Network Administrators:

- Deploy, configure, and maintain desktops, laptops, servers, operating systems, databases, and network infrastructure.
- Implement network security measures, including firewalls, IDS/IPS, and secure communication protocols.
- Apply timely OS, software, and security patches on all systems.
- Monitor and manage backups, restoration tests, and secure storage of backup media.
- Control access rights and privileges as per role-based access control (RBAC) policy.
- Implement endpoint security measures such as antivirus/EDR on desktops, laptops, and servers.
- Monitor email systems for security threats and enforce secure email practices.
- Scan removable media before use and enforce restrictions on unauthorized devices.
- Maintain logs, monitor system activity, and report any suspicious events.
- Assist in testing and executing BCP/DR plans, including DR site readiness.
- Manage secure disposal of IT assets and data in accordance with retention and disposal policy.

5. Database Administrators (DBAs):

- Ensure secure configuration, access control, and regular patching of all databases.
- Implement encryption for sensitive data at rest and in transit.
- Monitor database activity logs for anomalies and unauthorized access.
- Maintain periodic database backups and validate restoration procedures.
- Coordinate with IT Head/CISO on database security and regulatory compliance.

6. All Employees / Users:

- Comply with IT, information security, and data protection policies.
- Maintain strong passwords and secure login credentials; do not share passwords.
- Use desktops, laptops, and IT systems responsibly; do not install unauthorized software.
- Follow clean desk, clean screen, and removable media policies.
- Report lost, stolen, or compromised devices immediately.
- Participate in IT awareness and security training programs.
- Ensure proper handling of sensitive data, following classification, retention, and disposal guidelines.
- Adhere to secure email practices and do not open suspicious links or attachments.

7. Vendors / Third-Party Service Providers:

- Comply with all contractual and security requirements defined by the Bank.
- Ensure access to Bank systems is controlled, monitored, and restricted to approved purposes.
- Follow data protection, confidentiality, and encryption requirements.
- Report any security incidents or breaches promptly to the Bank's IT/CISO team.

8. Compliance & Audit Teams:

- Conduct periodic audits of IT systems, processes, access controls, backups, and BCP/DR readiness.
- Verify compliance with internal policies, RBI guidelines, and regulatory requirements.
- Report gaps and recommend corrective actions to management and the Board.

The Mahaveer Co-operative Bank Ltd., Belagavi

Chief Executive Officer/Vice-Chairman/Chairman