THE MAHAVEER CO-OP. BANK LTD., BELAGAVI

CYBER SECURITY POLICY

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

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

Cyber Security Policy

Purpose

The document establishes a comprehensive framework for the protection of information assets of The Mahaveer Co-operative Bank Ltd. (TMCBL), ensuring their secure use, access, and disclosure to safeguard against cyber threats and attacks in compliance with applicable standards, laws, and RBI guidelines; it also incorporates key aspects of the Bank's Information Security Policy to provide assurance of secure banking operations and robust information system controls, and TMCBL reserves the right to modify, amend, suspend, withdraw, or terminate this policy, either in whole or in part, at any time as deemed necessary. The Cyber Security Policy serves the below purpose for the bank-

- To ensure confidentiality, integrity, and availability (CIA) of information assets.
- To protect customer data and maintain trust in digital banking channels.
- To comply with RBI Cyber Security Framework for UCBs and other regulatory requirements.
- To establish preventive, detective, and corrective controls.

Confidentiality, Integrity and Availability (CIA) of Information Assets

This clause is framed in alignment with RBI guidelines on Cyber Security Framework for Urban Co-operative Banks, IT Governance Directions, and CERT-In requirements.

Confidentiality, Integrity and Availability (CIA)

1. Confidentiality

1.1 The Bank shall keep customer and sensitive information secure and prevent unauthorized access.

1.2 Access shall be given only to authorized persons on a need-to-know basis.

1.3 Strong login controls and MFA (Multi-Factor Authentication) shall be used for important systems.

1.4 Data shall be protected through encryption and monitoring systems.

2. Integrity

2.1 The Bank shall ensure that all data is accurate and not altered without authorization.

2.2 Proper controls shall be in place to prevent data tampering.

2.3 All important activities shall be recorded through logs and audit trails.

2.4 Maker-checker system shall be followed for transactions.

3. Availability

3.1 The Bank shall ensure systems like CBS and payment services are always available.

3.2 Backup and recovery systems shall be maintained.

3.3 BCP and DR plans shall be implemented and tested regularly.

3.4 Systems shall be monitored and maintained to avoid downtime.

Scope

This Cyber Security Policy applies to all persons who access or use the Bank's information systems, including management, employees, administrators, contractors, and third parties.

It covers all IT systems of the Bank, including hardware, software, networks, applications, and data.

The policy is applicable to the Head Office, Data Centre, and all branches of the Bank.

It includes all important information assets such as:

- Bank's business and internal information
- Employee and customer data
- Vendor and third-party information
- Core Banking System (CBS) and other software
- Servers, computers, networks, and communication systems
- Digital services like UPI, IMPS, NEFT/RTGS, ATM, and Mobile Banking (Android)

This policy also applies to all vendors and service providers, including CBS vendor **M/s Wintech Software Consultants Belagavi.** and hardware vendor **M/s Oasis Computers Belagavi**, along with any other outsourced service providers.

Any new systems or services introduced by the Bank will also be covered under this policy.

If there is any conflict with laws or RBI guidelines, the Bank will follow the applicable laws and regulations.

Management Commitment

TMCBL shall establish and maintain an effective cyber security and information security framework supported by appropriate policies, procedures, and controls.

The Bank shall constitute an **IT Committee** to oversee IT governance, cyber security initiatives, and compliance with RBI guidelines. The Committee shall periodically review IT risks, security posture, and implementation status.

The Bank shall conduct an annual Cyber Risk Assessment covering operational, technological, regulatory, vendor-related, and fraud risks, and shall implement appropriate controls based on the assessment.

Management shall identify and manage various risk types, including inherent risk, residual risk, and acceptable risk, and ensure adequate mitigation measures are in place.

TMCBL shall allocate necessary resources, including budget and manpower, for effective implementation of cyber security measures.

All cyber incidents shall be reported to regulatory authorities such as RBI and CERT-In within prescribed timelines.

The Bank shall ensure:

- Compliance with applicable laws, RBI guidelines, and regulatory requirements
- Implementation of security controls based on risk assessment
- Regular training and awareness for employees
- Continuous monitoring and improvement of information security practices

The Bank shall implement appropriate controls to protect the confidentiality, integrity, availability, and privacy of information and ensure access only to authorized persons.

Understanding Cyber Attacks and Risks

A cyber-attack refers to any attempt to gain unauthorized access, disrupt operations, misuse IT systems, or cause financial loss to the Bank or its customers through digital means. Such attacks may originate from internal or external sources.

Common types of cyber threats include:

- **Application and system vulnerabilities (including CBS and other applications)**
  Weak points or errors in software that can be misused. Attackers can use them to access or change data.
- **Denial of Service (DoS) / Distributed Denial of Service (DDoS) attacks**
  Too much traffic is sent to a system to overload it. This makes banking services slow or unavailable.
- **Malware and ransom ware attacks**
  Harmful software that can damage systems or steal data. Ransom ware locks data and asks for money to unlock it.

- **Phishing, spear phishing, whaling, and vishing attacks**
  Fake messages or calls pretending to be from trusted sources. They try to steal passwords, OTPs, or bank details.
- **Web-based attacks (like cross-site scripting)**
  Attacks on websites or applications using hidden malicious code. They can steal information or affect system working.
- **Unauthorized downloads and browser-based attacks**
  Downloading unknown files or visiting unsafe websites. This can install viruses or spyware on the system.
- **Privilege escalation and unauthorized access**
  Getting access to systems without proper permission. This can allow full control over data or systems.
- **Internal threats (misuse by staff)**
  Employees misusing system access or sharing data wrongly. This can lead to fraud, data loss, or security issues.

Potential risks and impact include:

- Financial frauds affecting the Bank and its customers
- Loss, theft, or leakage of sensitive customer data
- Failure or disruption of IT systems, network, and services
- Interruption of banking operations and customer services
- Reputational damage to the Bank
- Non-compliance with RBI guidelines and applicable laws

The Bank shall establish appropriate controls and monitoring mechanisms to identify, prevent, and mitigate cyber risks and ensure secure and continuous banking operations.

Compliance

Non-compliance with the Bank's Cyber Security Policy and related standards by employees or third parties shall attract disciplinary action, including termination of employment or contract, in accordance with the Bank's rules and applicable regulatory provisions. Such non-compliance may also attract penalties under relevant laws and RBI guidelines.

All employees, vendors, and service providers shall promptly report any actual or suspected information security incident, including data loss, breach, or system compromise, to the Bank Management/Information Security Officer. The Bank shall ensure timely investigation, containment, and reporting of such incidents to RBI, CERT-In, or other regulatory authorities, as applicable.

The Bank shall appoint qualified Information Systems (IS) Auditors to conduct annual IS Audit and Cyber Security Audit covering the Head Office, Data Centre, and all branches, in line with RBI guidelines. Audit findings shall be placed before the Board/IT Committee, and compliance shall be ensured within stipulated timelines.

The Bank shall obtain and review annual security and compliance reports from critical vendors, including CBS provider M/s Wintech Solutions Pvt. Ltd., such as:

- Cyber Security / Information Security Audit Certificate
- Business Continuity and Disaster Recovery (BCP/DR) test reports
- Vulnerability Assessment and Penetration Testing (VAPT) reports
- Any other reports as required by RBI or the Bank

The Bank shall maintain proper records of compliance, audit reports, and corrective actions for review by regulators and auditors.

Disciplinary Action

Any violation of the Bank's Cyber Security Policy, procedures, or controls, including involvement in any unauthorized or malicious activity, shall be treated as a serious misconduct.

The Bank shall initiate appropriate disciplinary action against employees, contractors, or third parties found in breach of the policy. Such action may include suspension, termination of employment/contract, and/or legal proceedings, depending on the nature and severity of the violation, in accordance with the Bank's internal policies and applicable laws.

The disciplinary framework is intended to ensure accountability, enforce compliance, and act as a deterrent against security breaches and policy violations.

Operational Setup of Banking

The Bank's IT and digital banking operations are supported by authorized service providers as detailed below:

- **Core Banking System (CBS):** Provided and maintained by M/s Wintech Solutions Pvt. Ltd.
- **Switching Services (UPI / IMPS / ATM):** Provided by M/s Sarvatra Technologies Pvt. Ltd.
- **NEFT/RTGS Services:** The Bank operates as a sub-member through Host-to-Host arrangement with HDFC Bank and Yes Bank
- **CTS (Cheque Truncation System):** The Bank operates as a sub-member of IDBI Bank

- **ATM Acquirer Bank:** IDBI Bank
- **Hardware Maintenance:** Managed by M/s OASIS Computers
- **Server Infrastructure:** Hosted and maintained in-house by the Bank

The Bank currently operates from the following locations:

Head Office (HO):
The Mahaveer Co-operative Bank Ltd., Belagavi
1157, "Shree Renuka Towers", Anantshayan Galli, Belagavi – 590002

Branches:

1. Main Branch
2. Angol Branch
3. Vadagaon Branch
4. Kakati Branch
5. Basvan Kudachi Branch
6. Peeranwadi Branch
7. Shahapur Branch

(*The number of branches may be increased in future.*)

At branch level, the Bank has deployed the following infrastructure:

- Computer systems for banking operations
- Local Area Network (LAN) connectivity
- Internet connectivity for communication and banking services
- Wi-Fi (wherever applicable)
- CCTV systems for monitoring
- UPS for power backup

Data Centre / Server Room Controls:

- In-house servers with restricted access
- Air-conditioning (AC) to maintain required temperature
- Proper ventilation and clean environment
- Fire safety and firefighting equipment
- Continuous power backup (UPS)

Human Resource Management – User Responsibilities & Accountability

All employees and contract staff of the Bank shall be responsible for safeguarding information systems and data. They shall be held accountable for all activities carried out using their assigned user credentials

Information security responsibilities shall be clearly defined as part of job roles, including compliance with security policies and protection of critical information assets. These responsibilities shall be communicated at the time of recruitment, included in employment terms, and monitored throughout the employment period.

1. New Joining (Hiring)
All employees and contract staff shall be informed about confidentiality of Bank information, customer data privacy, and non-disclosure requirements.
This shall be acknowledged through appointment letters, service rules, and security awareness training.

with agreement

2. User ID Creation

- User IDs for CBS and other systems shall be created only with approval from the respective Branch Manager or Department Manager.
- User access shall be granted based on roles and job responsibilities.
- Official email IDs shall be created with appropriate approval from the Manager/Management.

3. Resignation and Termination
All employees and contract staff shall follow the Bank's formal exit procedures.
On separation, the concerned Manager shall ensure:

- Recovery of all Bank assets, documents, and confidential information
- Immediate disabling of user IDs and email access
- Proper documentation and record maintenance of exit formalities

4. Review of Access
User access rights in CBS and other systems shall be reviewed by the respective Branch Manager or Department Manager to ensure that access is appropriate and no unauthorized access exists.
Such review shall be conducted at least on a quarterly basis and documented for audit purposes.

Specific Security Controls

a) Data Classification and Inventory
The Bank shall classify data as:

- **Sensitive:** Strategic, legal, and restricted management data
- **Confidential:** Customer data, account details, internal communications, system configurations
- **Public:** Information approved for public use such as services and financial statements

The Bank shall maintain an inventory of all IT assets including hardware, software, network, vendor details, licenses, and system configurations. Access to system documentation shall be restricted to authorized personnel.

Sensitive documents and backup media shall be securely stored in locked/fireproof cabinets and disposed of safely when no longer required.

b) Prevention of Unauthorized Software Access

- Users shall not have administrator rights on PCs
- Only authorized software shall be installed
- Antivirus shall be installed and updated on all systems
- USB access shall be restricted
- Remote access shall be allowed only with approval

c) Physical and Environmental Controls

- Servers and network devices shall be kept in secure locations with restricted access
- CCTV surveillance shall be maintained at critical areas
- Proper environmental controls such as air-conditioning, cleanliness, and fire safety shall be ensured
- UPS and backup power systems shall be available

d) Network Security

- Secure connectivity between branches and Data Centre using VPN/leased lines
- Firewalls and routers shall be configured securely with strong passwords
- Internet access shall be restricted to authorized users
- Wi-Fi shall be secured with strong encryption
- Network logs shall be monitored regularly
- Secondary network links shall be maintained for redundancy

e) Secure Configuration

- Systems and servers shall be hardened by disabling unused services and ports
- Default passwords shall be changed

- Logs shall be enabled and reviewed periodically
- Only required applications shall be installed

f) Anti-Virus and Malware Protection

- Standard antivirus software shall be installed on all systems
- Antivirus shall be regularly updated and not disabled without authorization
- Systems shall be protected from malware, spam, and malicious code

g) User Access Control

- Access shall be provided based on role and approval from Manager
- Users shall follow strong password practices
- Access shall be removed immediately upon exit
- Access rights shall be reviewed periodically

h) Email and Data Security

- Official email IDs shall be used for Bank communication
- Public email services shall be restricted
- Data sharing shall be done through secure channels only (VPN, SFTP, etc.)
- Public-facing systems shall be protected through firewall and SSL
- Periodic VAPT shall be conducted

i) Removable Media Control

- Use of USB and external media shall be restricted and monitored
- Backup media shall be securely stored and tracked
- Media shall be securely disposed when no longer required

j) Security Awareness

- Regular training programs shall be conducted for employees and contractors
- Topics include password security, phishing, system usage, and incident reporting
- Training records shall be maintained

k) Customer Awareness

- Customers shall be educated on safe banking practices through SMS, email, or other channels

- Awareness shall include fraud prevention, OTP/PIN safety, and digital usage

l) Backup and Recovery

- CBS data backup shall be maintained by vendor (real-time/daily)
- Branch and system data shall be backed up periodically
- Backup records and retention shall be maintained as approved by management

m) Vendor Risk Management

- Vendors shall be selected after proper due diligence
- Agreements shall include SLA, security requirements, and audit rights
- Vendors shall sign Non-Disclosure Agreements (NDA)

n) Business Continuity

- The Bank shall maintain BCP and ensure availability of backup systems
- Risks such as power failure, network failure, fire, and natural disasters shall be addressed
- Emergency contact details shall be maintained at all branches

o) Incident Management

- All security incidents shall be reported immediately to management
- Major incidents include data breach, fraud, unauthorized access, and system attacks
- Incident records shall be maintained and reviewed
- Significant incidents shall be reported to RBI/CERT-In as applicable

Password Policy

- Minimum 8 characters with mix of upper/lower case, numbers, and special characters.
- Unique passwords for each system; no sharing of credentials.
- Passwords must be changed every 90 days or immediately upon suspected compromise.

Digital Payment Security

The Bank shall implement appropriate security measures to ensure the safe and secure processing of digital payment transactions, including UPI, IMPS, and ATM operations.

- **Transaction Monitoring:** Daily monitoring of all digital payment transactions shall be conducted to detect unusual or suspicious activities.
- **Fraud Detection and Alerts:** Robust fraud detection mechanisms shall be in place, with automated alerts for potential frauds or unauthorized transactions.
- **Reporting:** Any identified anomalies or fraudulent attempts shall be immediately reported to Bank Management for investigation and regulatory reporting, as required by RBI guidelines.

Access Control

The Bank shall implement strict access control measures to ensure that only authorized personnel can access information systems and critical banking operations.

- **Role-Based Access Control (RBAC):** Users shall be assigned access rights based on their roles and responsibilities; ensuring access is limited to what is necessary for their job functions.
- **Maker-Checker Concept:** Critical transactions in the Core Banking System (CBS) shall follow the maker-checker principle to prevent errors or unauthorized activities.
- **Periodic Access Review:** User access privileges shall be reviewed periodically to ensure appropriateness and compliance with Bank policies.
- **Immediate Revocation:** Access rights shall be promptly revoked for employees or contractors upon termination, resignation, or role change.

Business Continuity & Disaster Recovery (BCP & DR)

The Bank shall ensure continuity of critical banking operations and minimize disruption in the event of system failures, disasters, or other unforeseen incidents.

- **BCP & DR Plans:** Comprehensive Business Continuity and Disaster Recovery plans shall be maintained, documented, and approved by Bank Management.
- **Periodic DR Drills:** Disaster Recovery drills shall be conducted periodically to validate the effectiveness of recovery procedures and ensure readiness of IT and operational teams.
- **Continuous Improvement:** Lessons learned from drills or actual incidents shall be incorporated into the BCP and DR plans to strengthen the Bank's resilience.

Acceptable Use Policy

1. General Use and Ownership

All information, systems, and data created, stored, or processed on the Bank's IT infrastructure shall remain the property of the Bank. Users shall ensure that the use of IT resources is appropriate, limited to official purposes, and in line with Bank policies.

The Bank reserves the right to monitor, review, and audit all systems, networks, and data to ensure security, integrity, and compliance with applicable regulations.

2. Security and Proprietary Information

Users shall maintain confidentiality of login credentials and shall not share user IDs or passwords under any circumstances. Systems shall be secured when unattended to prevent unauthorized access.

Users shall exercise due caution while handling emails, attachments, and external links to prevent malware infections. All systems shall have approved and updated antivirus protection.

Any communication on behalf of the Bank, including through email or social media, shall be made only with proper authorization.

3. Unacceptable Use

Use of the Bank's IT resources for any unlawful activity or in violation of Bank policies, RBI guidelines, or applicable laws is strictly prohibited.

4. Prohibited Activities

The following activities are strictly prohibited:

- Unauthorized access to systems, data, or network resources
- Installation or use of unlicensed or unauthorized software
- Introduction of malware or malicious programs
- Sharing of login credentials or misuse of user accounts
- Unauthorized copying, transmission, or disclosure of Bank information
- Bypassing or attempting to bypass security controls
- Use of hacking tools, scanning tools, or similar activities
- Any activity that may disrupt systems, services, or operations of the Bank
- Unauthorized communication or public statements on behalf of the Bank

Email and Communication Activities

The following activities are strictly prohibited while using the Bank's email and communication systems:

- Sending unsolicited or bulk email messages (spam)
- Sending offensive, abusive, or harassing messages through email, telephone, or other communication channels
- Forging, altering, or misrepresenting email header or sender information

- Creating, forwarding, or participating in chain mails, Ponzi schemes, or unauthorized religious, political, or fraudulent communications
- Excessive personal use of network resources, including video streaming, torrent downloads, or large unauthorized downloads

Branch Cyber Security Policy

All Branch Managers shall read, understand, and acknowledge the Cyber Security Policy of the Bank. A copy of the policy shall be maintained at each branch for reference and compliance.

The Bank has deployed necessary IT infrastructure at branch level, including computer systems, network connectivity, internet access, CCTV systems, power backup (UPS), and required environmental controls to support secure banking operations.

Cyber Security Controls at Branch Level

a) User System Controls

All user systems shall be configured and maintained in a secure manner. Users shall be provided access strictly based on their roles and responsibilities. Administrator rights shall not be granted to end users.

All systems shall be protected with updated antivirus software. Use of external media, remote access, and internet browsing shall be controlled and permitted only with proper authorization. Access to critical systems such as NEFT, RTGS, and ATM operations shall be restricted to authorized personnel only.

b) Physical and Environmental Controls

Physical_Security:

Branch premises shall be secured through appropriate physical controls. CCTV surveillance shall be implemented for monitoring critical areas on a continuous basis, and recordings shall be maintained for a defined retention period.

Environmental_Controls:

Branches shall maintain proper environmental conditions including cleanliness, adequate temperature, and humidity control. Power supply shall be supported by UPS and backup arrangements. Fire safety measures, including installation of appropriate firefighting equipment, shall be ensured.

c) Network Security
Network infrastructure at branches shall be securely configured and managed by authorized personnel. Any changes to network configuration shall be carried out only with prior approval.

Internet access shall be restricted and monitored. Firewalls and filtering mechanisms shall be implemented to allow only authorized access to required services and websites.

Wi-Fi Security:
Wi-Fi networks, wherever deployed, shall be secured using strong encryption and passwords. Access shall be restricted to authorized systems, and use of personal devices shall not be permitted.

d) Anti-virus and Patch Management
All systems shall be protected with approved antivirus and anti-malware solutions. Such solutions shall be regularly updated and shall not be disabled without authorization.

Necessary security patches and updates shall be applied periodically to ensure protection against known vulnerabilities.

e) Incident Management
All security incidents or suspected weaknesses shall be reported immediately to the Branch Manager and Bank Management.

Branches shall maintain proper records of incidents and related actions taken. Incidents impacting operations, customer services, or data security shall be treated as critical and handled on priority.

Indicative incidents include unauthorized access, cyber-attacks, data leakage, phishing attempts, and financial frauds.

Revision of Policy
The Board of Directors shall review the Cyber Security Policy annually and update it as needed to address operational changes, market conditions, and RBI guidelines, ensuring its effectiveness and compliance.

The Mahaveer Co-operative Bank Ltd., Belagavi

Chief Executive Officer/Vice-Chairman/Chairman

THE MAHAVEER CO-OP. BANK LTD. BELAGAVI