CyberSecurityPolicy

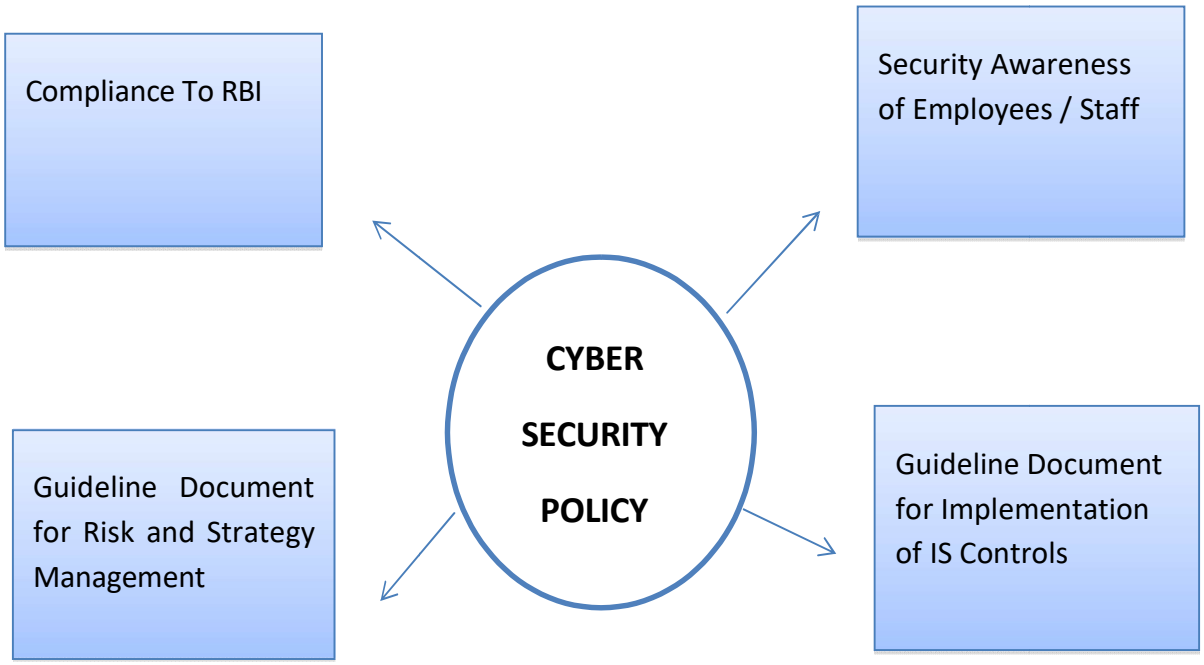
1.1 Purpose

This document provides the framework for the protection of The Mahaveer Cooperative Bank Ltd. (TMCBL) information assets, and to allow the use, access and disclosure from Cyber Threats, attacks in accordance with appropriate standards, laws and RBI Guidelines.

The **Cyber Security policy** adequately includes the **Information Security Policy** aspects of the bank to provide assurance on secure banking operations and IS Controls.

TMCBL reserves the rights to change, amend, suspend, withdraw, or terminate any or all of the policies, in whole or in part, at any time.

The Cyber Security Policy serves the below purpose for the bank-



1.2 Executive Summary

"Information" is an asset and consequently needs to be appropriately protected. There are wide ranging threats to the banking and financial industry and it may impact the bank, customers in case suitable precautions are not put in place.

The number, frequency and impact of cyber incidents / attacks have increased manifold in the recent past, more so in the case of financial sector including banks.

Cyber security policy is driven by the following control objectives for protection of assets:

- **Confidentiality**relatestotheprotectionofsensitiveinformationfromunauthorizedaccess.
- **Integrity** relates to the accuracy and completeness s of information ; and the validity of information in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process. It also deals with safeguarding necessary resources and associated capabilities.
- **Privacy** relates to controls over authorized access of personal information, KYC and other details of customers used for banking operations.

Information security is achieved by implementing suitable sets of administrative, physical and technical controls, which could be policies, practices, procedures, organizational structures, technology and software.

1.3 Scope

The Cyber Security Policy applies to any person (management, users and administrators, contractors and third parties) who access information using TMCBL IT, business systems, regardless of geographic location.

The term Information Systems defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware, software, and information. The Cyber Security Policy is applicable at Bank HO /AO and Branches.

In particular, the bank Cyber Security Policy applies to the following information assets of TMCBL:

- All proprietary information that belongs to TMCBL.
- Personnel information relating to employees of TMCBL.
- All customer related information held by TMCBL.
- All suppliers, contractor and other third-party information held by TMCBL.
- All software assets such as TMCBL Banking data, other databases, application software,tools and utilities.
- All physical assets, such as hardware computer equipment, communications equipment, media and equipment relating to facilities.
- All services, such as power, lighting, HVAC associated with TMCBL information systems.
- TMCBL Human Resources

If any aspect of this policy is in conflict with any national, state, local and other laws, TMCBL will comply with the laws and regulations and inform the management when such laws prohibit compliance.

1.4 Management Commitment

TMCBL is committed to have a comprehensive control environment that includes policies, processes and control activities that leverage various aspects of TMCBL IT infrastructure, services environment.

Management of TMCBL shall prepare long term and short-term strategic business plans along with suitable Cyber Security management plans.

TMCBL shall review the strategic business plan on Annual basis. IT strategy plans are prepared in line with strategic business plans.

IT strategy group is responsible to take key decisions, provide guidelines, handle conflict tsand review status of projects. IT strategic group may include -

- CEO
- Head IT
- 1or2 Board Members

CyberRiskAssessmentshallbedoneonAnnualbasisbybanktoassessbelowaspects-

- Current Banking Operations, Infrastructure
- Cyber Risk Scenario
- IT Failures, Data Loss aspects
- External Factors-including Vendors, competition, market factors
- Laws, regulations as per IT Act 2000,RBI
- Resource failure or non-availability risks
- Financial fraud

Management shall engage, to understand Cyber Risks and type of attacks affecting the financial sector industry. Management shall understand the different type of risks and strive to implement additional IS controls as required. Type of Risks are-

- **Inherent Risk**-that applie stop ssible financial fraud setc. Of the banking and financial industry.
- **Residual Risk**-that remain seven after implementation of suitable best IS controls.
- **Acceptable Risk** - that of possible losses in case of any failure / Cyber-attacks, which the management should plan to absorb in case it happens.

TMCBL management is committed to provide resources, budgets and approvals to drive the IT, Cyber and Information Security Objectives.

Management recognizes the need to provide timely information regarding any breach or intrusions to the respective authorities Cert-in, Department of Cooperative Bank super visionor any other authorities as required in future.

Bank shall implement the security controls as feasible and those covered in the policy document. The implementation of this policy is a testimony of BANK's commitment to establish, implement, maintain, and continually improve the information security management.

Cyber Security policy is aligned to the requirements of the BANK, which is committed to:

- Comply to all applicable laws and regulations and contractual obligations
- Implement information security requirements following the results of applicable risk assessments
- Communicate these Objectives to all interested parties
- Provide resources to meet information security requirements
- Instruct all members of staff about the needs and responsibilities of Information Security Management
- Implement continual improvement initiatives, including risk assessment and risk treatment strategies

BANK shall implement procedures and controls at all levels to protect the **Confidentiality, Integrity, Availability and Privacy** of information stored and processed on its systems and ensure that information is available to authorized persons as and when required.

1.5 Understanding Cyber Attacks and Risks

Cyber-attack means any attack that tries to misuse IT services, create data or financial loss or cause disruption to the banking operations, customer services through digital means such as through Internet, email, mobile devices, networks, whether started from Inside the bank or outside shall be termed as Cyber Attack Risk.

Attack Types-Indicativelist

- **Application Vulnerabilities-**Include CBS, Website, other software
- **Denial of service attack**: A denial-of-service attack (DoS attack) generally consists of the concerted efforts of a person/persons to prevent an internet site or service from functioning efficiently. A DoS attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.
- Cross Site Scripting - Injecting of malicious code and data in the transactions using application weakness.
- Web/Online Application Other Vulnerabilities-As per OWASPT op10

- **Distributed denial of service (DDos)**: In a distributed denial-of-service (DDoS) attack, large numbers of compromised systems (sometimes called a Bot net) attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby, denying the service of the system to legitimate users.

- **Ransom ware**: Ransomware is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

- **Malware**: Malware is the term for maliciously crafted software code. Special computer programmers now exist that enable intruders to fool an individual into believing that traditional security is protecting him during online banking transactions. Attacks involving malware are a factor in online financial crime.

- **Phishing**: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

- **Spear phishing**: Phishing attempts directed at specific individuals or companies have been termed spear phishing. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success.

- **Whaling**: The term whaling has been coined for spear phishing attacks directed specifically at senior executives and other high-profile targets. In these cases, the content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email may be an executive issue such as a subpoena or customer complaint.

- **Vishing**: Vishing is the illegal access of data via voice over Internet Protocol (VoIP). Vishing is IP telephony's version of phishing and uses voice messages to steal identities and financial resources. The term is a combination of 'voice' and 'phishing'.

- **Drive-by downloads**: Drive-by download means two things, each concerning the unintended download of computer software from the Internet:

- Downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically
- Any download that happens without a person's knowledge, often a computer virus, spyware, malware or crime ware.

- **Browser Gateway frauds**: The information sent and received from a PC/device is routed through anun desired path on the network there by exposing it to unauthorized entity. The only gateway to outside world for the PC/device being the browser that has been compromised.
- **Ghost administrator exploit**: A ghost administrator exploit is a code that takes advantage of a software vulnerability or security flaw to gain Administrator's rights/privileges in the system. This exploit allows the attacker to mask his identity in order to remotely access a network and gain Administrator rights/privileges, or move deeper into the network. In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor viruses and/or spyware to steal user information from the infected systems.
- **Internal Attacks** (initiated by insiders working in banking network) - Misuse of IT systems, Misuse of Access authority, Data Thefts, Information Disclosure and technical information leakage.

Risk Types and Impact

- Financial frauds in the bank accounts
- Financial frauds affecting customer accounts
- Failure of Servers, Infrastructure and Network
- Loss of Customer Private data
- Reputation Risk of Bank
- Failure of Customer Services
- Failure of Banking Operations

- Data loss to unauthorized parties
- Failure of compliance to IT Act 2000,RBI Guidelines

1.6Compliance

Failure to comply with bank's Cyber Security Policy and standards by employees or outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable TMCBL procedures.

In the case of outside affiliates/vendors, term in at ion of the affiliation/contracts. Further, penalties associated with local, state, national laws may apply.

Any person who becomes aware of any loss, compromise, or possible compromise of TMCBL information, or any other incident which has information security implications, will immediately inform the Bank Management who will initiate immediate investigation or take action to prevent further compromise or loss.

TMCBL shall engage qualified IS Auditors to perform Annual audit at HO / Branches to assess IT and cyber risks to ensure compliance with this policy and as per RBI guidelines.

The Bank shall collect compliance reports once a year, from CBS vendor-

- Cyber and information Security Audit Certificate
- Evidence of Business Continuity DR Drills
- Vulnerability Assessment Test Reports(VAPT)
- Any other

1.7 Disciplinary Process

Disciplinary process is applicable for any untoward or unwanted incident that violate the TMCBL Cyber Security Policies. Such a process would act as a deterrent to employees / contractors who may disregard the basic controls desired by the bank and Cyber Security Policy.

The disciplinary action may be taken in case of breach of the bank policies including up to suspension, termination or legal actions as per the merits of the incident.

1.8 Operational Setup of Banking

Bank has contracted with Wintech Software Consultants to provide the CBS solution.

As part of the solution **Responsibilities**

Provision of CBS Software Services

- Allied bank in services as allowed by RBI such as NEFT,CKYC,ATM,SMS
- Primary Data Centre and DR site
- Maintenance service of CBS Application as per RBI guidelines
- Performance Management of Server, Data Centre Infrastructure solution(s)
- Business Continuity of CBS solution
- Data backup services

Current setup at bank is as per below-

BANKcurrentlyOperatesfromthefollowinglocation/branches*intheregion-

Type	Name/Location
HO	The Mahaveer Co-Op. Bank Ltd., Belagavi 1157,"Shree Renuka Towers", Anantshayan Galli, Belagavi - 590002
Branches	1. Main Branch 2. Angol Branch 3. Vadagaon Branch 4. Kakari Branch 5. Basavan Kudachi Branch 6. Peeranwadi Branch 7. Shahapur Branch (More branches may be added in future)

*Numberofbranchesmaybeaddedgoingforward.

At Branches BANK has the deployed the following Infrastructure–

- Computer Terminals/ PC for banking operations
- Local Network connectivity for inside the branch
- Internet Connectivity for email, communication systems
- Wifi Network, if needed
- CCTV camera(s) for monitoring
- UPS for power backup to systems
- Environmental Controls including
    - Dust Free and Humidity free and Clean work areas
    - Air-conditioning, Firefighting equipment

1.9 Human Resource Management

User Responsibilities/ Accountability

The protection of the information systems resources is a responsibility of all BANK employees. Employees and contract staff will be held accountable for all activities performed by them on BANK information systems resources.

Job definition includes general responsibility of implementing or maintaining security policies as well as specific responsibility of protection of critical assets and security processes or activities.

Security responsibilities will be addressed at the recruitment stage, included in employee contracts, and monitored during an individual's employment.

New Joining (Hiring)

All employees and contract staff will be informed about confidentiality of bank data, Customer Privacy protection and non-disclosure of information without approvals.

The staff shall be informed and shall acknowledge understanding of these clauses through- Appointment Letters or Service Rule Book And through security awareness training.

Log in ID Creation

Banking Login ID: ID shall be created for users post approval by respective Head of Departments (HOD).

The ID creation process request shall include details such as-
Employee Name, ID created, User Group and Role
Email ID: Corporate email ID (eg@corpbank.in/com) Shall be created, duly approved by the management / HOD.

Resignations and Terminations

All Employees and contract staff will complete at termination process/separation procedures of the BANK.

At time of EXIT due to resignation or termination cases, the employee's manager will ensure that files, documents, manuals, brochures, privileged information, passwords and laptops/mobile devices in possession of the employee or contract staff, are recovered.

Disable user ID/Email ID of the user on the date of exit from IT Systems

Records of employee exit or separations hall be maintained in personal files.

Review of Access

Respective HOD shall review User Access in CBS as per Roles and confirm the same to HO to ensure no unauthorized user exist in system

Process should be completed once every 3months (quarter).

1.10 Specific Security Controls

a) Data Classification and Inventory

Data of TMCBL shall be classified as below-

Sensitive	Data related to future strategies of bank or any other data which is for restricted use by senior management only. Information related to legal matters Any other as deemed suitable by Management
Confidential	Customer Private data, Customer accounts / personal or financial details, communication/documents pertaining to customers. Bank Internal Communications between HO/Branches Bank transaction, Signatures Data Operational Problems details Technical Configuration of systems, IT, Networking and CBS applications
Public	Bank Services details Notification set c published on websites Approved financial statements Any other deemed suitable by bank

b) Inventory Management of Business IT Assets

- IT shall maintain documentation related to
    - IT Hardware, Software and networking assets
    - Details of vendor contracts, SLA
    - Software Licensing details
    - Problem/change registers of Software, hardware, networking complaints(tickets) and closure details
    - Network Diagrams of HO and Locations
    - Important Configuration settings of OS, applications
    - Legacy systems and equipment (OLD server, applications)

- TechnicalSystemdocumentationwillbesecured,backuptakenandphysicallyprotected.

- The distribution of confidential system documentation like network or system design will only be restricted to authorized users.

- All system documentation (technical manuals, user manuals, client documentation etc.) must be stored in a secure environment and protected from unauthorized access. Protections procedures should restrict both machine and physical access to only authorized users.

Sensitive Documents and Media

- Sensitive documents will be stored in suitable locked cabinets, when not in use, especially after working hours.

- Computer media like back up of CBS, CD drives will be stored infire proof locked cabinets /safes.

- Incoming and outgoing mail points, unattended faxes and photocopier machines will be protected from unauthorized use outside normal working hours.

- Any business sensitive document in hard copy, if not required, must be shredded or securely destroyed.

c) Preventing access of unauthorized software

User PC/ Desktop Notebooks

- Bank Users shall not have Administrator RIGHT Son PC. Users shall use be given STANDARD users access
- PC shall be protected by suitable and updated Anti-virus solution.
- Remote access(RDP)from PC shall not be allowed, unless approved
- USB port shall be disabledon PC.
- Provide Security Awareness Training of staff and users
- Define Acceptable use policy of the bank

d) Physical and Environmental Controls

TMCBL shall put in place suitable controls to provide a good working environment to Servers, Network and other equipment at Data center and branches.

- Servers, Firewall, networking equipment shall be maintained in as ecure environment with physical controls at Data Centre and Branches.
- **Physical Security**
    - Physical security shall be maintained
    - CCTV systems monitor sensitive and relevant are as of the HO, Branch office premises using night vision cameras on 24x7x365 basis.
    - The recordings are captured using PC or DVR systems.
        - Recordings shall be moved to external HDD backup media on a weekly basis.
- **Environmental Controls**
    - Proper Cleanliness, Temperature and Humidity controls shall be ensured
    - Air-conditioning systems shall supply suitable temperatures (15-20C)in Data Centre areas.
    - Network cabling shall be maintained in proper condition
    - Stable Power supply shall be made available using transformers and UPS
    - Back up power shall be supplied by generator systems at all locations, as feasible.
    - Proper and serviced Fire Fighting equipment shall be installed at all locations.

e) Network Management and Security

Banks shall install and maintain suitable devices for connectivity between branches and data centre.

- Network bandwidth is installed after due capacity requirements for:
    - Secure network Links shall be established using-VPN, Leased Lines, SSL
    - Firewall and routers shall be configured using following rules-
        - Minimum Access
        - Open Allowed services/IPS our cesonly
        - Reset of Default password with STRONG passwords
        - AMC of Firewall/Routers shall be taken by Bank
            - Keep Device and Software up-to-date
    - WiFi Services
        - Configure WPA2 Security
        - Setup STRONG password (atleast 10 characters)
        - Allow only on Authorized PC
        - Do not Allow to be used on Personal Devices(Notebook/ Mobile)
    - Secure and limited access to Internet services at each location.
        - Allowed to select and authorized users only
        - Implement Internet FILTERS for allowing access to required sites only.
    - Redundant(secondary)links preferably from alternate ISP are established incase of failure of primary links.
    - Set up mechanisms and tools for detection for problem, error and changes tracking

- Review Device logs on regular basis.

- ISP services and SLA shall be reviewed on quarterly basis.

- Link bandwidth utilization report shall be prepared / taken from vendor, once a month for review of utilization, over and under use of bandwidth.
- Incase required bandwidth capacity and quality of services are reviewed with management.
- Secure links between HO and branches shall be established using Leased Links, VPN and SSL and other prescribed methods.
- For NEFT / RTGS / ATM and other sensitive operations allocate specific PC which shall be allowed to be used by authorized personal only.

f) Secure Configuration

Configuration of sensitive devices such as Firewall, Routers, Server setc shall be maintained as per below standards.

- Local Bank Servers (If, Available)shall be hard ened-

  - Install only required OS, applications and software only
  - Close Ports/Services not in use
  - Do NOT use Administrator user ID
  - Create alternate User with Administrator ID Access
  - Enable logs/Review logs Periodically
  - Keep Backup of logs for period of 30days

g) Anti-virus

TMCBL will employ malware protection mechanisms at critical information system entry and exit points (e.g., mail servers, web servers and at workstations, servers, or mobile computing devices on the network. Malware protection will also include SPAM protection).

- Authorized standard anti-malware anti-virus software will be installed on all servers, laptops and desktops.
- The anti-malware software will be updated automatically or periodically.

- Anti-malware protection will NOT be disabled during normal functioning of systems unless authorized through change management process.
- Anti-malware mechanisms will be used to detect and CLEAN malicious code and/or SPAM (e.g., viruses, worms, Trojan horses, spyware) transported by electronic mail, electronicmailattachments,Internetaccesses,removablemedia(e.g.,USBdevices, diskettes or compact disks), or other common means; or by exploiting information system vulnerabilities.

h) User Access Control/ Management

Users working at TMCBL shall be provided Access to PC,CBS,post approval from respective HODs.

- Access to user shall be allowed for specific work/roles-Eg:Supervisor,Clerical, Manager, Other type of Users.
- Users shall be created after approval of respective Managers.

- Access to File/Folders (in case of share)shall be allowed as per “Need to Use”basis only.
- Admin access to PC shall not be allowed.

- Users shall change password-As per defined policies of Servers, CBS operations

- Passwords should be 8 or more characters long(Complex should been abled,if desired)

- User access shall be removed, when user leaves/resigns from bank services

i) Secure mail and messaging systems

The policy is to ensure that all data communication within/outside the bank is performed as per security best practices.

EMAIL

- Banks should use OWN corporate email ID for work purposes(egab.coopbank.com/ in)
- Open email accounts such as Gmail, Yahoo etc shall NOT be used. If required in special case, it may be allowed to ONE or TWO authorized users only.
- Email access should be allowed from within bank office premises.
- Web Access to email may be provided to select HOD(users)only.
- Creation/Management of email account, shall be done by approval of management only.

Data Exchange

- Use of OPEN storage (Drop box, Google Drive, etc)shall be disallowed.
- Exchange of data shall be with authorized and approved links only (Eg HDFC, host bank etc).
- Exchange of data shall be done through VPN, SSL, SFTP and secure links only.
- Exchange of data shall pass through in Firewall devices installed at location.

Public Facing Server(if,Applicable)-Devices directly connected to Internet using Public IP

- Servers shall be accessible through Firewall only and Secure Socket Layer (SSL) should be implemented.
- Annual Vulnerability Assessment and Penetration Testing (VAPT)shall be completed for such servers / devices deployed by bank in the Data Centre or Cloud hosting locations.

j) Removable Media

- Only authorized users/access may be allowed for removable media in case used for backup and official purposes (External HDD/Tapes etc).
- Removable media Inventory shall be maintained.
- Media shall be labeled and stored in Fire Safe cabinets only.
- Access to USB on authorized systems shall be monitored.

Disposal of Media

- Media shall be disposed of securely and safely when no longer required.
- The following items will require secure disposal:
    - Any paper document containing sensitive information-Shredder should be used.
    - Any media HDD, CD, USB containing sensitive information.Secure disposal methods will be established such as shredders, disk wiping based on DoD standards, physical destruction of disks and/or degaussing.

k) Security Awareness-Users/Employees

Staff at TMCBL shall be made aware of the Information Security Policies and Procedures. To facilitate this awareness training programs shall be conducted on periodic basis, to explain the need for information security and provides the users with adequate learning.

- Users will receive training on security awareness and responsibilities as well as training in the correct use of information processing facilities e.g. logon procedure, software privileges.
- SecurityAwarenessOrientationSessionswillalsobeconductedforlong-termcontractors also, who will access TMCBL Information System infrastructure and resources.
- The Security Awareness Orientation program will include following areas:
    - Introduction to Information Security
    - Password Guidelines
    - E-mail system
    - Internet Usage
    - Desktop/Laptop Security
    - Personal Data Backup
    - Virus Controls
    - Clear Desk and Clear Screen

- Physical Security
- Reporting of Security Incidents
- CBS, Secure Banking

- The employees, staff and long-term contractors will sign a declaration confirming the attendance and understanding of the security awareness sessions.
- Training records shall be maintained by Bank.

l) Customer Education and Awareness

TMCBL shall provide training to customer regarding Cyber risks, use of safe banking, online e-commerce, other are as through regular programs. Awareness should cover InternetBanking, ATM, CVV, PIN, ID and Password, Hacker tricks, Safe digital use tips etc.

The program shall help build the Brand image of the bank and overall banking experience to become safe for the customers of the banks.

- Banks shall send periodic email to customers
- Banks may educate customers through Mobile SMS, Mobile App or any other method for safe banking, e-commerce etc.

m) Backup and Restoration

TMCBL shall ensure suitable backup are available of bank data, infrastructure and that bank is ready to provide secure services to the customers.

Backup and Recovery Procedures are as per below-

- CBS Data backup–is maintained on Real time, DAILY and offsite by CBS Vendor
- Bank Files and folders on PC/Notebooks–WEEKLYBACKUP–Alternate Storage Media
- CCTV back up at each Branch–WEEKLY–Offline Media(External HDD)
- Email data backup–WEEKLY BACKUP–Using Alternate Storage Media(External HDD)

- The frequency of backup and retention period of the backup data will be determined and approved by the management.

n) Vendor/Outsourcing Risk Management

Vendor services are critical to run banking operations. Bank may engage software, hardware, networking and other service vendors to manage smooth IS operations.

Bank must ensure vendors-

- Get selected after appropriate evaluation of their background, experience and quality of services. Bank may validate vendor services from other customers serviced by vendors.
- Commence work after proper contractual agreements defining Scope, SLA of services, Period of contracts, right to audit, Escalation Matrix and penalty clauses as applicable.
- Sign suitable Non-disclosure agreements, in respect to on site / off site services for the bank.
- Contracts are reviewed, revised and approve do nan annual basis.
- Service records, service short coming are recorded and maintained by IT / Other teams as applicable.

o) Business Continuity

A management process by BANK is in place to protect the Organization, especially its critical business processes, from the effects of a major failure or disaster, and minimize any damage or loss caused by such events.

BANK maintains the following –

- UPS for power backup
- Fire Protection Systems
- Primary link for CBS(provided by CBS Vendor)
- Secondary Network Link managed by Bank
- Ability to operate CBS from Alternate Branches, if required during network / other disruption at branch.

CBS Vendor SIPL shall provide Business Continuity Services of the Primary Data Centre and DR sites, Primary Network link as required.

However, bank management should address the following at branches-

- Secondary Network Link Up time and failure
- Power Failure
- Fire Situations
- Water Flooding during rains/as per location
- Hardware and Network Failure(s)
- Availability of Bank Operational and IT

Staff Bank should consider-

- Identify the events and environmental surroundings that can adversely affect the Organization and its facilities with disruptions or disasters, the likelihood and impact of such occurrences.
- Providing awareness and training programs in event of such situations, including emergency and crisis management procedures.
- Assigning responsibilities for the co-ordination, development, implementation, review and update of the business continuity plans;
- Consider and purchase suitable insurance as part of the process
- Paste-Emergency Contact List Including

Emergency Contact List –Publish Emergency Contact List with phone numbers, emails of relevant persons. The below list shall be displayed at all BRANCH locations, with details of:

- Hospitals
- Fire Stations
- Police Stations
- Bank CEO
- Key Managers(minimum two)of the Bank
- Head IT
- Account Manager-of SIPL
- Any other Vendors

p) Incident Management

Staff should be made aware and informed to note and report any observed or suspected security weakness or threats to procedures, policies, systems or services. They should report these matters to the supervisory authority as quickly as possible.

Incidents which affect bank operations consisting of multiple customers / users / Full Branch, shall be termed as "Major" Incidents.

Some Major Incidents are-

- Probing of Critical Networks
- Attacks on Networks
- Unauthorized Access of IT Systems
- Bank Data Theft/leakage/disclosure
- Identity Theft/Spoofing/Phishing attacks
- Financial Frauds/Attempts

Bank should maintain Incident record and details of Major Incidents, along with problem register.

If a security breach or attack is suspected or any other incident is reported, the Bank Management should be notified immediately. Bank management shall decide, if incident is causing any impact on bank, for suitable reporting to RBI.

In case the incident impacts data or operations related BULK customer of BANK, Bank Management shall decide, if it is appropriate to inform Regulatory authority or customers of such an incident.

In case any major Incident is recorded Report should be submitted for each quarter to RBI. Incident may be of any type above causing a major impact on the bank. In case NO incident is recorded, incident report is not mandatory.

Critical or impact causing Incidents may also be reported to appropriate authorities such as Cert-in (Computer Emergency Response Team, under Ministry of IT and Communications) as per ITAct2000, Digital law of India.

Section2-UserPolicy–Do'sandDon'ts

The policy out lines the acceptable use of computer equipment and CBS Application software in use at the BANK.

All employees and contractors(Vendors working inside bank premises)should read the below sections.

Copy of Policies shall be available with Managers at branches as required.

The rules provide Security Awareness, Do's and Don'ts to be understood and used by employees for their own safe working and banking operations.

Inappropriate use may expose the BANK to risks including virus attacks, compromise of network systems and services, and legal issues.

Acceptable Use

General Use and Ownership

- The BANK network and security administration provides a reasonable level of privacy, users should be aware that the data they create on the BANK systems remains the property of BANK.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use of IT systems while in the BANK.
- BANK recommends that any information that users consider sensitive or vulnerable should be protected. Protection can include access restriction and/or encryption.
- For security and network maintenance purposes, authorized individuals within BANK may monitor equipment, systems and network traffic at any time.
- BANK reserves the right to audit networks and systems on a periodic basis to insure compliance with this policy.

Security and Proprietary Information

- Keep passwords secure and do not share Log in ID of accounts. Authorized users are responsible for the security of their own passwords and accounts.
- When not in use, PCs, laptops and work stations should be secured by locking the machine / screen (ctrl-alt-del).
- In case using Notebooks, take special care to protect data and login ID.
- Users should not make post without approval. In case posting to newsgroups, social media Do not use BANK e-mail account unless BANK has authorized.
- PCs used by the employee are connected to the BANK Internet/LAN /WAN shall have approved virus-scanning software with a current virus database.
- Employees should use CAUTION before opening e-mail attachments or Clicking URL in email messages. Such mails may contain viruses, worms, Trojan horse code, malware and may infect your PC.
- Understand CLEAR reason and type of attachment from the sender, before opening file.

Unacceptable Use

The following activities are, in general, prohibited:

- Under no circumstances is an employee of BANK authorized to engage in any activity that is illegal under local, state, RBI regulations while utilizing IT resources.

System and Network Activities

The following activities are strictly prohibited,with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by BANK.
- Unauthorized copying of material including, but not limited to, digitization and distribution of Reports, copyrighted music, and installing any software for which the BANK does not have a license is strictly prohibited.

- Introduction of malicious programs (virus / Malware) into the network or server (e.g. Viruses, worms, Trojan horses, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes to family and other household members when bank work is being done at home.
- Making fraudulent offers of products, items, or services originating from any BANK account.
- Making public statements or posting on social media about services, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to,
    - Accessing data of which the employee is not an intended recipient or
    - Logging into a server or account
    - Use Port scanning, hacking or security scanning tools is expressly prohibited
    - Circumventing or bypass user Login ID authentication or security of any Server, network or account.
    - Interfering with or denying service to any other user (e.g. Denial of service).
    - Download, use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a BANK operation, via any means, locally or via the Internet/Intranet/Extranet.
    - Providing information about, or lists of, BANK employees to parties outside the company.

EmailandCommunications Activities

- Sending unsolicitede mail messages, including thesending of "junkmail"or other advertising material to individuals (email spam).
- Sending any form of harassment via email, telephone or paging, whether through language
- Unauthorized use, or forging or modifying of email header information.
- Creatingorforwarding"chainletters","Ponzi",Faith,ReligiousorPoliticalor Fake schemes / offers of any type.

- Personal use of network such as internet streaming and download technologies (continuous radio broadcast, You tube or video streaming, torrent, large downloads, etc.)

Section3-BranchCyberSecurityPolicy

Branch managers should Read and Acknowledge the Section 1 - Cyber Security policy ofthebank. Copy of the Cyber Security policy shall be available at all branches.

However certain aspects are important for Information Security to be managed at branches also. At Branches BANK has the deployed the following Infrastructure –

- Computer Terminals/PC for banking operations
- Local Network connectivity for inside the branch
- Internet Connectivity for email, communication systems
- Wifi Network
- CCTV camera(s) for monitoring
- UPS for power backup to systems
- Environmental Controls including
- Dust Free and Humidity free and Clean work areas
- Air-conditioning, Firefighting equipment

Cyber Security Controls applicable at branch level are listed below.

a) User PC/Desktop Notebooks Controls

- Bank Users shall NOT have Administrator RIGHTS on PC. Users shall use be given STANDARD users access
- PC shall be protected by suitable and updated Anti-virus solution.
- Remote access(RDP)from PC shall not be allowed, unless approved
- USB port shall be disabled on PC.
- Access to NEFT /RTGS/ATM and other sensitive PC shall be allowed to authorized personal only.
- In case Internet required on PC, only Authorized List of sites should be allowed through-Trusted Sites (in Browsers).

b) Physical and Environmental Controls

- Servers, Firewall, networking equipment shall be maintained in a secure environment with physical controls at Branches.
- **Physical Security**
    - CCTV systems monitor sensitive and relevant areas of the HO, Branch office premises using night vision cameras on 24x7x365 basis.
    - The recordings are captured using PC or DVR systems with limited capacity. CCTV recordings shall be backed up and moved to external HDD backup media every WEEK. CCTV backup should be available for at least ONE month.
- **Environmental Controls**
    - Proper Cleanliness, Temperature and Humidity controls shall be ensured
    - Air-conditioning systems shall supply suitable temperatures for computer equipment.
    - Network cabling shall be maintained in proper condition
    - Stable Power supply shall be made available using transformers and UPS
    - Backup power shall be supplied by generator systems at all locations, as feasible.
    - Proper and serviced Fire Fighting equipment shall be installed at all branch locations. Recommended Fire Extinguishers are of ABC types.

c) Network Security

- Firewall and routers configuration shall be managed by authorized resources only.
- Ensure Network connections are not Added/Removed without approvals
- Internet Content filters are installed in Firewall devices for allowing restricted access to sites.
- Secure and limited access to Internet services shall be provided at location.

- Allow access to authorized websites only.

- **WiFi Services,if installed**
  - Configure WPA2 Security
  - Setup STRONG password(at least 10 characters)
  - Allow use of on Authorized PC/Notebook only.
  - Do not allow use of Wifi on Personal Devices(Notebook/ Mobile)

d) Anti-virus and Patch Management

TMCBL will install malware and virus protection software at servers, PC/workstations or Notebook connected to bank network.

- Malware protection will also include SPAM protection.
- Authorized standard anti-malware anti-virus software will be installed
- The anti-malware software will be updated automatically or periodically.
- Anti-malware protection will not be disabled during nor malfunctioning of systems.
- Renew Anti Malware/Antivirus support services, ONCE each year.
- Anti-malware mechanisms will be used to detect and eradicate malicious code and/or SPAM (e.g., viruses, worms, Trojan horses, spyware) transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or by exploiting information system vulnerabilities.

e) Incident Management

Bank staff should make a note and report any suspect or misuse related activity regarding Bank / customer data security or any threats to bank procedures, policiesandcomputersystemssystems.Staffshouldreportthemattertotheappropriate authority at Branch and HO as quickly as possible.

Incidents which affect bank where disruption is there in branch operationor customer services, are termed as Incidents.

Branch should maintain Incident record and details of Major Incidents, along with problem register.

Type of Incidents are-

- Attacks on Bank Networks
- Unauthorized Access of IT Systems
- Bank /Customer Data Theft/leakage/disclosure
- Identity Theft/Spoofing/Phishing attacks
- Financial Frauds/Attempts

If any of above issuspectedor reported, the Bank Management at H.O should be notified immediately.

The Mahaveer Co-operative Bank Ltd., Belagavi
Sd/-
Chief Executive Officer/Vice-Chairman/Chairman