‘Cyber Security Policy’

Version 1.3

THE JANATA CO-OPERATIVE BANK LTD.

H.O. 32, Netaji Subhash Marg, Darya Ganj, New Delhi-110 002

Telephones: 23256272-74, **E-mail**: ho-manager@janatabank.in

Document Version History

Version No.	Revision Date	Approved by
1.0	1st January, 2019	Board
1.1	8th August, 2020	Board
1.2	25th June, 2021	Board
1.3	5th September, 2022	

THE JANATA CO-OP. BANK LTD. 32, F.F. N.S. MARG, DARYA GANJ NEW DELHI

Table of Contents

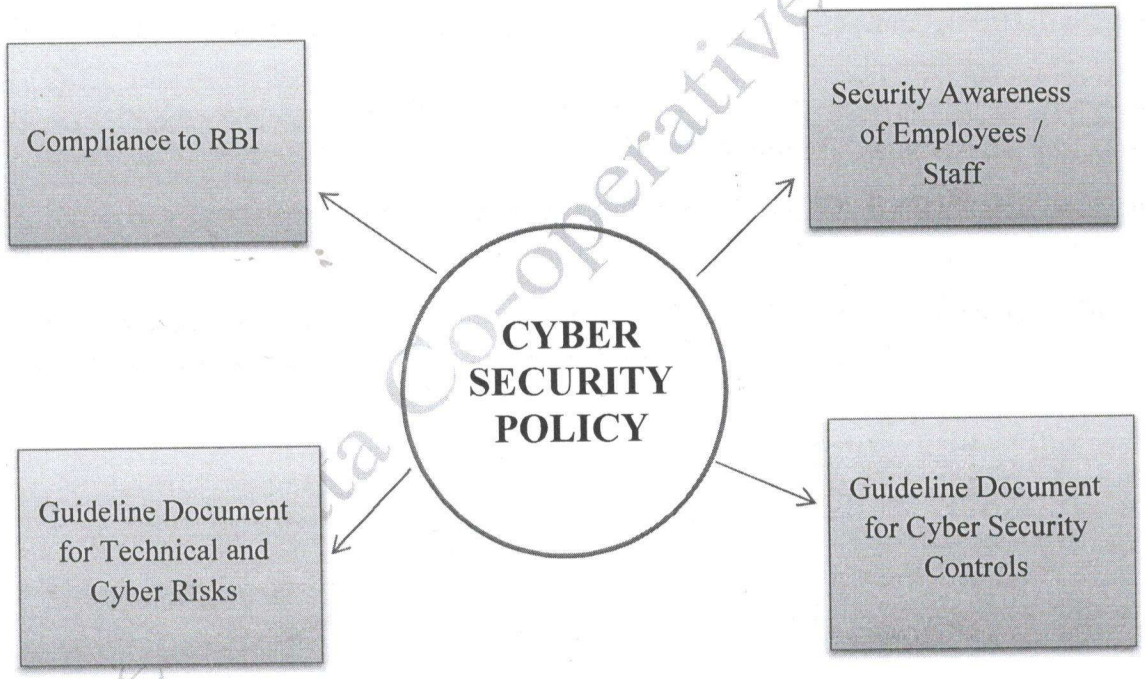
1.1 Purpose

This document provides the framework for the protection of ***The Janata Co-operative Bank Ltd. (JCBL)*** information assets, setup controls for use, access and disclosure of assets from Cyber Threats, attacks in accordance with appropriate standards, digital laws and RBI Guidelines.

The **Cyber Security policy** cover Threats, vulnerabilities to the bank operations and suitable technical, procedural controls to provide assurance that bank operations are secure.

JCBL 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 policy applies to **Head Office, Administrative Office and Branches** of the bank. The Cyber Security Policy serves the below purpose for the bank-



1.2 Cyber Threat Landscape

Bank IT Architecture should be Cyber security compliant. The IT architecture includes network, server, database and application, end user systems, etc., that are installed at Bank Head Office and branches network.

Bank should monitor and ensure security measures are enabled and working at all times. Bank Board or IT Sub-committee of the Board should review controls on periodic basis or at least **ONCE** a year.

For this purpose, JCBL may carry out the following steps:

- Identify weak/vulnerable areas in IT systems and processes,
- Allow restricted access to networks, data bases and applications
- Assess the cost of impact in case of data breaches/failures
- Put in place suitable Cyber Security System to address Cyber threats to bank operations
- Specify and document clearly the responsibility for each of above steps.
- Maintain a proper record of the entire process to enable supervisory reviews

1.3 Understanding Cyber Attack Types 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-Indicative list

- **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 OWASP Top 10

- **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.

- **Ransomware**: 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 programmes now exist that enable intruders to fool an individual into believing that traditional security is protecting him during online banking transactions. Attacks involving malware area factor in online financial crime.

- **Phishing**: Phishing is the fraudulent attempt to obtain sensitive information such as user names, 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 an undesired path on the network thereby 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 back door 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.

1.4 Specific Cyber Security Controls

a) Data Classification and Inventory

Data of JCBL 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 Notifications etc published on websites Approved financial statements Any other deemed suitable by bank

b) Asset Inventory Management

- IT shall maintain documentation related to
  - IT Hardware Servers, PC
  - Software Applications
  - Firewall, switches assets
  - Details of vendor contracts, SLA
  - Software Licensing details
  - Network Diagrams of HO and Locations
  - Important Configuration settings of OS, applications
  - Legacy systems and equipment (OLD server, applications)
- Technical System documentation will be secured, backup taken and physically protected.
- 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 backup of CBS, HDD, CD drives will be stored in fireproof 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

Security controls on user PC –Desktop or Notebooks

- Bank Users shall not have Administrator RIGHTS on PC.
- Users ID shall have STANDARD users access
- Users shall not download or install any software (not required by bank) on PC
- 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.
- Internet Access to Allowed sites only

d) Physical and Environmental Controls

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

- Servers, Firewall, networking equipment shall be maintained in a secure environment with physical controls at HO and Branches.

Physical Security

- Physical security at Entry and Exit shall be maintained
- CCTV systems monitor sensitive and relevant areas of the HO, Branch office premises using night vision cameras on 24 x 7 x 365 basis.
- The recordings are captured using PC or DVR systems.
  - Recording shall be moved to external HDD backup media or Alternate System on a weekly basis.
  - Backup shall be maintained for 30 days on external media
  - In case of locker backup shall be maintained for 7 months

Environmental Controls

- Proper Cleanliness, Temperature and Humidity controls shall be ensured
- Air-conditioning systems shall supply suitable temperatures in Data Centre, computer work areas.
- LAN Network cabling shall be maintained in proper condition
- Stable Power supply with Earthing shall be provided using transformers and UPS
- Backup power shall be supplied by generator systems, 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 / IP Sources only
    - Reset of Default password with STRONG passwords
    - AMC of Firewall / Routers shall be taken by Bank
    - Keep Device and Software up-to-date

Wi-Fi Services

- Wi-Fi Name – Not recognizable as bank Wi-Fi – Eg - Eagle, Dragon
- Configure WPA2 Security
- Setup STRONG password (at least 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 white list – Allow access to required sites only.
- Redundant (secondary) links preferably from alternate ISP are established in case of failure of primary links.
- Setup mechanisms and tools for detection for problem, error and changes tracking
- Enable Logs, 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.
- In case speed issues are observed review capacity and quality of service of ISP.
- 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) Vulnerability Assessment and Penetration Testing - VAPT

Firewall Devices and Servers (if, installed)

- In-House Servers and Firewall - VAPT Vulnerability Assessment and Penetration Testing shall be completed **Once a Year** for such servers / Firewall and devices deployed by bank in the Data Centre or cloud hosting locations.
- Public Facing Firewall - VAPT shall be conducted ONCE a Year from external locations using Public IP.

g) Data Leakage Prevention

Confidential Data of bank, customers record shall be protected against unwanted Data leakage attempts and thefts. The bank follows the following strategies-

- USB on PC shall be blocked

- ☐ Antivirus, Anti malware protection shall be enabled
- ☐ Admin Access on PC shall not be allowed
- ☐ Monitor outgoing email and attachments of Bank users IDs
- ☐ Restricted Internet access is allowed to select users only as required for banking operations
- ☐ CBS computers should not allow Internet Access
- ☐ One Drive, Google Drive, Drop box, Cloud Share folders shall not be allowed
- ☐ Email Access should be allowed from bank premises only

h) Audit Logs

- ☐ Logs shall be enabled on Server, Firewall and other devices (If installed at bank)
- ☐ Configure Audit logs to send Alert to bank IT Teams
- ☐ Transaction logs shall be available in CBS applications
- ☐ Review logs on Periodic basis

Configuration of sensitive devices such as Firewall, Routers, Servers etc shall be maintained as per below standards:

- Servers (If, available at bank) shall be hardened-
  - 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 30 days
  - Check and update firmware once in 3 months

i) Anti-virus Anti Malware

JCBL will install malware, spam protection mechanisms at critical information system entry and exit points (e.g., mail servers, web servers and at workstation PCs, servers, or mobile computing devices on the network).

- Authorized standard anti-malware anti-virus software will be installed on all servers, laptops and desktops.
- The anti-malwares 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, 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.
- Protection software shall enable below features (If available)-
    - Anti Loggers
    - Privacy Protection
    - Data Leakage Prevention
    - Ransom ware Protection

j) User Access Control / Management

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

- Access to user shall be allowed for specific work / roles- E.g.: Supervisor, Clerical, Manager, Other type of Users.
- Users shall be created after approval of respective Managers.
- Access to File / Folders (in case of share folder) 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 be enabled, if desired)
- User access shall be removed, when user leaves / resigns from bank services
- User creation, exit records shall be maintained

k) 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 (e.g. ab.coopbank.com/in)
- Open and Free 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 usersonly.
- Email access should be allowed from within bank office premises.
- Install Outlook or Thunderbird etc for email access in bank
- Web Access to email may be provided to authorized users only.
- Creation / Management of email account, shall be done by approval of management only.
- DMARC settings, spam filters shall be enabled

Data Exchange

- Exchange of data shall be with authorized and approved links only (Eg HDFC, host bank NPCI etc).
- Exchange of data shall be done through VPN, SSL, SFTP, emails and secure links only.
- Exchange of data shall pass through in Firewall devices installed at location.

l) Removable Media

- Only authorized users / access may be allowed for removable media in case used for backup and official purposes (External HDD/Tapes etc).
- Authorized 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, CDs and / or degaussing.

m) Security Awareness - Users / Employees

Staff at JCBL 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.
- Security Awareness Orientation Sessions will also be conducted for long-term contractors also, who will access JCBL 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 acknowledgement of attendance and understanding of the security awareness sessions.
- Training records shall be maintained by Bank.

n) Customer Education and Awareness

JCBL shall provide training to customer regarding Cyber risks, use of safe banking, online e-commerce, other areas through regular programs. Awareness should cover Internet Banking, 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 over all banking experience to become safe for the customers of the banks.

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

o) Backup and Restoration

JCBL 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 areas per below-

Responsibility	What to Backup
CBS Vendor	CBS Data, Signatures, related transactions data

Bank The frequency of backup and retention period of the backup data will be determined and approved by the management.	Weekly or Periodic backup on external HDD or Alternate Systems - Files, Folders, Notebook - CCTV - Emails

p) 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 approved on an annual basis.
- Service records, service short coming are recorded and maintained by IT / Other teams as applicable.

q) Business Continuity (Crisis Management)

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 and Secondary link for CBS
- Ability to operate CBS from Alternate Branches, if required

CBS Vendor SIPL shall provide Business Continuity Services of the Primary Data Centre and DR sites.

However, bank management should address the following at branches-

- Power Failure
- Fire Situations
- Water Flooding during rains / as per location
- Hardware and Network Failure(s)
- Availability of Bank Operations and IT Staff

Bank should –

- 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 general or Cyber insurance as part of the process

Emergency Contact List – Banks shall Publish Emergency Contact List with phone numbers, emails of relevant persons. The list shall be displayed at 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

r) Change Management

- Infrastructure Servers, Firewall or Network changes
  - Changes shall be done based on requests from bank management or Staff post approval.
  - IT Team with help of vendor shall get the changes done.
  - Where feasible, before deployment testing shall be done to ensure smooth working of bank operations.
  - Keep OS up-to-date on Servers, PC on periodic basis
- CBS or Software Changes
  - Bank Team shall inform bank IT for any issues or changes in CBS software.
  - The problems shall be reported to CBS vendor for change.
  - Track completion of changes by vendor
  - Test changes on UAT site provided by CBS vendor before approving change for deployment
- Keep Record or register or emails of ALL change requests

s) Incident Management

Staff should be made aware and informed to note and report any observed or suspectedor unusual activity or security weakness or threats to procedures, policies, systems orservices. They should report these matters to the supervisory authority as quickly aspossible.

Any adverse or unusual Incidents which affect bank operations services to multiple customers / users / Full Branch, shall be termed as Incidents. These incidents cause service disruption of more than 3-4 hours.

Type of Major Incidents are-

- Malware / Ransom ware Attacks

- ☐ Probing or hacking attack on Network
- ☐ Unauthorized Access of IT Systems
- ☐ Bank Data Loss / Theft / leakage / disclosure
- ☐ Identity Theft / Spoofing / Phishing attacks
- ☐ Financial Frauds / Attempts

Bank shall maintain Incident record and details of Major Incidents, along with problem register and use Incident Templates.

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, which is suitable for 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.

Submit Incident Report to RBI every quarter, only in case incident is reported. Incident may be any of above types causing a visible impact on the bank.

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 IT Act 2000, Digital law of India.

For The Janata Co-operative Bank Ltd.

(P.S. Pathania)
Managing Director

End of Document

THE JANATA CO-OP. BANK LTD. 32, F.F. N.S. MARG DARYAGANJ NEW DELHI