Cyber Security Policy

"The Bhiwni Central Co-Operative Bank Limited"

(Bhiwni)

Version: 1

Date:

Approved By: Board of Directors

DOCUMENT VERSION CONTROL

DATE	W.E. F	VERSION	PREPARED BY	REVIEWED BY	APPROVED BY	RELEASE DATE
		1				

Document Definition: This document is designed to assist the Bank against Cyber Threats & Frauds. The policy gives a comprehensive overview on the various sets of measures, activities, tools and techniques ensuring protection of Bank's cyber space and IT infrastructure against various Cyber Threats. The policy is designed in accordance to:

- NABARD Circular No. 50/DoS-16/2018 dated 16th March, 2018
- NABARD Circular No. 32/DoS-07/2020 dated 06th February, 2020
- Industry's Best Practices.

Contents

CHAPTER 1

1. General Matters

1.1 INTRODUCTION

Information Technology has become an integral part of Business Operating Systems in the present day scenario. With use of extensive Information Technology by banks, the cyber risk associated with bank has also increased. The number, frequency and impact of Cyber Incident attack have increased manifolds. Cyber incidence risks may directly leads to the reputational and financial loss which may have the ability to affect the bank's bottom line. It can be costly, compromising to customer confidence and in some cases, the bank could be held legally responsible. Beyond the impact to the bank, cyber risks have far-reaching economic consequences.

The Cyber Security Policy deals with Set of measures, activities, tools and techniques ensuring protection of Bank's cyberspace against cyber threats and cyberspace vulnerabilities. It means that in Cyber Security, we are dealing only with threats via cyberspace.

Bank has a comprehensive **Information Technology & Information Security Policies,** Board approved date 24.03.2014 vide version no. 1 (which forms the base for Cyber Security and Resilience Framework Policy). All Information assets of "The Bhiwni Central Co-operative Bank Limited" will be governed under Information Security Policy and Cyber Security Policy draws its references from the Information Security Policy.

1.2 OBJECTIVE

The objective of —"Cyber Security Policy" is to provide guidance and direction to combat cyber threats given the level of complexity of business and acceptable levels of risk, specific to "The Bhiwni Central Co-operative Bank Limited".

National Bank for Agriculture and Rural Development (NABARD) has provided guidelines to all the SCBs/DCCBs to develop a Cyber Security Policy & Cyber Resilience Framework. The same is

required to be developed considering established standards for IT Security such as ISO 27001, ISO 27002 and COBIT. The Cyber Security Policy and Cyber Security Resilience Framework of "The Bhiwni Central Co-operative Bank Limited" has considered the required standards while framing this policy.

The specific objectives of the Cyber Security Policy are outlined as 5 domains as under:

1. **Identify** internal and external cyber security risks.

2. **Protect** banks systems, assets, and data from identified cyber risks.

3. **Detect** system intrusions, data breaches and unauthorized access.

4. **Respond** to a potential cyber security event.

5. **Recover** from a cyber-security event by restoring normal operations and services.

1.3 SCOPE

The Cyber Security Policy is to be complied by following persons/entity:

1. The policy contained herein shall apply to any person who has access or accesses to bank's information or uses any of the bank's Information resources / assets.

2. The policy shall be applicable to employees, customers, vendors, contractors, sub-contractors, external parties and any other third-party hosting services or wherein data is held outside the bank.

1.4 COVERAGE

1. The Information Systems covered under the Cyber Security Policy include all the assets like people, process, data and information, software, hardware, and communication networks etc., operated by the bank, whether used locally or regionally.

2. This asset may be owned by the bank, leased, hired, developed in-house or purchased.
3. It includes services that are contracted or outsourced to other parties but operated for the bank.

1.5 AUTHORITY

The Cyber Security Policy is issued under the authority of The Board of Directors. The Board of Director is the owner of this policy and ultimate responsible for Information Security in the Bank. The Cyber Security Policy document is strictly for internal circulation among the employees of the "The Bhiwni Central Co-operative Bank Limited" only.

1.6 DEVIATION, VIOLATION, MISCONDUCT

Cyber Security Policy shall be adhered to and any deviation shall be dealt with appropriately. Deviation, violation and misconduct with respect to Cyber Security Policy will be dealt as per Penalty for Security Violation (Chapter no. 7) of Cyber Security Policy.

1.7 REVIEW OF THE CYBER SECURITY POLICY

As Cyber security landscape is undergoing rapid changes at a faster pace, this Cyber Security Policy is intended to be a baseline document.

The policy will be reviewed at yearly intervals to make suitable changes/amendments considering the technological changes or may be reviewed when there is a change in the technology implementation.

1.8 MANAGEMENT DIRECTION FOR CYBER SECURITY

The Board and the Management actively supports Cyber Security functions within the bank through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of Cyber Security responsibilities.

Management is committed to:

- Ensure that Cyber Security goals are in tune with business goals, are identified and meet the bank's requirements, and are integrated in relevant processes.
- Formulate, Implement, Monitor, Review and Approve Cyber Security policy
- Review the effectiveness & implementation of the Cyber Security policy
- Support the Cyber Security initiatives
- Provide the resources and investment needed for Cyber Security
- Initiate plans and programs to maintain Cyber Security Awareness
- Approve assignments of specific roles and responsibilities for Cyber Security across the bank.
- Mitigation of risks and reduction of potential impacts on information resources to the acceptable level

1.9 CYBER SECURITY AWARENESS

All the stakeholders i.e., BOD/ Senior Level Management/ Departments/ Employees/ Customers/ Vendors/ Contractors/ Sub-contractors shall be informed of the importance of Cyber Security through Cyber Security Awareness Education Program/ Seminar/ Workshop/ Email & SMS Alert / Pamphlets / Banners / Letters etc. to create an environment of sound cyber security practices within the bank.

1.10 SECURITY ORGANISATION

The bank shall appoint / designate Chief Information Security Officer (CISO). CISO's role will be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and NABARD controls, and direct the establishment and implementation of processes

and procedures as per the cyber security and resilience policy approved by the Board of the Directors.

He will be coordinator between Bank and Cyber Security and Information Technology Examination (CSITE) cell, NABARD which will help the banks in obtaining collective threat intelligence, timely alerts and adopting proactive cyber security measures

The bank shall constitute an IT Sub Committee of the Board comprising members proficient in technology and governance. This IT Sub Committee shall on a regular basis without gap of more than three months to review the implementation of the cyber security policy approved by the Board, and such review shall include review of their current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience. The review may be placed before the Board of Director for appropriate action.

CHAPTER 2

DETECTION OF SYSTEM INTRUSIONS, DATA BREACHES, AND UNAUTHORIZED ACCESS IN BANK's IT INFRASTRUCTURE.

2.1 Monitoring Deviations from Normal Operations

To mitigate threats proactively bank shall, use controls and sensors that automatically work to prevent or limit unauthorized access to computer networks, systems, or information.

Bank shall ensure proper inventory of information assets and additionally, monitor networks, systems, and applications to establish a baseline traffic pattern or establish a measure for —normal operations.

CHAPTER 3

PROTECTION OF BANK SYSTEMS, ASSETS AND DATA FROM IDENTIFIED CYBER RISKS.

3.1 CYBER SECURITY CONTROLS

Broadly Cyber Security Controls can be of technical (detective, preventive and corrective) and administrative in nature. The Critical Security Controls for cyber defence are a baseline of high-priority information security measures and controls that can be applied across the bank in order to improve its cyber defence.

The bank has self-assessed its controls and as per Comprehensive Cyber Security Circular dated 06th February, 2021, bank is falling under Level 2 category.

Cyber security controls that shall be put in place to protect from cyber security threats covering different types mentioned above are:

3.1.1 Inventory of IT Assets

Actively manage (inventory, track, and correct) all IT Assets i.e., hardware, software, key personnel, network devices, documents etc. in the bank infrastructure so that only authorized IT Assets are given access, and unauthorized IT Assets and unmanaged devices are found and prevented from gaining access.

Assets of Bank which are managed by Third Party Vendor (ASP) should also form part of Inventory Register. All the assets will be classified based on criticality of assets i.e., Critical/High/Moderate/Low.

Classification of Information Assets

All information assets should be classified based on a defined category of sensitivity. The classification of assets should be conducted periodically as asset classification may change based on Business needs.

Example:

Classifications could include such categories as:

- Confidential—having a severe impact to the institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized;
- Internal Use Only—having minimal to limited impact to the institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized;
- Restricted—having limited impact to the institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized; and
- Public Information—having minimal to no impact to the institution, its critical functions, business partners, or customers if lost, damaged, or if disclosure is unauthorized.

3.1.2 Secure Configurations for Hardware and Software on and Servers, Network / security devices, Mobile Devices, Laptops, handheld devices, Workstations etc.

Establish, implement and actively manage (track, reporting, correct) the security configuration of network infrastructure, laptops, servers and workstations including Third Party Data Centre using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Manage (track/control/correct) the ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability available to attackers.

The processes and tools used to track/control/prevent/correct the use, assignment and configuration of administrative privileges on computers, networks and applications.

3.1.3 Continuous Vulnerability Assessment and Penetration Testing

Continuously acquire, assess and take action on new information in order to identify vulnerabilities and perform penetration testing to identify the window of opportunity for attackers.

a. All critical systems should be subject to a VAPT audit at least twice in a year in order to assess the current IT Security posture from External Agencies
b. Scope of audit should at a minimum include the following: -
    - Network Penetration Testing
    - Secure Mail and Messaging System
    - Website Security Audit
    - Critical Application Hosted on Public Domain
    - Secure Endpoints Audit and Server installed at Bank Premises
c. As bank is on ASP model; Bank has to ensure to obtain CBS Application VAPT certificate and Server & Network Infrastructure VAPT certificate periodically from the ASP Vendor.

3.1.4 Remediation of Vulnerabilities

CISO of the bank shall on urgent basis take necessary remedial steps to mitigate critical and high findings of VAPT report. Also, a periodicity for mitigating VAPT findings of Medium and Low level to be decided and adhered with. Status report to be discussed with IT sub committee on quarterly basis.

3.1.5 Patch Management

Bank should periodical patch following IT Infrastructure:

a. Networking Devices i.e. Firewall, Routers, Switches
b. End Points
c. Applications
d. Server, if hosted in Bank premises

Bank should put in place systems and processes to identify, track, manage and monitor the status of patches of above mentioned devices

3.1.6 Change Management

Any changes in the critical IT Assets i.e. Firewall, Routers, Switches, Applications, Server, if any, critical systems should be approved through CISO before implementation on live environment.

The changes may include configuration changes, technology changes, business processes changes etc

3.1.7 Application Software Security

Manage the security lifecycle of all in house developed and acquired software in order to prevent, detect and correct security weaknesses if bank intends to develop in future.

3.1.8 Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS) i.e., Dongal, Wi-Fi, Hotspot etc, access points and wireless client systems.

3.1.9 Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage and analyses audit logs of events that could help detect, understand or recover from an attack.

Bank shall ensure that audit logs of Networking Devices, Servers, Critical End Points, Mail & Messaging system are generated and analysed by CISO and his team on fortnightly basis whether hosted in-house/Third party location. The logs should be retained for at least last six months for proper analysis and in requirement of forensics.

3.1.10 User Access Control

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which

persons, computers and applications have a need and right to access these critical assets based on an approved classification.

3.1.11 Account Monitoring and Control

Actively manage the lifecycle of system and application accounts, their creation, use, dormancy, deletion in order to minimize opportunities for attackers to leverage them.

3.1.12 Data Loss/Leakage Prevention

The bank shall have arrangement for ensuring safety of business and customer personal identifiable information through implementation of comprehensive data and leakage solution. Bank shall have the arrangement of adding such clause in the Service Level Agreement (SLA) with the ASP vendor and also appropriate end point DLP solution in place.

3.1.13 Environmental Controls

Bank shall ensure appropriate environmental controls for securing location of critical assets providing protection from natural and man-made threats. Mechanisms for monitoring of breaches / compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the bank.

3.1.14 Cyber Security Insurance Policy

As part of risk mitigation and protection against claims, the organisation shall purchase cyber Security Insurance Policy either directly or be part of the group policy coverage.

3.1.15 Vendor Risk Management

Bank shall appropriately conduct due-diligence of Third Party Vendor/ Service Provider and Partners.

The bank shall ensure to have a proper Service Level Agreement (SLA)/ Non-Disclosure Agreement (NDA)/ Background checks for all third party vendors.

Bank / Regulatory shall have access to all the information from ASP Vendor and also Right of Audit by the Bank and Inspection by the Regulator (NABARD, RBI) of the country.

Irrespective of Bank's infrastructure, whether In-house or outsourced, the final responsibility would be that of Bank.

3.1.16 Secure Mail and Messaging

The bank shall implement set of activities, tools and techniques to ensure that bank and also his vendors take appropriate measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

3.1.17 Authentication Framework for Customers

The bank shall have arrangement for ensuring safety of business and customer personal identifiable information stored at Bank premises or at ASP Vendor Database. Bank shall also have arrangements for alert/notification in case of data breach at ASP vendor location.

ASP Vendor shall not share customer information with Third Party vendor for processing or any other purpose without written authorization with Data owner (Bank)

Bank shall ensure that customer information shall be deleted from Vendor's system completely once the bank ends business relationship with customer.

Bank shall maintain proper login authentication for Mobile Banking, ATM i.e. Password Based Authentication and One Time Password (OTP).

In case of any fraud identified, a Fraud Management Mechanism should be in place.

3.1.18 Advanced Real Time Threat Defence and Management

The bank shall ensure that it has measures to prevent and detect execution of signature less Advanced Persistent Threat. Bank is under ASP model and the same shall be implemented at CBS vendor level.

3.1.19 Removable Media

The bank shall ensure for restricted use of Removable Media.

The restricted use of removable media will be allowed only after proper authorization.

The removable media shall be scanned for detection of malware/ virus prior gaining to access.

Centralized logs to be maintained and reviewed by CISO on periodic basis.

3.1.20 Anti Phishing

The bank shall configure Sender Policy Framework (SPF), DKIM, DMARC for preventing spoofing of bank email. Awareness training shall be given to bank employees for such anti phishing campaign to be executed by bank.

3.1.21 Risk Based Transaction Monitoring

Bank shall put in place with the help of ASP Vendor to detect and prevent fraudulent transaction for all delivery channels. The monitoring system should notify customer through SMS on registered mobile number for exceptional transaction i.e. High value, different location etc.

3.1.22 Cyber Security Operations Centre (C-SOC)

Bank shall ensure that ASP vendor formulate Security Operations Centre (SOC) and generate and submit reports/logs on periodical basis to CISO for his review and necessary action for critical devices i.e. Server/ Networking Devices being managed by ASP.

Notification/alerts shall be provided on real time basis to CISO, in case of any critical errors with the Bank Infrastructure identified.

Bank shall also have arrangement for implementing Security Incident and Event Management (SIEM) solution for critical devices i.e. Server, if any, Networking Device and Critical End Points.

3.1.23 Forensics

Bank shall have arrangement for conducting Forensics, in case of any Cyber incidence. Also, bank can demand for logs of critical devices from ASP Vendors for details required by forensic experts.

3.1.24 Continual Improvement

Bank shall ensure continuous testing and validating of the effectiveness of current security measures, and to help drive the priority with a forward looking approach.

Bank shall automate cyber security defenses so that it can achieve reliable, scalable, and continuous measurements of its adherence to the Controls and related metrics.

CHAPTER 4

RECOVER FROM A CYBER SECURITY EVENT BY RESTORING NORMAL OPERATIONS AND SERVICES.

4.1 Recovery from a Cyber Security Incident

Bank shall Develop and implement a recovery plan that includes appropriate processes and procedures for restoration of systems and data in case of occurrence of a cyber-security incident.

Broadly, the following steps are involved in recovery from a cyber-security incident. (This may differ from case to case depending on the type of asset affected /impact in the bank's operations.)

1. Recover Infrastructure: A step-by-step plan for rebuilding servers, databases, network devices that may have been compromised, and restoring baseline configurations.
2. Restore Data: If the integrity of data was impacted or content deleted, have a plan in place for restoring it.
3. Reconnect Service: Bank's recovery plan should lay out how bank will reconnect services with minimum disruption.

4.2 Review of Incident response plan execution

Once impaired systems are restored and back online, the CISO should:

1. Determine what cyber security management improvements are necessary to prevent similar attacks from occurring;
2. Review the CISO's execution of the incident response plan; and
3. Consider whether the incident response plan can be improved;

4.3 Testing of Incident Response Plan

Bank shall review the incident response plan periodically and as and when any changes occur in threat landscape to understand the effectiveness and scope for improvement.

Bank may test the plan periodically for better execution and to identify gaps.

CHAPTER 5

PENALTY FOR SECURITY VIOLATIONS

Employees' who use the technology and information resources of Bank must be aware that they can be penalized if they violate this policy. Upon violation of this policy, an employee of Bank may be subject to disciplinary action. The specific discipline imposed will be determined by a case-on-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and laws and all other relevant information.

In a case where the accused person is not an employee of Bank the matter shall be submitted to Bank IT Sub Committee. The IT Sub Committee may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

BIBLIOGRAPHY

Cyberspace- The virtual space created by interconnected **computers** and **computer** networks on the Internet

Cyber-attack – An attack, via cyberspace, targeting an enterprise's use of cyber space for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber security – The ability to protect or defend the use of cyberspace from cyber-attacks.

Sabotage: Is defined as deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or information.

Risk – The potential for loss, damage, or destruction of an asset as a result of a threat exploiting vulnerability.

Threat – Any circumstance or event with the potential to adversely impact bankal operations

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Data ex-filtration- Is the unauthorized transfer of sensitive information from a target's network to a location which a threat actor controls

Vulnerability Scanner-Is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

Risk treatment Process-Is a process that involves developing a range of options for mitigating the risk, assessing those options and then preparing and implementing action plans

Firewalls- A computer firewall is a hardware/software limits the data that can pass through it and protects a networked server or client machine from damage by unauthorized users.

Routers - This is a hardware device that routes data (hence the name) from one network (e.g.: LAN) to another network.

Switches- A switch is used to network multiple computers together

Annexure – Cyber security Threats

Some of the major cyber security attacks targeting financial institutions are explained below:

Distributed Denial of Service (DDoS) attacks

DDoS is a type of attack that attempts to make an online service unavailable by overwhelming a website with excessive traffic from multiple sources that interrupts normal services. In the latter half of 2012, an increased number of DDoS attacks were launched against financial institutions by politically motivated groups. These DDoS attacks have increased in sophistication and intensity. They have caused slow website response times, intermittently prevented customers from accessing institutions' public websites, and adversely affected back-office operations.

Website defacement

Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. Defacement is generally meant as a kind of electronic graffiti and, as other forms of vandalism, is also used to spread messages by politically motivated "cyber protesters" or hacktivists. The most common method of defacement is using a SQL injection which allows gaining administrative access. Another method of defacement is through FTP once the username and password are obtained.

Hacking

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in computer hacking activities are typically referred to as —hackers. Hacking may involve siphoning off money or simple unauthorized access to systems.

Ransomware attacks

Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. The crypto virology form of the attack has ransomware systematically encrypt files on the system's hard drive, which becomes difficult or impossible to decrypt without paying the ransom for the decryption key. Other attacks may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan, whose payload is disguised as a seemingly legitimate file.

Malware attacks

Malware attacks are done using malicious software that are specifically designed to gain access or damage a computer without the knowledge of the owner. There are various types of malware including spyware, keyloggers, Trojan horses, viruses, worms, or any type of malicious code that infiltrates a computer.

Phishing, Vishing and Smishing

These are social engineering attacks to lure customers to disclose their sensitive credentials for fraudulent purposes. Phishing normally involves creating fake websites or forms and sending the links of such websites and forms in emails. Vishing is done through phone calls to the customer and Smishing is though sending SMS. These attacks are outside of the Bank's cyberspace.

Spear phishing attacks

Spear phishing is an email or electronic communications scam targeted towards a specific individual, bank or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.

Skimming

The act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe, is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder.

Spamming

Email spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. This may contain malwares also to do further damages through the recipient's PC.

****