JHALAWAR KENDRIYA SAHKARI BANK LTD.,
JHALRAPATAN

CYBER Security Policy Framework

Table of contents

Revision History

Sr no	Summary of change	Written by	Approved by	Administrator/ Chairman Approved Date	Effective date
1	Original policy Ver.1	Independent Consultant	Administrator/ Chairman		

Cyber Security policy framework

1.Introduction:

Information is an asset to all the Banks and Information security refers to the protection of these assets to achieve organizational goals. The purpose of IS policies is to control access to sensitive information, ensuring sue only by legitimate users so that the data cannot be read or compromised without proper authorization. This is policy for the cyber security framework is prepared for Jhalawar Kendriya Sahkari Bank Ltd., Jhalrapatan as per the directions of Nabard (NB.DOS.HO.Plo.NO./4813 /J-1/2017-18 dated 16th March 2018./RBI/2018-19/63DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 October 19, 2018

As per the directions the Cyber security policy should be distinct and separate from the IT policy/ IS security policy of the bank so that it can highlight the risks from cyber threats and the measures to address /mitigate these risks. This policy is prepared on the basis of the above circular and coves all the point mentioned their in. Additionally, the bank is also having separate IT/IS policies in detail.

2. Responsibilities

a) A cyber crisis Management team should be formed which should consider the requirements of cyber security plan/ policy and introduce the required controls as and when necessary.

B) The responsibility for the implementation depends upon the IT policy implementation team.

3. Introduction of cyber security: Points to be noted.

a) The approach is to follow the cyber crisis management plan (CCMP) which is included in the cyber security policy and disseminate them to micro level so that all the staff is aware of the precaution to be taken to avoid cyber threats.

a) Vulnerability can be defined as an inherent flaw while developing a software internally. Vulnerability assessment is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk and the cost involved and may devise strategy for managing or eliminating the same.

b) Cyber security preparedness is finding out the adequacy and adherence of the solution developed. These should be checked while doing the User acceptance test (UAT) and independent compliance check and audits. Documentary evidence may be kept for future use.

c) IT strategic committee will address the following 4 aspects once the incident is come to the notice:

i) ***Detection*** of the incident (preventive action)

ii) ***Response*** to the incident (corrective action)

iii) ***Recovery*** of the data.

iv) ***Containment*** of subsequent happening.

d) **Sharing of information on cyber-security incidents**: The Bank is required to pass on the information on cyber security incidents whether it is successful or were attempts which did not fructify to the CSITE cell of NABARD.

e) **Technology scenario at Jhalawar Kendriya Sahkari Bank Ltd., Jhalrapatan**

- In coordination with RSCB Apex bank, Jhalawar Kendriya Sahkari Bank Ltd., Jhalrapatan has adopted Licensed model for implementation of their CBS operations through TCS. There is a separate server room in the data centre(DC) and DR is located at Jodhpur. The day to day activities are handled by RSCB in coordination with NICSI New Delhi. Service level agreement entered between RSCB and TCS is expiring on 14.2.2021. There are outsourced staff who is stationed to handle some of the functions. The responsibility for the design and implementation of the information systems and the related controls including adequate disclosures is that of the NICSI/TCS as per the SLA entered and the management is responsible for correcting/ controlling lapses, if any.

  The ATM /payment solutions are on outsourced model through Cash link Global and FIS with DC/DR wot respective vendors through separate agreements.

Baseline cyber security controls

1. **Inventory Management of business assets:**

   Necessary inventory register should be maintained to take care of all the assets including the business data/hardware/software /network devices,

key personnel, services etc. Incase these assets are hosted at an outsourced location, /the details of the asset owned by the bank should be obtained and kept on record.

1.2 Classification of data and information based on the classification criteria fixed by the bank.

1.3 Bank should manage and provide protection for the data /information stored, transmitted, processed, accessed and put to use within and outside the banks.

2. Use of unauthorized software:

2.1 Bank to maintain proper inventory in centralized manner for all the software authorized /un-authorized software.

2.2 Control should be exercised for all the software/applications on end user PC's, Laptops, work stations, servers, mobile devices etc and proper mechanism

2.3 Patches for the software solutions should be done as per the patch management policy of the bank. Any new patches supplied by the vendor should be authorized by the concerned personnel through a patch management process.

2.4 Any exceptions should be properly recorded and kept on record and should be reviewed on a specific interval.

3. Environment control:

3.1 Proper safeguards is to be ensured for protecting the assets from natural and man- made threats.

3.2 Appropriate physical security measures should be taken to protect the critical assets of the bank. (eg; temperature, water, smoke, access alarm, power outage, telecommunications networks etc.)

4.Network management and security

4. Up to date network architecture diagram should be available.

4.2 Maintain up to date details in register about the authorized devices connected to the banks network/ outside banks network.

4.3 Network devices are to be configured properly and appropriate controls should be established on LAN and wireless networks.

4.4 Identify and provide connectivity only to authorized hardware (eg. Laptop, mobile phones etc) which meet the security requirements prescribed by the bank.

5. Secure configurations

5.1 Provide baseline security configurations to all devices (work stations, mobile devices, operating systems, data bases, applications and network end points etc and review periodically.

5.2 Periodically evaluate the critical devices like firewall, network switches, etc including the Data center and third party hosted sites.

6. Application security Live cycle (ASLC)

6.1 in respect to critical applications bank may consider conducting source code audit by a competent authority or from the service providers that the application us free from embedded malicious/ fraudulent codes.

6.2The test and production environments are to be clearly segregated.

6.3 Security requirements relating to system access control, authentication, authorization, data integrity, audit trails, session management etc. are to be clearly specified at the initial and ongoing stage.

6.4 Software /application development approach should be based on secure coding principle and threat modelling

6.5 Bank should consider implementing measures such as installing a containerized apps on mobile, smart phone for executive business use that is encrypted and separated from other smartphone data /applications.

7. Patch /vulnerability & change management

7.1 Strict patch and vulnerability management should be ensured for all the IT components that need to be pathed.

7.2 Bank to put in place system and process to identify, track, manage, monitor, the status of patches to operating system and applications.

7.3 Conduct the VA/PT for internet facing web/mobile applications, servers& network components throughout the Life cycle.

7.4 Periodically evaluate the access device configuration, patch levels to ensure all access points, nodes between (i) different VLANs in the DC (ii) LAN/WAN interfaces, (iii) Banks network to external network connections with partners, vendors, service providers etc.

8. User Access control/Management

8.1 Bank to provide secure access to banks assets /services from within and outside banks network by protecting data /information through use of encryption if supported by the device.

8.2. Administrative rights to be discontinued at the work stations /PCs/ Laptops and provide access rights on need to know access.

8.3 Implement centralized systems and controls to allow, manage, log and Monitor, privileged super user / administrative access to critical systems.

8.4 Bank to implement strong password policy, two factor /multi factors authentications depending upon the risk assessment.

8.5. Implement controls to minimize invalid logons, deactivate the dormant Accounts.

8.6 Monitor any abnormal changes in pattern of logons.

8.7 Implement controls on installation of software on PCs/laptops and control for remote management /wiping/locking of mobile devices including
laptops.

9.Authenticaiton framework for customers

9.1Authentication framework/mechanism to provide positive identify verification of bank customers.

9.2. Customer data to be kept secure. Bank to use secure authentication technologies.

10. Secure mail and messaging systems

10.1 Bank to implement secure mail and messaging system including those used by bank's partners and vendors, and include measures to prevent e mail spoofing, identical mails domains, protection of attachments, malicious mails etc.

11. Vendor risk management

11.1 Bank is accountable for ensuring appropriate assurance on security risks in outsourced a partner engagement.

11.2 Bank to evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment.

11.3 Due diligence on the third parties to be undertaken by the banks

11.4 Bank to ensure that the service providers including another bank adheres to all regulatory and legal requirements of the country.

11.5 Bank to provide access to RBI/NABARD to all information resources 9 online/in person) when sought.

11.6 Bank shall thoroughly satisfy about the credentials of vendor/third party accessing and managing the banks critical assets.

11.7 Necessary background checks, non- disclosure and security policy compliance agreements to be mandated to all third-party service providers

12.Removable media

12.1 Bank to prepare a policy for restrictions and secure use of removable media/BYOD and various type /categories of devices including not limited to work stations PCs/laptops/Mobile devices /servers etc and ensure erasure of data on such media.

12.2. Removable media should be scanned for malware/anti-virus prior to providing read/write access.

12.3 Restrict removable media use through centralized policies through active directory or end point management system to whitelist /backlist etc.

12.4 Use of removable media should not permit unless specifically authorized.

13. Advanced Real-time Threat defense and management

13.1 Bank to build a robust defense against the installation, spread, and execution of malicious code at multiple points.

13.2 Bank to implement anti-malware, anti-virus, protection including behavioral detection systems for all categories of devices / end points like PCs/Laptops /mobile devices etc.

14.Anti-phising

14.1 Bank to subscribe to anti phishing /anti rouge app services form external service providers for identifying and taking down phishing websites /rouge applications

15.Data leak prevention strategy

15.1 To safeguard sensitive business and customer data and information bank to develop a comprehensive data loss/leakage prevention strategy. This includes protecting the data in transmission, as well as data stored in server and other digital devices. this includes vendor management facility as well.

16.Maintenance, Monitoring, and analysis of Audit logs

16.1 Manage and analyze the audit logs in a systematic manner to detect, understand and recover from an attack.

16.2 The storage of logs collection is to be decided by all the stake holders.

16.3 Audit logs pertaining to user actions in a system should be captured

17.Audit logs settings

17.1 validate and capture the appropriate logs /audit trails of each system software and application software and ensure the logs contains minimum information to identify the event details. (example date, timestamp, source address, destination address etc.)

18. Vulnerability assessment and penetration testing (VA/PT) and Red team exercise

18.1 Conduct vulnerability assessment and penetration testing exercises for all critical systems particularly in internet.

18.2 Findings after the VA/PT should be assessed and necessary follow up action to be initiated to plug the loop holes.

18.3 Red teams may be used to identify the vulnerabilities and the business risk and efficacy of the defenses and check mitigating controls.

19. Incidence response & Management.

19.1 Bank to put in place an Incidence response policy/ program to be approved by the Board.

19.2 Include the incident response procedure including the role of the staff /outsourced staff handling such incidents, responses include readiness to meet various incident scenarios.

19.3 Any lessons learned may be put on record.

Recovery from cyber incidents:

19.4 Banks BCP/ DR capabilities shall adequately and effectively support the banks cyber resilience objectives. It should be designed in such a way that ban to recover rapidly from the cyber-attacks /incidents and safely resume critical operations within a short period of time.

19.5 The testing will include testing of crisis, communication to customers And other internal and external stake holders, reputation management.

19.6 The same may include such as (i) Define incidents, method of detection

Reporting system etc. (ii) Establish and implement security operations Centre (iii) Establish and implement systems to collect and share threat information to concerned agencies, (iv)Document and communicate strategies (v)Contain the level of cyber-attack and (vi) implement a policy

& framework for aligning security operations with security operations Centre, Incident response team and digital forensic to reduce the business Downtime.

20. Risk based transaction monitoring:

20.1 Risk based transaction monitoring or surveillance process shall be implemented as part of the Risk management system.

20.2 Bank shall notify the customers through alternate communication channels all payment or fund transfer transactions above a certain limit.

21. Metrics

21.1 Bank to develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators. (example coverage of anti-malware software, up-dation percentage, patch latency, extent of user awareness training, etc.)

22.Forensics:

22.1 Bank to periodically participate in cyber drills conducted by CERT-in, IDRBT/other agencies etc. and to have support /arrangement for forensic investigation/DDOS mitigation services etc.

23.User/Employee/Management awareness

23.1 Bank to define and communicate to users/employees, vendors and partners about the security policy covering secure and acceptable use of banks network and assets.

23.2 Staff training should be given to encourage the report the suspicious incidents. Evaluate the awareness level periodically. Conduct cyber security programmes in all the training schedule

23.3 Board members may be provided with necessary training on IT Risk and cyber security risk and evolving best practices. They may also be sensitized on various technological developments and cyber security related matters.

24. Customer education and Awareness

24.1 Bank to create awareness among the customers about the cyber security risks, encourage them to report any phishing mails etc. to take corrective action immediately. The awareness may be created during the customer meeting at the HO/ branch level.

Managing Director

Signature

Administrator

Signature