Name of the Policy	**Cyber Security Policy**
Department	**Information Technology (IT)**
Year	**2023-24**

I. Introduction:

Use of Information Technology by banks and their constituents has grown rapidly and is now an integral part of the operational strategies of banks. 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. In view of the low barriers to entry, evolving nature, growing scale/velocity, motivation and resourcefulness of cyber-threats to the banking system, it is essential to enhance the resilience of the banking system by improving the current defenses in addressing cyber risks. These would include, but not limited to, putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions, if and when they occur.

Hence, there is a need to put in place a robust cyber security/resilience framework in the Bank to ensure adequate cyber-security preparedness on a continuous basis and shall have advanced real time threat defense and management.

IT Cyber security policy covers all information used/ generated by the bank, which is stored, processed, transmitted or printed by a computer system or network and communication lines, and on any storage, medium including printed output. It applies to all the Bank employees and all others who directly or indirectly use or support the bank's computing services or information. The scope of the cyber security policy can be enhanced to cover any other organization, which may be created to fulfill our legal or operational requirements. In this regard the cyber security policy so designed shall cover entire bank, all its IT assets and Policy applies to:

a) All departmental functions.
b) All branches and geographical locations.
c) All information technology assets used; and
d) Third parties with whom we have a long-term association for regular operations as well as independent service providers engaged to provide infrequent or on-off services.
e) Vendor/ASP are who are providing service for the PDCCB.

II. Baseline Cyber Security and Resilience Requirements:

As per the NABARD Circular EC No.32/DoS-07/2020 dated:06.02.2020 guidelines on comprehensive **Cyber Security Framework** for Rural Cooperative Banks (RCBs), the list of Baseline Cyber Security and Resilience Requirements being implemented by the Bank roles and responsibilities of various stakeholders are listed out as under:

1. Inventory Management of Business IT Assets:

1.1. The Bank shall maintain an up-to-date inventory of Assets, including business data/information including customer data/information, business applications, supporting IT infrastructure facilities – hardware/software/ network devices, key personnel, services, etc. indicating bank business criticality.

1.2. The Bank shall classify data/information based on information classification /sensitivity criteria of the bank.

1.3. The Bank shall appropriately manage and provide protection within and outside organization borders/network taking into consideration how the data/information are stored, transmitted, processed, accessed and put to use within the bank's network, and level of risk exposed to depending on the sensitivity of the data/information.

1.4. As the CBS and Payment Channel switching/Interface services are also provided by M/s TCS under ASP model, the ASP shall ensure that, assets inventory to be maintained by the ASP to the extent of the Hardware or Software assets of DC/DR, Branch Servers and network equipment's in tune with the NABARD/RBI guidelines. The Bank shall review the compliance on regular basis.

2. Cyber Crisis Management Plan:

Apart from these, the traditional BCP/DR (Business Continuity Plan/Disaster Recovery) arrangements being taken care by the Application Service Provider(ASP) in connection with the CBS and Payment Channel switching/Interface, the Bank shall adopt the Cyber Crisis Management Plan in tune with the various initiatives taken up by the Government of India organization, CERT-In (Computer Emergency Response Team - India, a Government entity) in strengthening Cyber Security by providing proactive/reactive services and guidelines, threat intelligence and assessment of preparedness of various agencies in different sectors, including the financial

sector. The Bank shall refer to the CERT-In/ NCIIPC/RBI/IDRBT guidelines as reference material for their guidance.

3. Cyber Intrusions:

The Bank should promptly detect any cyber intrusions (unauthorised entries) so as to respond/recover/contain impact of cyber-attacks. The Bank should take necessary detective and corrective measures/steps to address various types of cyber threats viz. denial of service (DoS), distributed denial of services (DDoS), ransomware/crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

4. Preventing execution of unauthorized software:

4.1. The Bank shall maintain an up-to-date and preferably centralized inventory of authorised/unauthorised software(s). Considers in implementing whitelisting of authorised applications / software/libraries, etc.

4.2. The Bank shall manage overall installation of software/applications on end-user PCs, laptops, work stations servers, mobile devices, etc. and shall have a mechanism to block /prevent and identify in8stallation and running of unauthorised software/applications on all such devices/systems.

4.3. The Bank shall continuously monitor the release of patches by various vendors /Original Equipment Manufacturers (OEM), advisories issued by CERT-In and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank. If a patch/series of patches is/are released by the OEM/ manufacturer/vendor for protection against well-known/ well publicized/ reported attacks exploiting the vulnerability patched, bank has a mechanism to apply emergency patches expeditiously following an emergency patch management process from time to time.

4.4. The Bank shall have to define a framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) at senior levels who are well equipped in understanding the business and technical context of these exception(s).

4.5. All the web browser settings are to be set to auto update by disabling scripts like JavaScript, Java and ActiveX controls, when they are not in use.

4.6. As the CBS and Payment Channel switching/Interface services are availed from M/s TCS under ASP model, all CBS connected systems are being connected to separate network. Usage of Internet shall be in systems connected in separate network. For providing of internet connectivity to systems outside the CBS network, the permission from DGM(IT) is compulsory.

4.7. In scenarios where authorized software or any new software/patches from the vendors/OEM/Manufacturer, the DGM (IT) is the competent authority for providing the approval based on the requirement.

5. Environmental Controls:

5.1. Bank to have an appropriate environmental control for securing location of critical assets providing protection from natural and man-made threats.

5.2. Bank shall have pre-defined mechanisms for monitoring of breaches/ compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication and servers), access logs, etc. Appropriate physical security measures are taken to protect the critical assets of the bank.

5.3. ASP shall have follow all the environmental controls prescribed regulators like RBI/NABARD at DC/DR for CBS and Switching services of payment and delivery channels.

6. Network Management and Security:

6.1. The Bank has to have an up-to-date network architecture diagram at the organisation level including wired/wireless networks;

6.2. The Bank has to have up-to-date/centralized inventory of authorised devices connected to bank's network (within/outside bank's premises) and authorised devices enabling the bank's network. The bank has central monitoring system to monitor the devices connected to banks network including branches.

6.3. All the network devices are to be configured appropriately and periodically assessed whether the configurations are appropriate to the desired level of network security.

6.4. The Bank has to have appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

6.5. The Bank has to have a mechanism to identify authorized hardware/mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided with connectivity only when they meet the security requirements prescribed by the bank.

6.6. Has to have strong mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.

6.7. Has to have strong mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

6.8. Have to establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

6.9. To have a Security Operation Centre to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.

6.10. Should have boundary defenses of the Bank which is multi-layered with properly configured firewalls, proxies, Demilitarized Zone(DMZ) perimeter networks, and network-based Intrusion Detection System(IDS) and Intrusion Protection System(IPS) mechanism to filter both inbound and outbound traffic.

6.11. As the CBS and Payment Channel switching/Interface services are availed from M/s TCS under ASP model, the ASP shall ensure that, up-to-date network architecture diagram of DC/DR, connectivity to Branches/ATMs, and Payment & Delivery Channels switches inventory is in tune with the NABARD/RBI guidelines.

7. Secure Configuration:

7.1. To document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.) throughout the lifecycle and carry out reviews periodically.

7.2. The systems such as network, application, database and servers shall be used dedicatedly for the purpose for which they have been set up.

7.3. The Bank shall disable remote connections from the outside machines to the network hosting critical payment infrastructure like RTGS/NEFT, ATM Switch, IMPS/UPI interface etc., the Remote Desktop Protocol(RDP) shall be disabled for the infrastructure used for critical services.

7.4. Periodically evaluate critical device such as firewall, network switches, security devices, etc. configurations and patch levels for all systems in the bank's network including in Data Centers, in third party hosted sites, shared-infrastructure locations like branches/ATMs.

7.5. The bank shall ensure that

a) Disabling of PowerShell in servers where not required and disable in all Desktop systems

b) Restriction of default sharing including Inter-Process Communication (IPC) share.

7.6. As the CBS and Payment Channel switching/Interface services are availed from M/s TCS under ASP model, the ASP shall ensure that

a) Enabling of IP table to restrict access to the clients and servers in all switches of payment and delivery channels environment only to the authorized systems.

b) The Software integrity of payment and delivery channels related applications.

8. Application Security Life Cycle (ASLC):

8.1. As the CBS and Payment Channel switching/Interface services are availed from M/s TCS under ASP model, the ASP shall ensure that all security measures across all stages of application life cycle in tune with the NABARD/RBI guidelines from time to time.

8.2. In respect of other critical business applications, the bank may considers conducting source code audits by professionals by having assurance from application providers/OEMs that the application is free from embedded malicious /fraudulent code. Secure coding practices are implemented for internally /collaboratively developed applications.

8.3. The Bank shall take following measures for applications, which are not provided by CBS ASP: -

a) The development, test and production environments are to be properly segregated. The data being used in development and testing shall be masked.

b) Software/Application development approach shall be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secure rollout.

c) Software/application development practices adopt principle of defense-in-depth to provide layered security mechanism.

d) Adoption of new technologies shall be adequately evaluated for existing/evolving security threats and IT/security team of the bank reach reasonable level of comfort and maturity with such technologies before introducing for critical systems of the bank.

9. Anti-virus and Patch Management:

9.1. The Bank shall follow documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

9.2. As the CBS and Payment Channel switching/Interface services are availed from M/s TCS under ASP model, the ASP shall ensure timely patch management and implement and update the anti-virus protection to all IT components managed by them. For the purpose, the Bank need to obtain a certificate from ASP periodically.

9.3. For the IT components managed by the Bank, the Bank shall ensure

a) Appropriate systems and processes are in place to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems / Databases / Applications / Middleware, etc.

b) Implement and update the anti-virus protection for all IT infrastructure viz., Desktops, VSN endpoints, firewall, servers etc., through centralized system.

10. Periodic Testing:

10.1. The Bank shall conduct Vulnerability Assessment/ Penetration Testing (VA/PT) of internet facing web/mobile applications, servers and network components through their life cycle i.e., pre-implementation, post implementation and after changes if any from time to time etc., The VA of all critical applications and those on DMZ shall be conducted at least once in every 6 months and PT shall be conducted at least once in a year.

10.2. With regard to CBS and other payment and delivery channels infrastructure

handled by the ASP, the ASP shall ensure the conduct of VA/PT on regular basis and the Bank shall obtain the reports from the ASP periodically.

10.3. Application security testing of web/mobile applications shall be conducted before going live and after every major change(s) applied in the applications.

10.4. Penetration testing of the public facing systems as well as other critical applications shall be carried out by the professional qualified teams to be engaged by Bank.

10.5. The findings of the VA/PT and follow up action necessitated shall be monitored and reviewed by the Information Security Committee regularly. The vulnerabilities detected are to be remedied promptly in terms of Banks' Risk Management policy, so as to avoid exploitation of such vulnerabilities.

11. Change Management:

The Bank shall have a well-documented change management process to record/monitor all changes that are moved/pushed in the production environment. Changes to the business applications, supporting technology, service components and facilities shall be managed using robust configuration management process, which is major component of change management process adopted by the Bank to ensure integrity of any changes thereto. The ASP, which is taking care of CBS and Payment delivery channels shall follow Change Management policy and committee, which will meet at a periodic interval for process and approval of identified change process.

12. User Access Control / Management:

a. The Bank shall disallow administrative rights on end-user workstations/PCs/ laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.

b. To implement centralized authentication and authorization system like active directory authentication for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, also exploring two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.

c. The Bank shall provide secure VPN access to the bank's assets/services from within/outside bank's network by protecting data/information at rest and in-

transit.

d. The Bank shall protect user access credentials such as logon user ID, authentication information and tokens, access profiles, etc. against leakage/attacks.
e. Shall implement centralized systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (Servers/ OS/DB, applications, network devices etc.).
f. Shall implement policy level controls to minimize invalid login counts, deactivate dormant accounts.
g. To monitor any abnormal change in pattern of logon.
h. To implement measures to control installation of software on PCs/laptops, etc.
i. To implement appropriate controls for remote management/wiping/locking of mobile devices including laptops, etc.

13. Authentication Framework for Customers:

a) To implement authentication mechanism to provide positive identity verification of bank to customers.
b) Customer identification information shall be kept secure.
c) Bank shall act as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

14. Secure mail and messaging systems:

a) Bank specific email domains with anti-phishing and anti–malware, Domain based Authentication Reporting and Conformance(DMARCS) controls to be enforced in the email solution.
b) Have to subscribe at firewall level for Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites /rouge applications.
c) To implement secure mail and messaging systems, including those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.
d) To document and implement email server specific controls.
e) Bank strictly implementing domain mail mechanism. Not to entertain ouside mails except from official domain mails from onstitutions

15. Vendor Risk Management:

a) The Bank shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.

b) Bank needs to carefully evaluate the need for outsourcing critical processes like facility management services, desktop management, UPS management, Database Management, Network Management etc. and selection of vendor/partner need to be based on comprehensive risk assessment done by the Bank.

c) Among others, bank shall regularly conduct effective due diligence, oversight and management of third party vendor's/service providers & partners.

d) Bank shall establish appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities.

e) Banks shall ensure and demonstrate that the service provider (including another banks) adheres to all regulatory and legal requirements of the country. PDCCB necessarily enter into agreement with the service provider that amongst others provides for right of audit by the bank and inspection by the regulators of the country.

f) RBI / NABARD shall have access to all information resources (online/in person) that are consumed by banks, to be made accessible to RBI/ NABARD officials by the banks when sought, though the infrastructure/enabling resources may not physically be located in the premises of banks.

g) The Bank thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the bank's critical assets.

h) Background checks, non-disclosure and security policy compliance agreements are mandated for all third-party service providers.

i) With regard to IT components Bank shall follow Vendor/Outsourcing Risk Management Policy in tune with the guidelines issued by RBI from time to time.

16. Removable Media:

a) To defined and implemented policy for restriction and secure usage of removable media/Bring Your Own Device (BYOD) on various types/categories of devices including but not limited to workstations/PCs/Laptops/Mobile devices/servers, etc. and secure erasure of data on such media after use.

b) To limit media types and information that could be transferred/copied to/from such devices.
c) To get the removable media scanned for malware/anti-virus prior to providing read/write access.
d) To consider and implement centralized policies through Active Directory and Endpoint management systems to whitelist/blacklist/restrict removable media use.
e) As a default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorized for defined use with duration of use.
f) ASP shall have a policy for restriction and use of removable media/BYOD on various types/categories of devices including but not limited to Laptops/Mobile devices/servers, etc. and secure erasure of data on such media after use at DC/DR.

17. Advanced Real-time Threat Defense and Management:

a. To build a robust defense at perimeter level and other required levels against the installation, spread, and execution of malicious code at multiple points in the enterprise.
b. To implement Anti-malware, Antivirus protection including behavioral detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralized management and monitoring.
c. To consider and implement whitelisting of internet websites/systems at firewall level and also at end point security level.
d. To consider and implement secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway.
e. The Security Operations Centre (SOC) of ASP has to send the security alerts of DC/DR/other IT assets managed by them on behalf of Bank to the Bank.

18. Data Leak prevention strategy:

a) To develop and implement a comprehensive data loss/leakage prevention strategy at firewall level to safeguard sensitive (including confidential) business and customer data/information.

b) This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

c) ASP has to ensure that Customers data/ any other data of the Bank need to be protected and not to be disclosed without the prior permission from the bank and data loss/leakage prevention strategy has to be developed and implemented.

d) The Bank and ASP shall take periodic back up of the important data and store that data off-line- i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files.

19. Maintenance, Monitoring, and Analysis of Audit Logs:

a) Log retention is as per the recommendations and best practices by consulting all the stakeholders before finalizing the scope, frequency and storage of log collection.

b) Manage and analyze audit logs in a systematic manner so as to detect, understand or recover from an attack.

c) Enough care has to be taken to capture audit logs into a system log server pertaining to user actions in a system.

d) To implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software, ensuring that logs include minimum information to uniquely identify the log for example by including a date, time stamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.

e) ASP shall provide the audit logs of the users in the application which are being used by the Users of the Bank.

20. Incident Response & Management Responding to Cyber-Incidents:

a. The Bank shall have fully effective Incident Response program and procedures with due approval of the Board Management.

b. Shall have written incident response procedures including the roles of staff / outsourced staff handling such incidents; Response strategies, shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & co-ordination with stakeholders during response;

c. Shall have a mechanism to dynamically incorporate lessons learnt to continuously improve the response strategies, Recovery from Cyber -

Incidents:

d. The Bank's BCP/DR capabilities shall adequately and effectively support the Bank's cyber resilience objectives and shall also be so designed to enable the bank to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and ensure data is protected.

e. Banks shall ensure such capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative & coordinated resilience testing that meet the bank's recovery time objectives.

f. Such testing shall also include testing of crisis communication to customers and other internal and external stakeholders, reputation management. Adequate capacity shall be planned and maintained, in consideration thereof. The following may be considered:

   i. Define incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans.

   ii. Establish and implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incidents.

   iii. Establish and implement systems to collect and share threat information from local/national/international sources following legally accepted/ defined means/process

   iv. Document and communicate strategies to respond to advanced attacks containing ransom ware/cyber extortion, data destruction, DDOS, etc.

   v. Contain the level of cyber-attack by implementing shielding controls/ quarantining the affected devices/systems.

   vi. Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.

21. Risk based transaction monitoring:

a. The Bank is the sub member for the Centralized Payment System(CPS).

b. Risk based transaction monitoring and surveillance process are to be implemented as part of fraud risk management system across all-delivery channels.
c. The bank should notify the customer, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.

22. User / Employee/ Management Awareness:

a) To define and communicate to users/employees, vendors & partner's security policies covering secure and acceptable use of bank's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level.
b) To have the procedure to encourage them to report suspicious behavior incidents to the incident management team.
c) To conduct targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.). PDCCB made it part of the induction and ongoing training sessions to all employees.
d) To evaluate the awareness level periodically.
e) To establish a mechanism for adaptive capacity building for effective CyberSecurity Management. Making cyber security awareness programs mandatory for new recruits as part of induction.
f) Board members need to be sensitised on various technological developments and cyber security related developments periodically which is on monthly basis.
g) Board members shall be provided with awareness programs on IT Risk/ Cybersecurity Risk and evolving best practices in this regard so as to cover all the Board members at least once a year.

23. Customer Education and Awareness:

a. Improve and maintain customer awareness and education with regard to cybersecurity risks.
b. Encourage customers to report phishing mails/ Phishing sites and on such reporting take effective remedial action.
c. Educate the customers on the downside risk of sharing their login credentials/ passwords etc. to any third-party vendor and the consequences thereof.

24. Cyber Security Operation Centre (C-SOC):

As per the comprehensive Cyber Security Frame work guidelines stipulated for Cooperative Banks by the NABARD, the Bank is not required to maintain Cyber Security Operation Center (C-SoC) as the Data Center/Data Repository is being hosted by the CBS ASP. As per the terms and conditions of Service Level Agreement (SLA) entered with the CBS ASP, Cyber Security Management (IT) shall be conducted in the following manner:

a) ASP shall have a Cyber security policy as required by relevant statutory authority and shall share a copy with all member banks. Cyber security Policy shall ensure compliance of Cyber Security Frame work requirements for bank's centralized DC/DRC setup as issued by relevant mandatory authority and the branch servers and any hardware/software installations done by ASP.

b) Cyber Security Policy shall ensure secured transactions on electronic Banking product services offered to clients by enhancing information security processes and procedures for DCCBs and SCBs on periodic basis.

c) ASP shall be certified for ISO 27001:2005 standards towards its DC and DRC. DC and DRC shall have a detailed internal risk assessment process, procedures before undergoing any such certification. ASP shall conduct periodic internal reviews of the process deployed to ensure that gaps are assessed proactively, treated upon as prescribed by ISO 27001.

d) ASP shall get I.T. and Cyber Security Audit done for ASP's setup at DC/DRC as per relevant statutory authority and submit the certificate to the respective banks on a periodic basis.

e) The SSL Encryption shall be more than 128 bits, wherever applicable.

f) ASP shall establish a C-SOC (Cyber Security Operations Center) for ASP's DC/DRC setup as required by relevant statutory authority within 6 months from the start date of contract.

g) ASP shall ensure adequate cyber protection of all its systems, software and applications including third party application software provided through ASP to the banks.

h) ASP shall carry out VA/PT for all its applications including third party applications provided to the banks periodically and take corrective and preventive actions for security. The results of VA/PT and actions taken may be shared with the banks if required.

i) ASP shall implement CSOC, which shall include real time monitoring of its critical infrastructure and CBS and all other applications under this project.

j) ASP shall integrate SIEM with DLP Solution for the services at DC & DRC
k) ASP shall ensure Antivirus & Firewall monitoring and updation at all times of ASP managed servers through CSOC
l) Infrastructure of ASP shall be installed, hardened & secured on the basis of regulatory and industry guidelines
m) ASP shall deploy & manage IAM (Identity and Access Management) to ensure an effective Identity, Access & Authentication control in place for the infrastructure & services managed by ASP
n) ASP shall ensure that appropriate protection is deployed against network attacks for the infra managed by it. This shall be achieved by deploying IPS, firewalls and monitor it through C-SOC
o) The Bank shall obtain periodically certified copies from ASP stating they are following guidelines of statutory authorities without deviation.

Governance Mechanism:

1. Information/Cyber Security Cell at APEX Bank:

A separate cell namely Cyber Security Cell headed by the Chief Information Security Officer (CISO) created and placed in the Internal Audit Department(IAD), APCOB. The broad functions of Cyber Security Cell are given as under: -

a) To focus exclusively on Cyber Security Management in APCOB and also monitor and guide the implementation of Cyber Security Framework in all 13 DCCBs.
b) Cyber Security Cell shall monitor and review all IT related aspects such as technologies adopted, delivery channels, digital products being offered, internal and external threats etc.,
c) The Cyber Security Cell shall adequately resource in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment and forensic assessment etc.,
d) Cyber Security Cell asses the preparedness on base line controls indicated for implementation of effective Cyber Security Framework as per the Vulnerability Index for Cyber Security Framework(VICS) for both APCOB and DCCBs on half yearly basis as per the guidelines issued by NABARD and place the same before the Information Security Committee for review. The guidance note for VICS tool is given in Annexure 1 and VICS tool is given in Annexure-2.

2. Chief Information Security Officer (CISO):

A Senior level official (AGM/DGM) shall be designated as Chief Information Security Officer (CISO), responsible for articulating and enforcing the policies that the Bank uses to protect its information assets apart from coordinating the cyber security related issues/implementation within the organisation as well as relevant external agencies. The CISO shall be primarily be responsible for ensuring compliance to various instructions issued on information / cyber security by NABARD/RBI. The roles and responsibilities of the CISO are listed out as under:

a) The CISO should report directly to the Deputy General Manager or in his absence to the Chief Executive Officer directly.
b) The CISO should have a reasonable minimum term, preferably 3 years.
c) The CISO should place a separate review of cyber security arrangements/ preparedness of the Bank before the Board of management on a quarterly basis.
d) The CISO will be responsible for bringing to the notice of the Board about the vulnerabilities and cyber security risks that the Bank is exposed to.
e) The CISO, by virtue of his role as member secretary of information security and/or related committees(s), if any, may assess, inter alia, current/emerging cyber threats to banking (including payment systems) sector and ensure that the Banks's preparedness in these aspects are invariably discussed in such committee(s).
f) The CISO shall be a special invitee to the IT Strategy Committee and IT Steering Committee. The CISO may also be a member of (or invited to) committees on operational risk where IT/IS risk is also being discussed.
g) The CISO's office shall be adequately staffed with technically competent staff, if necessary, through recruitment of specialist officers, commensurate with the business volume, extent of technology adoption and complexity.
h) The CISO will be responsible for reporting of Cyber fraud incidents to the regulated entities as per the guidelines of RBI/NABARD from time to time.
i) The CISO shall not have any direct reporting relationship with the CIO/CTO and shall not be given any business targets.

3. Information Security Committee(ISC):

3.1. The composition of the Information Security Committee(ISC) is given as

under: -

Chief Executive Officer	Chairman
General Manager–IT Development/operations	Member
Deputy General Manager –IT & Development	Member
Assistant General Manager (ITD)	Member
Assistant General Manager (DoS)	Member
Chief Manager -IT &DoS	Member
Chief Information Security officer (CISO)	Member/Convener
Chief Information/Technology Officer (CIO/CTO)	Special Invitee

3.2. The Committee shall meet at least once in a quarter. The roles and responsibilities of the Information Security Committee(ISC) are listed out as under:

a) Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified risks are managed within a Bank's risk appetite.
b) Supporting the development and implementation of a Bank-wide information security management programme.
c) To review the status on implementation of Cyber Security Framework in tune with the policy guidelines through VICS tool and to place the observations and findings before the Board of Management for approval.

* CIO/CTO shall be well qualified who is in charge of technological needs in the Bank. CIO shall assess short and long term needs of the bank and utilizes capital to make investments designed to help the bank reach its business objectives.

4. IT Steering Committee:

4.1. The composition of the IT Steering Committee is given as under:

General Manager (ITD)	Chairman
General Manager (DoS)	Member
General Manager (Bkg/DoR)	Member
General Manager (PDD)	Member
Deputy General Manager (ITD)	Member/Convener
Chief Information/Technology Officer (CIO/CTO)	Special Invitee
Chief Information Security Officer (CISO)	Special Invitee
Chief Risk Officer (CRO)	Special Invitee

4.2. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the IT Strategy Committee, which is sub-committee of Board of Management of the Bank. The IT Steering committee shall appraise/report to the IT Sub-Committee periodically. The committee should focus on implementation. Its functions, inter-alia, include:

a) Defining project priorities and assessing strategic fit for IT proposals.
b) Reviewing, approving and funding initiatives, after assessing value• addition to business process.
c) Ensuring that all critical projects have a component for "Project Risk Management".
d) Sponsoring or assisting in governance, risk and control framework, and also directing and monitoring key IT governance process.
e) Provide direction relating to technology standards and practices.
f) Provide direction to the IT architecture design and ensure that IT architecture reflects the need for legal and regulatory compliance, ethical use of information and business continuity.

5. IT Strategy Committee: -

5.1. It is sub-committee to the board of management of the Bank. The composition of the IT Strategy Committee is given as under: -

Person In Charge/Chair person	Chairman
Chief Executive Officer	Member
General Manager (ITD)	Member/Convener
Deputy General Manager-(IT)	Member
Deputy General Manager (Development)	Member
Professional Director	Member
Chief Manager –(IT) &DoS	Member
Chief Information/Technology Officer (CIO/CTO)	Special Invitee
Chief Information security officer (CISO)	Special Invitee

5.2. Roles and responsibilities of the IT Strategy Committee are given as under:

a) Approving IT Strategy and policy documents and recommend for Board of Management for adoption.
b) Ensuring that management has to put an effective strategic planning process in place.

c) Ensuring that the IT organizational structure complements in business model and its direction.
d) Ensuring IT investments represents a balance of risks and benefits and the budgets are acceptable.

6. Audit Committee of Board (ACB): -

The Audit committee of the Bank, in addition to its prescribed role as per extant instructions, the ACB shall also be responsible for the following:

a. Performance of IS Audit and Evaluation of significant IS Audit issues - The ACB should devote appropriate and sufficient time to IS Audit findings identified and members of ACB need to review critical issues highlighted and provide appropriate guidance to the Bank's management.
b. Monitor the compliance in respect of the information security reviews/VA-PT audits under various scope conducted by internal as well as external auditors /consultants to ensure that open issues are closed on a timely basis and sustenance of the compliance is adhered to.

III. Reporting of Cyber Incidents:

An effective mechanism shall be in place to report the cyber security incidents in a timely manner and take appropriate action to mitigate the incident. Report all unusual cyber fraud incidents to CERT-In and IB-CART with in stipulated time.

IV. Cyber Security Related Returns:

As per the NABARD circular dt:17.07.2023 "*Cyber Security Related Returns-Certification by Internal Audit Head",* IS cell should submit following periodical returns to CSITE Cell, NABARD duly authenticated by Head of Internal Audit in order to ensure accuracy and consistency:

a) Vulnerability Index on Cyber Security (CS-01) - Every half year ending March and September.
b) Level of Exposure and Level of Compliance (CS-02) - Every half year ending March and September.
c) Storage of Payment data - Every year ending March.

Note: Internal Audit Head i.e., Head of Internal Audit Department will be personally held accountable for the accuracy of the submissions of returns.

V. Activities to be attended by IT Department5 to Enhance Cybersecurity:

1. **Unauthorized Software Removal**: In order to maintain a secure environment, please instruct your team to uninstall all unauthorized software from the systems. each bank should prepare a list of Authorized software to be used in the bank and should place it in board for approval.

The list of Authorized software in PDCCB is as follows:

- Microsoft Edge
- Win rar
- Firefox
- Google Chrome
- MS Office (365/Standard)
- Microsoft Teams
- Adobe Reader
- Notepad++
- Edit plus 3
- Printer/scanner drivers provided by OEM (HP, EPSON, Brother, etc)

2. **Installation of Licensed, Latest Software Versions**: It is crucial that the systems are equipped with licensed, up-to-date versions of the operating system, MS Office, and Antivirus software. Internet connected systems should be set to "update automatically to latest versions" in update screen.

3. **Disabling Unnecessary Access**: To minimize potential vulnerabilities, please ensure that Remote Desktop Protocol (RDP), Command Prompt (CMD), PowerShell, PowerShell ISE, Registry Editor (Regedit) and pen drive accesses are disabled on all systems. Maintain registers for recording the Remote connections and pen drive accesses given on prior approvals.

4. **CBS System Security**: Create Guest user accounts in the CBS systems and subsequently change the administrator passwords. These administrator passwords should only be shared with the ITD CBS section.

5. **Non-CBS System Security**: Similar to the CBS systems, update and safeguard the administrator passwords for non-CBS systems. These passwords should be shared exclusively with the ITD CBS section. No staff should login with Administrator access in both CBS and Non-CBS systems including IT Dept staff.

6. **Biometric Device Installation**: Install biometric devices in all CBS systems. Every employee should be provided 2FA for logins to CBS. Following installation, please obtain declarations from the respective staff members and submit the declaration forms to the IT Department.

7. **Screen Lock and Sleep Mode Activation**: To prevent unauthorized access,

enable auto screen lock after 3 minutes of inactivity and initiate sleep mode after 30 minutes of inactivity on all systems.

8. **Hardware Tagging**: Label all hardware components including monitors, CPUs, laptops, printers, scanners, etc. IT Dept should have a proper record of this with them for dynamic decision making and for submission of information to respective inspecting officials when asked. The configurations of each hardware are also to be noted down when tagging.

9. **OS Patch Updates**: Ensure that all systems have the latest OS patches installed for maximum security.

10.**Software Inventory Submission**: Compile a comprehensive software inventory for all systems and keep it in the IT Dept.

11.**Data Backup Prior to Formatting**: Before initiating formatting of any system, ensure that critical files are backed up and provided to the relevant staff members.

12.**Desktop Cleanliness**: Maintain a clutter-free desktop environment by relocating files to appropriate drives. Limit file saving options to the "Downloads" folder on the C Drive.

13.**Windows Firewall and Defender Activation**: Enable both the Windows Firewall and Windows Defender on all systems for enhanced protection.

14.**Hardware Arrangement**: Organize cables within server racks and ATMs to eliminate clutter and ensure a tidy appearance. Trim excess cable lengths as necessary. Remove any redundant hardware from racks and promptly keep them with the IT Dept.

VI. Review and Periodicity:

These terms & Conditions are subjected to periodic updation from time to time. For any change in the policy, Managing Director is empowered to modify the changes subject to the guidelines issued by RBI/NABARD/NPCI and any other statutory authority from time to time and place before the Board of Management for approval. Policy will be reviewed on annual basis.

Sd/-

CHIEF EXECUTIVE OFFICER