CYBER SECURITY POLICY

KANNUR CO-OPERATIVE URBAN BANK LTD.

ABSTRACT

Cyber Security Policy of Kannur Co-operative Urban Bank as per RBI guidelines.

Document Information

Prepared By:	Anil.C	Document Version No:	1
Title:	Information Security Consultant – TuxCentrix Consultancy Pvt. Ltd.	Document Version Date:	
Reviewed By:	Cyber Security Steering Committee	Review Date:	

Distribution List

From	Date	Phone/Fax/Email

Document Revision History

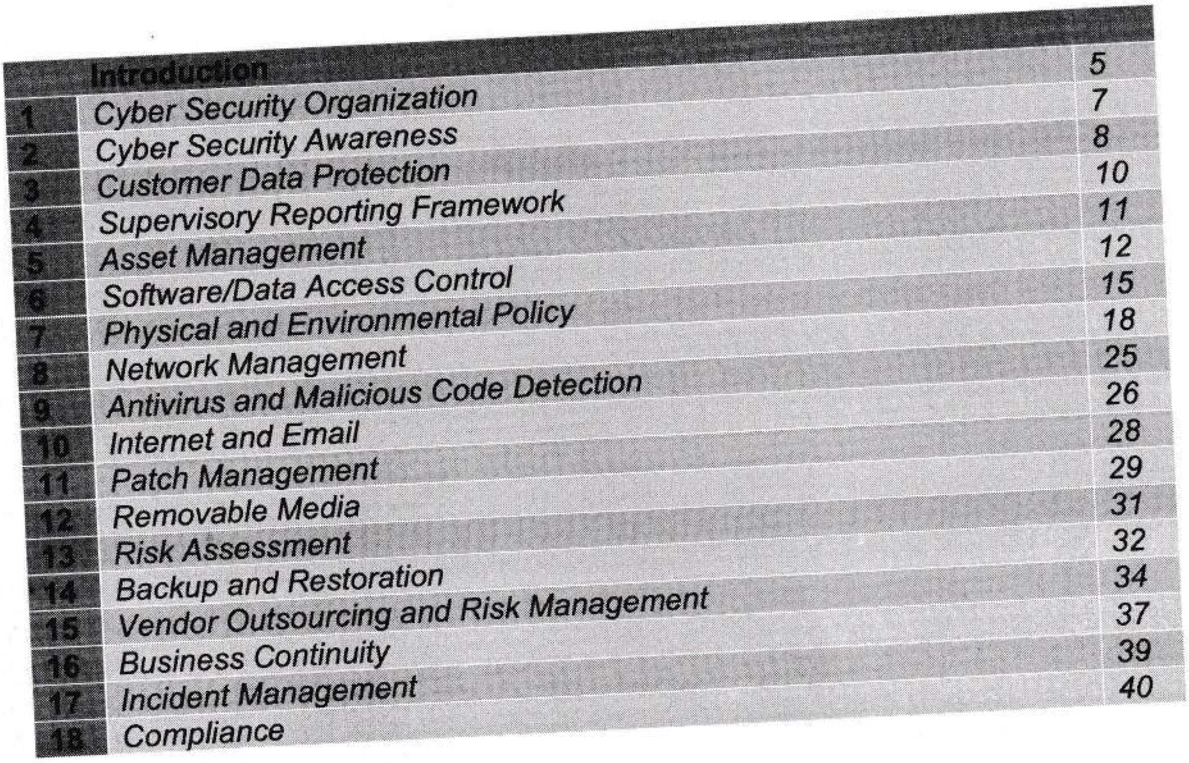
Ver. No.	Ver. Date	Prepared By	Reviewed / Approved By	Affected Section & Summary of Change
1.0.0		Anil.C	CSSC/Board of Directors	Nil

Errors and Omissions

When reading this document if you identify any errors or omissions please inform Cyber Security Steering Committee through email giving a brief description of the problem, its location within the document and your contact details at *****.com

Confidentiality

This document contains privileged and confidential information pertaining to Kannur Co-operative Urban Bank Ltd.. The addressee should honor his access rights by preventing intentional or accidental access outside the access scope.



THE KANNUR CO-OPERATIVE ... BANK LTD No.1534
H.O
KANNUR-670002

Cyber Security Policy

Policy scope

This policy applies to:

- The head office of Kannur Co-operative Urban Bank Ltd.
- All branches of Kannur Co-operative Urban Bank Ltd.
- All staff, customers, third party service providers, and stake holders Kannur Co-operative Urban Bank Ltd.

Introduction.

Owing to the vast development of Information and Communication Technology cyber space has become more vulnerable to a wide variety of challenges, risks and threats. Large-scale cyber attacks experienced in banking sector highlighted the necessity for Cyber Security Policy in order to provide safe and credible functioning of critical information systems.

"Cyber Security Policy" underscores several compelling priorities, the implementation of which is necessary to meet the objectives set out by RBI in Basic Cyber Security Framework for Primary (Urban) Cooperative Banks.

The first priority of "Cyber Security Policy" is to define the strategy in respect of cyber security provision. The Policy provides an overview of those principles that lead to the creation of safe infrastructure and strategies that will serve as a solid basis for safe protection of information systems and networks in the Bank.

This policy is approved by the Board and applicable to all employees, associates, vendors and those who access bank information technology infrastructure.

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to the bank owned Information System Policy. Additional administrative sanctions may apply; up to and including termination of employment or contractor status with the bank or expulsion of employees. Civil, criminal and equitable remedies may also apply.

STRATEGIC GOALS AND OBJECTIVES

Vision: Build and enhance robust, effective and secure information and communication technology systems for Kannur Co-operative Urban Bank Ltd.. that sets the standard in the RBI cyber security framework.

Mission: Build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents, to protect information systems of the Bank.

Objectives:

- Create secure cyber system in Bank, enhance infrastructure capabilities for the Bank.
- Set up a system to design all conceptual documents necessary for security implementation. The system will ensure documents to be in compliance with global security standards and best practice;
- Establish and enhance information technology security 24/7 incident response mechanisms to protect Bank infrastructure, carry out rapid identification of threats and risks, perform necessary responsive and preventive measures, in case of necessity provide crisis management through predictive, preventive, protective and recovery actions;
- Enhance the protection and resilience of functioning of the Bank by operating 24/7 mechanisms applying best practice on establishment, acquisition, development and operation of information resources;
- Create a workforce of professionals skilled in cyber security through capacity building, educational programs and training;
- Create a culture of cyber security users to act effectively in compliance with the defined rules;
- Encourage personnel to participate in cyber security related training and educational programs

Enforcement and Compliance

Cyber Security policy is the basis of organization's Cyber security. Many organizations have information Cyber security policy in place to ensure that their information is always secure. However, having a cyber security policy document in itself is not enough. It is very important to ensure that the contents must be implemented to be effective.

KANNUR CO-OPERATIVE URBAN BANK LTD. H.O KANNUR -670002

1. Cyber Security Organization

Cyber Security Steering Committee(CSSC) is formed to direct and manage cyber security governance of the Kannur Co-operative Urban Bank Ltd.. CSSC is responsible for policy maintenance activities including reviews and monitoring compliance and enforcement of this policy.

The Cyber Security Steering Committee is chaired by GM and consist of the following members.
1. General Manager
2. Board Member
3. Computer Programmer
4. Chief Accountant

The secretary of the committee is the IT manager of the bank who has the responsibility of arranging the meeting, preparation of the agenda of the meeting and recording of the minutes of the meeting.

Cyber Security Steering Committee (ISSC) is the entity, which has ownership of all cyber security policies and procedures. In this context, "ownership" is defined as responsibility for creating, monitoring, and enforcing the administrative, physical, and technical controls the Kannur Co-operative Urban Bank Ltd.. Cyber Security policies will be published and communicated to all employees, associates, and vendors, as appropriate.

ISSC will initiate annual risk assessments in order to determine the level of security risk and the efficacy of security controls within the bank. The purpose of these risks assessments will be to:

- Address changes to business requirements and priorities
- Consider new threats and vulnerabilities that might exist
- Confirm that security controls and mechanisms remain effective and efficient

CSSC will review and make necessary changes to the Policy on an annual basis or whenever a major change is made to the bank environment or a new technology is deployed. During the review, CSSC will evaluate the following:

- The overall policy's effectiveness
- The costs and impact of security controls and mechanisms on business efficiency.
- Changes in technology that affect the adequacy and / or appropriateness of security controls and mechanisms in the environment. CSSC will create a repository for the storage of all security policies. This repository must be accessible by all bank associates in some fashion.

CSSC will report to the executive leadership team via General Manager. The IT manager will determine the reporting schedule and formats for CSSC.

The overall responsibility for ensuring compliance with all security controls as specified by CSSC rest with the Senior Manager IT.

Individual department heads and team leadership are responsible for implementation of security controls in their respective domain by the direction of CSSC.

2. Cyber Security Awareness

Cyber security awareness should be imparted as appropriate at all levels including board employees, customer, stake holders and third party vendors at frequent intervals.

The strategy of security awareness program should be effective and ensure that all parties involved in the banks operation are aware of:

- the existence of cyber security policy;
- where to find it;
- how to comply with it;
- how it will aim to improve the operations of the company;
- how vital the protection of information really is; and
- the consequences of non-compliance.

The program should emphasize on explaining why "Information Security is everyone's responsibility" and teach each one, about their role in maintaining the security.

Once cyber security policy has been established, it must be communicated formally to all the people responsible for enforcing and complying with it. This should include employees, vendors, contractors, and other relevant users. Given the nature of the organization, it may also be necessary to communicate some or all policies to customers as well.

An essential part in this communicating process is to establish a record that those involved have read, understood, and agreed to abide by the policy. It is a big challenge to ensure that users understand and accept the policy that governs them.

3. Customer Data Protection

Data privacy is important to the bank. This means that we process data about identified or identifiable individuals, which is called personal data, with due care and in accordance with applicable data protection law.

The personal data we collect from individuals mostly consists of user data, such as name, business function, gender, business address, telephone number, email address and other personal data Users provide to us.

Reasonable and appropriate technical and organizational security measures to protect the personal data should be implemented and maintained, from unauthorized access, alteration, disclosure, loss or destruction.

General staff guidelines

1. When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
2. Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
3. If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
4. Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
5. Servers containing personal data should be **sited in a secure location**, away from general office space.
6. Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
7. Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
8. All servers and computers containing data should be protected by **approved security software and a firewall**.
9. When working with customer data, employees should ensure **the screens of their computers are always locked** when left unattended.
10. Customer data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
11. Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
12. Customer data should **never be transferred outside India**.
13. Employees **should not save copies of customer data to their own computers.** Always access and update the central copy of any data.
14. Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
15. Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No.1534
H.O.
KANNUR
-670002

16. When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.
17. When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
18. Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
19. **Data printouts should be shredded** and disposed of securely when no longer required.

Data Accuracy

1. The bank requires to take reasonable steps to ensure data is kept accurate and up to date.
2. The more important it is that the customer data is accurate, the greater the effort bank should put into ensuring its accuracy.
3. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Disclosing data for other reasons

1. In certain circumstances, Law allows customer data to be disclosed to law enforcement agencies without the consent of the customer.
2. Under these circumstances, bank will disclose requested data. However, the CCSC will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

4. Supervisory reporting Framework

Computer security incident response has become an important component of information security. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

An effective incident reporting system should be established which contributes to the collection of reliable and up-to-date data on information security incidents that ensures:

1. quick dissemination of information among interested parties,
2. a coordinated response,
3. access to a wide pool of expertise about such incidents,
4. that national authorities can follow up with the infrastructure managers in a regulatory capacity,
5. threat analysis; and
6. identification of good practices.

Establishing an incident response capability should include the following actions:

- Developing procedures for performing incident handling and reporting
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- Determining what services the incident response team should provide
- Staffing and training the incident response team.

Supervisory Reporting Framework

CSSC should report immediately all unusual cyber security incidents to the Department of Co-operative Bank Supervision Central office, C-9,1st Floor, BKC, Mumbai -400051 by email giving full details of the incident

A 'NIL' report shall be submitted on quarterly basis in case of no cyber security incidents.

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No. 1554
H.O.
KANNUR
-670002

5. Asset Management

This Policy defines the key principles and requirements which will apply to the information assets of the company.

Inventory of Software, Physical and Information asset shall be maintained in the format approved by CSSC. All information asset of the company shall be identified, listed in common format and shall identify the associated vulnerabilities/threats for risk assessment.

This policy ensure.

- accurate recording of asset information.
- accurate recording of asset movements.
- all responsible parties are aware of their roles and responsibilities regarding the assets of the organization.
- preventative measures are in place to control cyber security threats, eliminate theft, loss, misuse and misuse.

Ownership of assets

Ownership and maintenance of inventory shall be assigned to a responsible person/team. CSSC should define the ownership of Inventory to maintain and keep it up to date. Inventory can be maintained in written or electronic form. It should be available to all respective peoples who will use it only for official purpose. Data should be classified and ownership should be defined.

Acceptable use of assets

Rules for acceptable use of assets shall be defined and communicate to all the users and external parties. ISSC should define the rules for acceptable use of the assets. This gives the guidelines to the asset handler about the maintaining security while handling the assets.

Information Asset Classification

The Information asset owner must classify all the information assets of of bank as per classification scheme to represent its sensitivity and criticality to the organization. Information owners will be responsible for assigning and maintaining appropriate data classifications. Files and electronic mails created by individuals will be classified by them.

All information processed, maintained, stored, and generated by he bank in the course of normal business operations must be treated as classified information and handled in accordance with the risk involved.

All sensitive information must have a formally assigned information owner, responsible for maintaining the security of their information. The information owner must develop appropriate protective and accountability controls to safeguard their data.

Information labeling and handling

All the information assets shall be labeled as per the data classification scheme. All assets need to be labeled from the time it is created to the time when it is destroyed. Such labeling shall appear on all manifestation of information.

6. Software/Data Access Control

Access to software, information assets and business processes must be controlled on the basis of business and regulatory security requirements.

Up-to-date and preferably centralised inventory of authorised software(s)/approved applications/software/libraries, etc. should be maintained.

Mechanism should be established to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. Also, put in place a mechanism to block/prevent and identify installation and running of unauthorised software/applications on such devices/systems.

The web browser settings should be set to auto update and consider disabling scripts like JavaScript, Java and ActiveX controls when they are not in use. Internet usage, if any, should be restricted to identified standalone computer(s) in the branches which are strictly separate from the systems identified for running day to day business.

The process for creating, changing and removing users from systems and application should be established. Allowed access rights should be audited and revised periodically. Access to bank's information asset should be allowed on the basis of business requirement.

Access Control Methods

Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Policy.

Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, user account privileges, server and workstation access rights, firewall permissions, network zone and VLAN ACLs, IIS / Apache intranet / extranet authentication rights, login rights, database access rights, encryption and other methods as necessary.

Access control applies to all Bank owned networks, servers, workstations, laptops, mobile devices and services run on behalf of Bank.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within banks Active Directory domains.

Access Approval

All access by any user or system (employee, contractor, third party service vendor) must be justified by a business reason for why the access is necessary, along with the parameters of access (what classification level, times/dates, from what locations, etc.) Access cannot be simply given to 'everything'. Justifications shall be kept on file for review, as well as forensic purposes.

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No. 1534
H.O.
KANNUR
-670002

Access Request

Users will request access in the following way:

- A formal access control request is made using an approved form and documentation.
- A valid business justification for the access is documented.
- Access requests will specify particular systems or information (no general access to all) commensurate with the person's access level.
- Access requests must be correctly approved
- Request forms should be stored by the administrators and retained until at least 90 days after the person has left the company

Changes in access must be requested and documented in the same way as original access requests (may be accomplished on the original form as notations and subsequent approval signatures)

Access Request Form

All access must be requested through an Access Request Form and routed through IT Department. Log register is to be maintained in IT Department server or related systems.

User registration

A registration and re-registration procedure shall be used for granting access to all information asset of the company. User should not get access without registration process and in case of violation of being a valid user; user rights should be de-registered with immediate effect.

User IDs

Each user must have a unique ID that only they should use for logical access. This ID may be used to access several systems but will not be used by anyone else. Employees should not share their unique ID or security access cards to secured areas. Users are responsible for all actions taken with their unique user ID, whether or not they are the ones who took the actions. Thus, it behoves the user to protect their IDs and passwords. Never give your password to anyone, including your supervisor. User IDs for users who have left the company must be deactivated or deleted. It is permissible to retain a user account for access to the user's data once they have left, but the password must be changed to prevent the user from accessing their account. Data will be recovered and moved as soon as possible, and the account disabled or deleted in this case.

Password

Password issuing, strength requirements, changing and control will be managed through formal processes.

Password issuing will be managed by the IT department for employees, associates, contractors, partners, and vendors. Password length, complexity and expiration times will be controlled through Group Policy Objects in operation system.

Privilege management

The allocation and use of privileges shall be restricted and controlled. Inappropriate use of system privileges may become a major contributory factor to the failure of systems hence access to critical systems should be filtered in such a way that nobody will be able to take disadvantage of the rights.

User Account Review

Administrators will conduct periodic (at least monthly) audits of all user accounts and disable/delete any accounts that have not been used in the past month. If the user is known to be away from the office (maternity leave, sabbatical, etc.) then the account must be disabled and a notation made as to why and the person's expected return. User accounts that have never been used in the month period must be deleted.

Review of user access rights

User access rights should be reviewed at regular intervals for effective control over access to data and information. User access to data and information should be reviewed on regular basis to keep updated access control. Transferred or left employees account gets removed in such periodic access audit.

User Access Termination

Users who leave, the bank will have their access to all systems terminated on their last day, or as soon as possible if they are being terminated for cause. All access must be terminated (through disabling, deleting, or changing the password), including physical access to facilities, and remote access. The user access request form and associated documentation must be used as a reference to ensure that all systems and networks are addressed. The access request form must be annotated that access has been terminated and how, (e.g. disabling).

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No. 1531
H.O.
KANNUR
-670002

7. Physical and Environment Policy

Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.

Bank's Branches / Departments are required to establish physical and environmental controls for assets under their physical control. Requirements within this policy extend to self contained facilities such as external data centers, as feasible, and should be considered prior to entering into a contract with an external data center, workplace, or facility. In conjunction with the Asset Management Policy, physical and environmental controls must follow the minimum requirements established within this policy.

Physical and Access Controls

Physical and access controls within the organization including branches and department systems will follow the requirements outlined below.

Sl.#	Control	Description
1	Policy and Standards	Develop, document, and disseminate formal physical and environmental protection standards that set criteria for: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2	Physical Access Authorizations and Maintenance	1. Develop and maintain a list of personnel authorized to enter controlled access facilities where information systems reside, and identify those areas in a facility which are designated publicly accessible 2. Manage the list and all associated logs of access, including: ● Track names and status of all who have been issued authorized credentials for facility access ● Identify and implement regulatory and policy log-retention requirements ● Regularly audit the detailed access log(s) of facility ● Regularly review the access list, and promptly remove individuals from the facility access list when access is no longer required
3	Physical Access Control	Enforce physical access controls for all physical access points to the controlled facility. This includes: ● Verify individual authorization before granting access ● Control entry to the facility using physical access devices and/or guards ● Maintain physical-access audit logs ● Provide additional controls: ➢ Escort visitors and monitor visitor activity ➢ Secure keys, combinations, and other physical access devices

		➢ Inventory physical-access devices annually ➢ Conduct routine maintenance checks to verify that devices are functioning properly ➢ Change combinations and keys annually or when keys are lost, combinations are compromised, or individuals are transferred or terminated ➢ Deactivate or revoke user access credentials upon transfer or termination
4	Access Control for Transmission Medium	Control physical access to system distribution and transmission lines, for example: (i) lock wiring closets, (ii) disconnect or lock spare jacks; or (iii) protect cabling by conduit or cable trays.
5	Access Control for Output Devices	Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
6	Monitoring Physical Access	Monitor physical access to the controlled facility to detect and respond to physical security incidents, including: ● Review physical access logs every 30 days and upon the occurrence of any known physical-access violation ● Coordinate the results of the reviews with the departments/branches incident response entity
7	Access Records	● Maintain visitor-access logs for controlled facilities per the department / branch retention guidelines, and ensure the logs are reviewed regularly. ● For information systems designated as High automated mechanisms should be established to facilitate the maintenance and review of visitor-access logs.

21.3.2 Environmental Controls

Environmental Controls within bank will follow the requirements outlined below.

Sl.#	Control	Description
1	Power Equipment and Power Cabling	Protect power equipment and power cabling for information assets from damage and destruction.
2	Emergency Shutoff	● Provide the capability to shut off power to information systems in a facility or individual system components in emergency situations ● Place shut-off switches or devices in a defined location to facilitate safe and easy access for personnel, while protecting emergency power shutoff capability from unauthorized activation
3	Emergency Power	● Provide a short-term uninterruptible power supply (UPS) to utilize if the primary power source fails. ● Information systems with a designation of High should be provided with a long-term alternate power supply that can maintain minimum operational capability in the event of an extended loss of the primary power source.
4	Emergency Lighting	● Employ and maintain automatic emergency

THE KANNUR CO-OPERATIVE URBAN BANK LTD No. 1554
H.O.
KANNUR
-670002

		lighting for the information systems that activates in the event of a power outage or disruption ● Lighting should be provided for emergency exits and evacuation routes within the facility
5	Fire Protection	Employ and maintain fire suppression and detection devices or systems for the information systems that are supported by an independent energy source such as UPS. ◆ Moderate: ➢Employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis ◆ High: ➢ Employ fire detection devices and systems that activate automatically and notify emergency responders ➢ Employ fire suppression devices and systems that activate automatically and notify emergency responders ➢ Employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis
6	Temperature and Humidity Controls	Maintain temperature and humidity levels at operational levels within the facility where the information systems reside, and continuously monitor temperature and humidity levels.
7	Water Damage Protection	Protect information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel
8	Delivery and Removal	Authorize, monitor, and control equipment deliveries, moves, and removals from the facility, and maintain records of those moves.
9	Alternate Worksite	At alternate work sites, employ IT controls, such as a logical and physical access controls, as necessary.
10	Location of Information Asset Components	Position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
11	Annual Testing	Test environmental systems and emergency sources at least annually to ensure continuous protections are in place.

8. Network Management and Security

The purpose of this policy is to establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of Bank's information handled by computer networks such as Internet / Intranet / LAN / WAN / External-related systems that are required to be served the interest of organization.

This policy applies to all networks, both the perimeter and the infrastructure, and the parties with which do businesses.

Business associates and any individual who are accessing the bank's information system must cooperate to protect the network by securing computers and network devices in order to secure access. In addition, they must certify that the devices connecting to the business unit's network are in compliance with the policies and procedures as established by Bank's IT Department.

The following rules define the policy regarding access to the Bank's network:

Only authorized people can gain access to bank's networks. Positive identification is required for system usage. All users must have their identities positively identified with user-IDs and secure passwords--or by other means that provide equal or greater security prior to being permitted to use bank owned computers.

User-IDs must each uniquely identify a single user. Each computer user-ID must uniquely identify only one user, so as to ensure individual accountability in system logs. Shared or group user-IDs are not permitted.

Access controls required for remote systems connecting to production systems. All computers that have remote real-time dialogs with bank IT production / test environment systems must run an access control package approved by bank's IT Department.

All log-in banners must include security notice. Every log-in screen for multi-user computers must include a special notice. This notice must state:

(1) the system may only be accessed by authorized users,
(2) users who log-in represent that they are authorized to do so.
(3) unauthorized system usage or abuse is subject to penalties, and
(4) system usage will be monitored and logged.

Security notice in login banner must not disclose system information. All log-in banners on network-connected bank computer systems must simply ask the user to login, providing terse prompts only where essential. Identifying information about the organization, operating system, system configuration, or other internal matters must not be provided until a user's identity has been successfully authenticated.

Users must log off before leaving sensitive systems unattended. If the computer system to which users are connected or which they are currently using contains sensitive information, and especially if they have special access rights, such as domain admin or system administrator privileges, users must not leave their computer, workstation, or terminal unattended without first logging-out, locking the workstation, or invoking a password-protected screen saver.

Operational, Administrative, and Supporting Technology Services' staff must:

THE KANNUR CO-OPERATIVE URBAN BANK LTD No.1534
H.O.
KANNUR
-670002

a. Follow policies and procedures, as established by IT Department, to validate firewall activation, operating system installation, application software security patches and virus protection updates for all devices in the unit's areas of physical or administrative control that are to be, or are configured to utilize network resources that are controlled and managed by IT Department.

b. Follow policies and procedures, as established by IT Department, for using automated tools to test devices connected to the business unit's local wired or wireless data network for compliance. Non-compliant devices are to be disconnected, disabled or quarantined until the device is brought into compliance. When devices are not compliant, operating units, or individuals and their information technology staff must employ compensating controls. Units must document compensating controls and/or any exceptions. These must be reviewed, tested, and approved by CSSC.

c. The operating business unit or individual must retain the approved documentation for audits as long as the device is in operation. Any connection to the Internet, or to a national or regional network from a private network operated by an operational, administrative, or support unit, must be made via bank's network resources. The IT Manager must approve any exceptions to this requirement.

All network access attempts (success or failure) must be logged and retained for auditing.

Server

This policy applies to all servers that bank's IT Department is responsible to manage. This explicitly includes any system for which IT Department has an obligation to administer. IT Department is responsible for system administration, network administration, IT department operational management, data management, digital media management, digital marketing management and must manage all internal and external servers. Approved server configuration guides must be established and maintained by the operational group, based on business needs and approved by CSSC. IT department Operational team should monitor configuration, compliance and implement an exception policy tailored to their environment. Each operational team must establish a process for changing the configuration guides, which includes review and approval by CSSC.

Servers Register must be kept, at a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable

Each device must meet the following minimum standards prior to, and after connecting to the data network or support infrastructure:

- The device must be guarded by an up-to-date and active firewall set to protect it from unauthorized network traffic.
- Current operating system and application software with current security patches must be installed.
- The device must be protected against malicious or undesired software such as viruses, spyware, or adware.
- Access to the device must require appropriate authentication controls such as account identifiers and robust passwords.
- The device must be certified and registered by CSSC as equipment that has met all security criteria, prior to connecting to the network.

Server General Configuration Guidelines

The following items serve as provisioning configuration guidelines for the servers that are managed by CSSC members:

- Operating System configuration should be in accordance with CSSC approved guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as Transmission Control Protocol (TCP) Wrappers.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is available.
- Do not use administrator account when a non-privileged account can performed the task.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from being operated in uncontrolled cubicle areas.

Internal network addresses must not be publicly released.

The internal system addresses, configurations, and related system design information systems and users outside the bank's internal network cannot access this information.

All Internet Web servers must be firewall protected.

All connections between bank's internal networks and the Internet (or any other publicly-accessible computer network) must be protected by a router, firewall, or related access controls approved by CSSC.

Inhouse public servers on Internet must be placed on separate subnets or De-Militarized Zone (DMZ). Internally hosted public Internet servers must be placed on subnets separate from internal networks. It can be either in DMZ or separate subnets. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

ROUTER

This policy describes a required minimal security configuration for all routers and switches connecting to the bank's network.

All routers within bank's organization must meet the following configuration stand

- Any user accounts and its authentication are required to be configured on routers must use industry standard methods or standards defined by CSSC.
- The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization

All routers within bank must disallow the following:

- IP directed broadcast. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
- TCP small services
- UDP small services
- All source routing
- All web services running ~~on~~ router

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No. 1534 H.O. KANNUR -670002

Any external network connections, inbound or outbound, must be authenticated or secured via approved standards.

Before users reach a log-in banner, all inbound lines connected to bank's internal networks and/or computer systems must pass through an additional access control point, such as a firewall, which has been approved by CSSC. Unless CSSC has first approved the action in writing, Bank's staff must not enable any trusted host relationships between computers connected to the Bank's internal network.

Use Enterprise standardized SNMP (Simple Network Management Protocol).

Routers must be included in the Enterprise Management System with a designated point of contact. Users must have explicit permission by CSSC to access or configure any router. All activities performed on these devices may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on these devices.

Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

FIREWALL

The firewall policy dictates how the firewall should handle application traffic. The policy describes how the firewall is to be managed and updated.

Real-time external network connections require firewalls.

Before reaching a log-in banner, all in-bound real-time external connections to Bank's internal networks and/or multi-user computer systems must pass through an additional access control point such as a firewall, gateway, or access server.

- The functionality of firewalls will be setup to ensure secure Internet connections and the connections to other networks.
- Firewall rule-sets must be created for implementing security controls as they pertain to the handling of applications traffic such as web, email and other business processing.
- Users, who are at remote locations, must verify that firewall appliances are in place to secure their connections to the Internet and Internet Service Providers before establishing the connection with the Bank's network.

Firewall configuration change requires CSSC permission.

Firewall configuration rules and permissible service rules established by IT Security and Disaster Recovery have been reached after evaluation. These rules must not be changed without first obtaining the permission of CSSC Information Security Management.

- The IT Department must monitor incident reports and security websites for information about current attacks and vulnerabilities.
- The firewall policy should be updated as necessary.
- A formal process must be used for managing the addition and deletion of firewall rules.
- The CSSC must ensure that administrators receive regular training in order to stay current with threats and vulnerabilities.

New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the DMZ Equipment Deployment Process.
- Configuration changes must follow the Bank's Change Management Procedures.
- Perform system/application audits prior to the deployment of new services.

Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

Network Management/ Access Requirements

- All networks in bank's environment including branch campus are installed and maintained by IT Department.
- To assure the integrity and availability of network services, networks or other means of communication shall be permitted on bank's facilities.
- No networking equipment (routers, managed switches, DHCP servers, DNS servers, WINS servers, VPN servers, remote access dial-in servers, wireless access points, hardware firewalls – shall be permitted without a written exception from CSSC.
- No device or program that has the potential to disrupt network service to others is permitted on the bank's Network without prior arrangement with CSSC.

Protocol Standards

The management of network protocols shall be performed by information systems administrators and network administrators to assure the efficiency, availability, and security of the common resources, in accordance with the governing Bank's Acceptable Use Policy.

Simple Mail Transfer Protocol (SMTP):

- All email protocol traffic shall utilize the centralized mail gateways. Inbound mail traffic with destination addresses for servers other than those operated by bank's shall utilize a DNS MX record to relay that traffic through the centralized mail gateways. All outbound traffic shall utilize the SMTP gateway.
- The use SSL or TLS based communication standards for email client to email server communication is preferred such that the authentication session is the protected transaction.

Domain Name Services Protocol (DNS):

- All hosts on bank's networks shall utilize the bank's DNS systems. All hosts connected to bank's networks receive a kucb.in domain name extension. No host connected to bank networks shall be addressable by any DNS name other than that provided by the bank.
- No host with a kucb.in domain name (and an IP address within the bank's network spaces) will use an IP address outside the bank's registered name space without a written exemption from IT Department.

Dynamic Host Configuration Protocol (DHCP):

- All hosts on bank's networks shall either obtain and use a static IP address or use the bank's DHCP service to obtain an assigned IP address. Users shall not use a self-assigned IP address, or operate a DHCP server. The use of bootstrap (BOOTP) shall be governed in the same manner as DCHP.

KANNUR CO-OPERATIVE URBAN BANK LTD H.O. KANNUR -670002

Banned Protocols:

- Bank's IT Department keeps a listing of banned protocols which have shown to interfere with the architecture and management of the network environment.

Remote Access

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private key with strong passphrases.
- At no time should any employee provide his or her login or email password to anyone, not even family members.
- Employees and contractors with remote access privileges must ensure that their Bank owned or personal computer or workstation, which is remotely connected to the enterprise network is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Employees, contractors and associates with remote access privileges to the Bank's network must not use non- Bank email accounts or other external resources to conduct Bank's business.
- Routers for dedicated Integrated Services Digital Network (ISDN) lines configured for access to the Bank's network must meet minimum authentication requirements of Challenge-Handshake Authentication Protocol (CHAP).
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time
- Frame relay must meet minimum authentication requirements of Data Link Connection Identifier (DLCI) standards.
- All hosts that are connected to the Bank's internal network via remote access technologies must use the most up-to-date anti-virus software; this includes personal computers.
- Third party connections must comply with requirements as stated in the Third Party Agreement.
- Personal equipment that is used to connect to the network must meet the requirements of Bank's owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the production network must obtain prior approval from CSSC.
- Direct network connections with outside organizations must be approved. The establishment of a direct connection between the Bank's systems and computers at external organizations, via the Internet or any other public network, is prohibited unless this connection has first been approved by the CSSC.
- Inventory of connections to external networks must be maintained. CSSC must maintain a current inventory of all connections to external networks including telephone networks, extranets, the Internet.

VPN

Approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefit of VPN, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.

- When actively connected to the Bank's network, the VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by CSSC.
- All computers connected to the internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the enterprise standard, this includes personal computer.
- VPN users will be automatically disconnected from the network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- Users of computers that are not owned by the Bank must configure the equipment to comply with VPN and Network policies.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the network, and as such are subject to the same rules and regulations that apply to the Bank owned equipment, i.e., their machines must be configured to comply with cyber security Policies.

THE KANNUR CO-OPERATIVE URBAN BANK LTD N° 1534
H.O
KANNUR
-670002

9. Ani-virus and Malicious code Detection

This policy will detail the appropriate measures to take in the event of a virus attack or the discovery of malware on a system or systems. It also highlights the fact that staff must not attempt to circumvent the malicious code detection, prevention and remediation techniques employed and that disciplinary action will be taken against anyone found to be trying to do so.

All computers that are connected to the bank's network must have the standard anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus definition files must be kept up-to-date.

All PC's are to be configured such that they schedule regular updates from the Network Services centralized anti-virus servers.

Any activities with the intention to create and/or distribute malicious programs into bank's network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

Virus-infected computers are removed from the network until they are verified as virus-free.

Portable computers issued and used to house or access bank network or services must have Personal Firewall and Anti-virus.

Non-adherence to the Malicious Code Policy and related policies will result in local disciplinary proceedings being implemented.

10. Internet and Email Policy

Email, and internet usage assigned to an employee's computer is solely for the purpose of conducting bank's business. Some job responsibilities at the bank require access to the internet and only people appropriately authorized, for bank purposes, may use the internet to access. This authorization is generally exclusive to decisions that the IT department makes in conjunction with CSSC.

All email protocol traffic shall utilize the centralized mail gateways. Inbound mail traffic with destination addresses for servers other than those operated by bank shall utilize a DNS MX record to relay that traffic through the centralized mail gateways. All outbound traffic shall utilize the SMTP gateway.

The use SSL or TLS based communication standards for email client to email server communication is preferred such that the authentication session is the protected transaction.

Mailbox should be daily backed

Any device or computer including, but not limited to, desk phones, smartphones, tablets, laptops, desktop computers, and iPads that the bank provides for your use, should only be used for bank business. Keep in mind that the bank owns the devices and the information in these devices. If you leave the company for any reason, the bank will require that you return the equipment on your last day of work.

Internet Usage

Internet use, on bank time, using bank-owned devices that are connected to the bank network, is authorized to conduct bank's business only. Internet use brings the possibility of breaches of the security of confidential bank information.

Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people, outside of the bank, potential access to passwords and other confidential information.

Removing such programs from the bank network requires IT staff to invest time and attention that is better devoted to making technological progress. For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit internet use.

Additionally, under no circumstances may bank owned computers or other electronic equipment, including devices owned by the employee, be used on bank time at work to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

Social Media

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No 1534
H.O.
KANNUR
-670001

We strongly encourage you to limit the use of social media to work-related content and outreach during work hours.

Additionally, you are prohibited from sharing any confidential information or protected information that belongs to or is about the bank.

In social media participation from work devices or during working hours, social media content that discriminates against any age, race, colour, religion, gender, national origin, disability, or genetic information is prohibited.

Any employee, who participates in social media, who violates this policy will lead to disciplinary action.
Email Usage at the Company

Email is also to be used for Company business only. Company confidential information must not be shared outside of the Company, without authorization, at any time. You are also not to conduct personal business using the Company computer or email.

Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste company time and attention.

Keep in mind that the bank owns any communication sent via email or that is stored on company equipment. Management and other authorized staff have the right to access any material in your email or on your computer at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored on work systems.

If you need additional information about the meaning of any of this communication, please reach out to your manager or the IT staff for clarification.

11. Patch Management

IT Department should ensure all servers have appropriate critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate. Patches must be applied to all software on the organization network where appropriate.

IT Department will adhere to the organization's Patch Management Procedure and keep a full record of which patches have been applied and when.

Controls against Malicious and Mobile Code

- Mobile code represents newer technologies often found in web pages and emails, and includes, but is not limited to:
- ActiveX.
- Java.
- JavaScript.
- VBScript.
- Macros.
- HTTPS.
- HTML.

The bank IT Department will put in place appropriate access controls (e.g. administration / user rights) to prevent installation of software by all users in order to prevent malicious and mobile code.

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No. 1534 *
H.O.
KANNUR
-670002

12. Removable Media

The is policy is related to the use of removable media in the bank IT infrastructure. The use of removable media devices will only be approved if a valid business case for its use is exist. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to IT department Approval for their use must be given by the CSSC.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

All removable media devices and any associated equipment and software must only be purchased and installed by IT Services. No other removable media devices **must not** be used to store any banking information or confidential information related to the bank

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted

Users should be aware that the bank will audit / log the transfer of data files to and from all removable media devices and bank owned IT equipment.

Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to IT department.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to IT department.

Damaged or faulty removable media devices must not be used. The data must be scanned by two functionally different virus checking software products, before the media is loaded on to the receiving machine.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity.

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the bank or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to IT department.

Special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with bank equipment or the network or to hold information used to conduct official banking business **must** only be purchased and installed by IT department. Any removable media device that has not been supplied by IT **must not** be used.
- All data stored on removable media devices **must** be encrypted where possible.
- Virus and malware checking software **must** be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices **must not** to be used for archiving or storing records as an alternative to other storage equipment.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

If any user is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

13. Risk Assessment Policy

To establish a process to manage risks to the Bank that result from threats to Data and Information Systems.

Cyber Security requirements shall be determined through a methodical assessment of risks. CSSC shall then balance the costs associated with implementing cyber security controls and mechanisms against the potential harm that could result from a security failure. When conducting risk assessments the following must be considered:

- Harm to the business as a result of a security failure, considering potential consequences of a loss of confidentiality, integrity and/or availability of information or other assets.
- The likelihood of a failure occurring in light of existing threats and vulnerabilities, and the security controls and mechanisms implemented in the Bank system environment.

Periodic reviews of information security risks and the implemented controls and mechanisms will be conducted annually to:

- Address changes to business requirements and priorities
- Consider new threats and vulnerabilities that might exist
- Confirm that security controls and mechanisms remain effective and efficient.
- Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.
- Each Information System must have a system security plan, prepared using input from risk, security and vulnerability assessments.

Responsibilities

1. Senior Manager IT is responsible for ensuring that the entire organization conducts Risk Assessment on Information System and uses the Bank approved process.
2. Information System Owners (ISOs) are responsible for ensuring that information systems under their control are assessed for risk and that identified risks are mitigated, transferred or accepted.
3. The IT Manager is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

14. Backup and Restoration policy

Bank recognizes that the backup and maintenance of data for servers are critical to the viability and operations. It is essential that certain basic standard practices be followed to ensure that regular back up of essential information and data should be taken for restoration of the system in case of disaster, system crash or data loss due to users' mistakes.

This policy is intended to provide details on the stipulations of data backup and retrieval operations. The purpose covers:

- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

This policy applies to all critical data from all departments and branch locations.

Systems will be backed up according to the schedule below:

Incremental backup of daily and Full backup weekly.
Mail server Mailbox will be daily backed
Configuration backups of critical system will be updated monthly or when changes occurs.

Backup will be and stored as described below:

All backups should be written to media with necessary capacity
Media will be clearly labeled and stored in a secure area that is accessible only to IT employees of the Bank.
During transport or changes of media, media will not be left unattended.
Daily backups will be stored on-site in a physically secured fire-proof safe located in a building separate from the Data Center.
Weekly backups will be stored in a physically secured, off-site media vaulting location as defined in the process of the Backup policy.

Prior to retirement and disposal of media, IT will ensure that:
The media no longer contains active backup images
The media's current or former contents can not be read or recovered by an unauthorized party.
The physical destruction of media prior to disposal.

Backups will be verified periodically.
On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimize backup performance where possible.

IT will identify problems and take corrective action to reduce any risks associated with failed backups.

Random test restores will be done once a week in order to verify that backups have been successful

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No.1534
H.O
KANNUR
-670002

IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

Data Recovery

In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.

In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made to IT Department,

Backup copies must be stored in an environmentally protected and access controlled secure offsite location.

Stored copies must be made available upon authorized request.
A record of the physical movements of all backup copies shall be maintained.

The IT Manager shall develop procedures for the handling and storage of information in order to prevent unauthorized disclosure, misuse or loss.

Backup copies are to be maintained in accordance with the Department's Retention and Disposal Schedule for backup copies.

All backup media shall be appropriately disposed.

15. Vendor /Outsourcing and Risk Management

Bank shall comply with security requirements while procuring, acquiring, and developing and maintaining new information system.

The policy ensure that security is an integral part of Bank's Information Systems throughout all phases of the acquisition, development, and maintenance lifecycle. Security must be considered at every stage of an information system's life cycle (e.g. feasibility, planning, development, implementation, maintenance, retirement and disposal) in order to:

- Ensure conformance with all appropriate security requirements
- Protect enterprise data throughout its life cycle
- Facilitate efficient implementation of security controls
- Prevent the introduction of new risks when the system is modified
- Ensure proper removal of data when the system is retired

Capacity Management:

- The use of information resources shall be planned, prepared, and monitored, and projections shall be made of future capacity requirements to ensure adequate performance.
- Procedures shall be developed to respond to audit log storage capacity issues according to the Audit Logging and Monitoring policy.

Business Requirements for New Information Systems:

- Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems, shall specify requirements for security controls.
- In acquiring new information systems and/or contracting with new vendors, Bank will ensure that the systems/entities are of high reputation and at least similar caliber to the current health information exchange vendors and that all such relationships comply with the terms of the Bank Policies.
- Security controls in business requirements shall include:
  - Consideration of business value and legal-regulatory-certificatory standards for information assets affected by the new/changed system.
  - Consideration of administrative, technical, and physical controls available to support security for the information system.
  - Integration of security controls early in requirements specification and system design.

Input Data Validation:

- Data input to applications and databases shall be validated to ensure that the data is correct and appropriate. Both automatic and manual methods of data input validation testing shall be used as appropriate.
- Bank shall define data input validation procedures.
- Bank shall define secure coding guidelines to prevent common vulnerabilities during software development.
- Bank shall develop system and information integrity procedures.

THE KANNUR CO-OPERATIVE URBAN BANK LTD.No.1534
H.O.
KANNUR
-670002

- Bank shall include data input validation checks in testing methodologies. Where possible data input validation testing shall be automated through use of tools or other non-manual methods.
- Applications developed by Bank or third parties shall be based on secure coding guidelines and shall undergo testing.
- Applications that store, process, or transmit confidential data shall undergo application vulnerability testing by a qualified third party at least annually.
- Third party vendors shall comply with vulnerability testing requirement and provide Bank reports in accordance with the Bank Audit Logging and Monitoring Policy.

Control of Internal Processing:

- Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
- Bank shall define integrity controls and develop a validation checklist.

Message Integrity:

- Requirements for ensuring authenticity and protecting message integrity in applications shall be identified.
- Message integrity controls shall be identified and implemented.

Output Data Validation:

- Data output from applications and databases shall be validated to ensure that the processing of stored information is correct and appropriate. Both automatic and manual methods of output data validation testing shall be used as appropriate.
- Bank shall define output data validation procedures.

Control of Production Software:

- Bank shall implement procedures to control the installation of software on production/operating systems to minimize the risk of interruptions to, or corruption of those systems.
- To minimize the risk of corruption to operational systems, the following procedures shall be implemented:
  - Only authorized System Administrators shall be allowed to implement approved upgrades to software, applications and program libraries
  - Production systems shall only hold approved programs or executable code (i.e., no development code or compilers).
- Third party software used in production systems shall be maintained at a level supported by the vendor.
- If systems in production are no longer supported by the vendor, Bank must provide evidence of a formal migration plan and obtain CSSC approval to implement the plan.
- Applications and production/operating systems shall be tested for usability, security, and impact prior to release in production.
- Production software must comply with the Change Management Policy and Configuration Management Policy.
- Physical or logical access shall be given to a third party for support purposes only when necessary, and only with senior leadership approval. The vendor's activities shall be monitored.

Protection of Test Data:

- Test data shall be selected carefully, and appropriately logged, protected and controlled.
- The use of operational databases containing confidential data for non-production (e.g., testing) purposes shall be avoided. If confidential data or internal use only data must be used for testing purposes, all sensitive details

and content shall be removed or modified beyond recognition (de-identified) before use.

- Bank shall establish controls and procedures to protect test data, test systems, and testing environments.

Access Control to Program Source Code:

- Access to program source code and associated items (e.g., designs, specifications, verification plans, validation plans, etc.) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

Outsourced Software Development:

- The development of software by third parties shall be done under the supervision of CSSC.
- The development of software by third parties shall be governed by a contract or a Service Level Agreement (SLA) that includes security requirements.
- Independent security and code reviews shall be conducted by an individual with certified security training before bringing new services into production.

E-commerce applications

E-commerce applications must be supported based on a flexible, scalable architecture, typically consisting of:

- Front-end web servers
- Mid-tier applications servers
- Back-end database servers and back-office servers

All electronic trading facilities provided to investors and other third parties must use secure session protocols such as SSL to encrypt sessions between browsers and web server to prevent sensitive data (e.g. account details) being intercepted. Strong encryption to protect sensitive data (personal information, credit card details) stored on servers or other systems that might be vulnerable to external access.

No confidential investor information may be stored directly on web servers. Web servers must be physically separate from database servers, and must reside on separate network segments.

All communication between web servers and other components of electronic trading systems must be subjected to firewall mediation and IDS/IPS inspection.

Roles and Responsibilities

CSSC Coordinator - Ensures the application of appropriate operational security controls for an information system; coordinates in the identification, implementation, and assessment of common security controls; plays an active role in developing and updating a system security plan and coordinating with an information system owner any changes to the system and assessing the security impact of those changes. This role may be filled by someone directly involved with the development, maintenance, and/or operation of the information system.

THE KANNUR CO-OPERATIVE URBAN BANK LTD. No.1534
H.O
KANNUR
-670002

16. Business Continuity policy

Business continuity management process shall be implemented by Bank to reduce the disruption caused by disaster and security failures to an acceptable level through a combination of preventive and recovery controls.

Business Continuity management process shall be developed and shall address the information security requirements for business continuity. CSSC has the responsibility of business continuity management. Managed process should be in place for developing and maintaining business continuity throughout Bank.

Business continuity Risk assessment and Development

The events that can cause interruptions to business processes shall be pre identified and shall be followed by a risk assessment to determine the impact of interruptions. Plans shall be developed to maintain or restore operations in the required time scale.

Plan Maintenance

Business Continuity plans should be tested regularly to ensure that they are up to date and effective. Business continuity plans should be maintained by regular reviews and updates to ensure their continuing effectiveness.

Principles and Commitments

The Business Continuity Policy shall be based on the following principles and commitments:

17. The protection and safety of people shall be the first premise and ultimate objective of this Policy, both under normal circumstances and during a crisis resulting from a disaster.
18. The designation of representatives in the various areas with appropriate experience and knowledge to actively participate in the preparation, implementation, review, verification and amendment of the Business Continuity Plans.
19. The development and implementation of Business Continuity Plans by Bank, taking into account the internal areas and departments, suppliers and services and using adequate and proportionate systems, resources and procedures.
20. The maximisation of the synergies generated through the development and implementation of the Business Continuity Plans in the organization, taking into consideration Bank common means and resources.
21. 5. The adoption of reasonable measures to ensure the operational continuity of processes and activities, based on their criticality as established by the Organization.
22. 6. The inclusion of safety and reliability criteria which reasonably ensure the continuity of the critical services provided by third parties, should said services be outsourced.
23. 7. The preparation, within the Business Continuity Plans, of appropriate communication procedures, both internal and external, which ensure their correct execution and timely delivery of information to all the interested parties.

24. 8. The communication to all the employees of their responsibilities and the procedures that may affect them, within the business continuity framework and through dissemination and training activities.
25. 9. The development of a Business Continuity Management System which includes reviews, verifications and amendments of the Business Continuity Plans, either on a regular basis or when significant changes arise, with the aim of continuously improving them.
26. 10. The constant willingness to cooperate with the authorities in case of disaster or need, as part of the spirit of service that inspires all Bank activities and its responsibility towards the business in which it operates.

Responsibilities

The CSSC shall be responsible for promoting the development and implementation of the Business Continuity Plans of the Bank, establishing and coordinating business continuity activities, while ensuring the enforcement, dissemination and periodic revision of this Policy.

Likewise, said Committee shall assume the executive direction and management of those crises resulting from a disaster, which have a global or multi-entity impact, require extraordinary economic investments or may significantly affect the reputation of the Bank

All other responsibilities related to Business Continuity management shall be further detailed in Bank's Business Continuity process.

17.Incident Management Policy

Incident response process must be documented. Incident response plan must be tested for effectiveness through appropriate means such as simulation exercises.

Information security incidents reporting.

Information security incident management process shall be developed, which shall address the information security requirements. Any event related to information security shall be reported and available for further analysis.

Employees shall report all security weaknesses and software malfunction to IT department.

All employees and customers should be aware of the procedures of reporting the incidents like security breach, threat weaknesses or malfunction that might have an impact on the information security.

Investigation

Information Technology department should conduct thorough investigations into the root cause of each security incident to:

- Reprimand, discipline or prosecute those responsible
- Update existing security controls or to introduce new ones to prevent a recurrence of the same incident

Review

Incident response plans and procedures must be reviewed on annual basis.

18. Compliance Policy

This policy will enforce the legal requirements that shall be considered to design, operate, use and management of information systems and to abide statutory, regulatory and contractual security requirements.

Compliance with Legal Requirement

Bank shall identity and analyze external regulatory requirements for their impact on its IT function, and take appropriate measures to comply with them.

The following areas shall be covered:

- Regulators including RBI and other governing body authorities guidelines, especially relating to business trading, e-commerce, information security etc.
- Relevant government and/or external requirements (i.e., laws, legislation, guidelines, regulations and standards) pertaining to external relationships and external requirements reviews
- Labour laws, especially addressing IT related safety and health (including ergonomics) requirements
- Compliance issues relating to IT
- Privacy issues especially pertaining to customer related information
- Intellectual property rights / software copyright laws
- Information systems security requirements, especially relating to use of cryptographic data, and transmission of data
- Relevant 'accounting standards/ pronouncements' relating to electronic commerce

Identification of applicable legislation

All relevant statutory, regulatory, contractual requirements and responsibilities to meet them shall be defined and documented. Monitoring of local legislation and regulations affecting the companies operations should be done by compliance department.

Intellectual Property Rights (IPR)

Intellectual property rights such as copyright, design rights, trademarks shall be abide. Non licensed copy of product should not be used. Strong disciplinary action should be taken against any person engaged in the unauthorized copying of software. In addition, any penalties imposed on the company as a result of the breach should be passed on the offending individual.

Software Copyright

Software products shall be used as per the terms and conditions in license agreement. Proprietary software products are usually supplied under a license agreement that limits the use of the product to specified machines and may limit copying to the creation of back-up copies only. All software used within the bank should be purchased and issued in accordance with the license agreements. The company will take strong disciplinary action against any person found to be engaging in the unauthorized copying of software.

Personal Information

Compliance with local legislation governing the protection of personal information in the jurisdictions covered by the e-commerce application should be identified and followed and must ensure that any personal information collected about investors is used only in ways associated with the company business.

Customer log-on credentials and transactional data traversing public networks must be encrypted by means of commercial grade encryption i.e. at least 128-bit SSL type encryption or equivalent standard.

Protection of Organizational Records

Important records of Bank shall be protected from loss, destruction and falsification. Records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Media used for storage of records should be secured from degradation and should have clear identification of their statutory or regulatory retention period.

Data protection and privacy of personal information
Bank shall determine the applicable regulations and implement appropriate controls for each applicable jurisdiction to reasonably protect the privacy of personal information.

Compliance with data protection legislation requires appropriate management structure and control to ensure the privacy and confidentiality of investor's related information.

Res. No: 32/19-20
Date 19.12.2019
PASSED
Chairman

Res. No: Audit Co/1
Date 5.5.2026.
PASSED
Chairman

Res. No: Audit Sub Co/2
Date 23.4.2021.
PASSED
Chairman

Res. No: Audit Co.
Date 18.4.2022.
PASSED
Chairman