KERALA STATE BACKWARD CLASSES DEVELOPMENT CORPORATION LIMITED

KSBCDC

(Information Technology Policy / Information Technology Strategic Committee / Information Security Policy / Business Continuity Plan)

Adopted by BOD Meeting No. 257 Date: 14.11.2025

Prepared by: Remya. C B. Com, FCA DISA
Membership No. 226650
Partner, A U R J & Associates (FRN No: 004972S)

Regd. Office: T.C. 27/588 (7) & (8), "SENTINEL", 2nd Floor, Pattoor, Vanchiyoor P.O.,
Thiruvananthapuram - 695 035. Phone: 0471-2577539, 2577550. Fax: 0471 2577539.
e -mail: ksbcdc@ksbcdc.com Web: www.ksbcdc.com
"Freedom from poverty and backwardness"

TABLE OF CONTENTS:

INFORMATION TECHNOLOGY POLICY

TABLE OF CONTENTS:

1. About the Information Technology Policy

Kerala State Backward Classes Development Corporation Ltd (herein after referred as KSBCDC Ltd or the company) provides and maintains technological products, services and facilities like Personal Computers (PCs), peripheral equipment, servers, telephones, Internet and application software to its employees for official use. The Information Technology (IT) Policy of the organization defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the employees pertaining to technological assets and services used for office work.

a. Purchase

1) The Procurement Department’s procedures & guidelines need to be followed to purchase new technological equipment, services, software for official purposes.

2) All approved equipment, services or software will be purchased through the Procurement Department unless informed / permitted otherwise.

3) The IT Department will assist the Procurement Department while evaluating the best and most cost-effective hardware or software to be purchased for a particular department / project / purpose based on the requirement. The IT Department will also make sure all hardware / software standards defined in the IT policy are enforced during such purchases.

4) Complete details related to purchase of technological equipment, services or software can be found in the Procurement Policy Manual.

b. *Compliance*

1) All employees are expected to comply with the IT Policy’s rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the organization.

2) Any employee who notices misuse or improper use of equipment or software within the organization must inform his / her Reporting Manager(s) immediately.

3) Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the Management Committee of the organization.

c. *Employee Training*

1) Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software.

2) Employees can request and / or the Management Committee can decide to conduct IT training on a regular or requirement basis.

d. IT support

1) KSBCDC Ltd uses an email system to register IT-related complaints.

2) Employees may need hardware / software installations or may face technological issues which cannot be resolved on their own. Employees are expected to get help from the IT Department for such issues via the IT support email ID only.

3) Any IT support work informed or assigned via emails sent on employee personal email IDs, chats or any other media except the IT support email ID would not be entertained.

4) For the sake of quick understanding, employees are expected to provide details of their issue or help required in the support email sent.

5) For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all employees to inform the IT Department.

6) For any damage to Personal Computers, approval from the Reporting Manager would be required for PC replacements.

7) After raising complaints / queries, employees should expect a reply from the IT Department within 1 working day. The IT Department may ask the employee to deposit the problematic equipment to the IT Department for checking and will inform the timeline for repair / maintenance / troubleshooting / installations or the required work.

8) If there is no response in 1 working day, then the IT Department designated staff should be asked for an explanation for the delay by the respective senior head of the department from which the query was raised. If no response is obtained in 3 working days, a complaint can be raised through an email to the employee’s Reporting Manager and IT Department designated staff.

9) Queries will be resolved on a first-come-first-serve basis. However, the priority can be changed on request at the sole discretion of the designated team in the IT Department.

2. Equipment Usage Policy

a. Objective

The Equipment Usage policy informs employees and managers about equipment purchase, organizational and project-level inventory management, rules for allocating & transferring equipment to employees, departments or projects and best practices for all equipment usage and maintenance.

b. Equipment Purchase

1) The following equipment is purchased by the organization and provided to individual employees, departments or projects for their official use. The list can be modified as and when required.
    - Personal computing devices (desktop, laptop, tablet)
    - Computer peripherals (printer, scanner, photocopier, fax machine, keyboard, mouse, web camera, speaker, modem etc.)

- Networking equipment & supplies (router, switch, antenna, wiring etc.)
- Cell phones
- Biometric devices

2) The Procurement Department's procedures and guidelines need to be followed to purchase new equipment for official purposes. All approved equipment will be purchased through the Procurement Department unless informed / permitted otherwise.

3) The Procurement Department will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders.

c. Inventory Management

1) The Procurement Department is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the organization

2) The following information is to be maintained for above mentioned assets in an Inventory Sheet:

   a. Item
   b. Brand / Company Name
   c. Serial Number
   d. Basic Configuration (e.g. HP Laptop, 120 GB HD, 2 GB RAM etc.)
   e. Physical Location
   f. Date of Purchase
   g. Purchase Cost

h. *Current Person In-Charge*

3) Proper information about all technological assets provided to a specific department, project or centre must be regularly maintained in their respective Inventory Sheets by an assigned coordinator from that department, project or centre on a regular basis. The information thus maintained must be shared with the Procurement Department as and when requested.

4) When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.

5) All technological assets of the organization must be physically tagged with codes for easy identification.

6) Periodic inventory audits will be carried out by the IT Department to validate the inventory and make sure all assets are up-to-date and in proper working conditions as required for maximum efficiency and productivity.

d. Equipment Allocation, De-allocation & Relocation

1) Allocation of assets:

    a. *New employees may be allocated a personal computer (desktop or laptop) for office work on the Day of Joining as per work requirement.*
    b. *If required, employees can request their Reporting Manager(s) for additional equipment or supplies like external keyboard, mouse etc.*

   c. *Allocation of additional assets to an employee is at the sole discretion of the Reporting Manager(s).*
   d. *No employee is allowed to carry official electronic devices out of office without permission from the Reporting Manager.*

2) De-allocation of assets:

   a. *It is the Reporting Manager's responsibility to collect all allocated organizational equipment and other assets from an employee who is leaving the organization.*
   b. *Updating the inventory sheet is mandatory after receiving back all allocated equipment.*
   c. *The received assets must be returned back to the Admin Department.*

e. Equipment Usage, Maintenance and Security

1) It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and / or being used by them.

2) Proper guidelines or safety information must be obtained from designated staff in the IT Department before operating any equipment for the first time.

3) Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff in the IT Department.

4) Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.

5) If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from the Reporting Manager is required for the same. The malfunctioning device needs to be submitted to the IT Department for checking, maintenance or repair. The IT Department staff person will give a time estimate for repair / maintenance.

6) The Reporting Manager can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT Department. The issue will then be resolved by the Reporting Manager in consultation with the IT Department Head. The management committee can be consulted in terms of serious disputes or unresolved issues.

f. Phone Usage Policy

1) Landline phone systems are installed in the organization’s offices to communicate internally with other employees and make external calls.

2) The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.

3) Long distance calls should be made after careful consideration since they incur significant costs to the organization.

4) The Admin Department is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted.

5) Employees should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization’s phone services.

3. <u>Personal Computer (PC) Standards</u>

a. Objective

The main aim of this policy is to maintain standard configurations of PC hardware and software purchased by the organization and provided to employees for official work. The hardware standards will help maintain optimum work productivity, computer health & security and provide timely and effective support in troubleshooting PC problems. The software standards will ensure better system administration, effective tracking of software licenses and efficient technical support.

b. General Guidelines

1) It is the responsibility of the IT Department to establish and maintain standard configurations of hardware and software for PCs owned by the organization. The standard can, however, be modified at any point in time as required by the IT Department Head in consultation with the Management Committee.

2) Multiple configurations are maintained as per the different requirements of various departments and projects in the organization, in consultation with the Department / Project Head.

3) Only in exceptional cases, when none of the standard configurations satisfy the work requirements, can an employee request a non-standard PC configuration. Valid reasons need to be provided for the request and written approval of the Reporting Manager(s) is required for the same.

c. Network Access

1) All PCs being used in the organization are enabled to connect to the organization's Local Area Network as well as the Internet.

2) Network security would be enabled in all PCs though Firewall, Web Security and Email Security software.

3) Employees are expected to undertake appropriate security measures as enlisted in the IT policy.

d. Data Backup Procedure

1) Data backup is set up during installation of the operating system in a PC. As an additional security measure, it is advised that employees keep important official data in some external storage device also.

2) File backup system:

   a. *The organization will be installing a file server for backing up data of all employees. All employees are expected to keep official data on the file system.*
   b. *Employee's Reporting Manager or the Management Committee or the IT Manager will have access to that data.*
   c. *All employees will login to the file server through user ID and password.*

3) Server backup:

   a. *The IT Department is expected to maintain an incremental backup of all servers such as punching server and tally server with at least 3 copies of all servers. At any time, 3 backups of all servers must be maintained.*
   b. *Replica mode of all running servers will be offline and it should maintain half-hourly backup.*

e. Antivirus Software

1) Approved licensed antivirus software is installed on all PCs owned by the organization.

2) Two configurations - basic and advanced are maintained for antivirus software installed on organization's computers. The configurations are installed on PCs as per work requirement of a particular department / project.

3) Employees are expected to make sure their antivirus is updated regularly. The IT Department should be informed if the antivirus expires.

4) Any external storage device like a pen drive or hard disk connected to the PC needs to be completely scanned by the antivirus software before opening it and copying files to / from the device.

f. PC Support

1) Guidance and tips given by the IT Department designated staff for maintaining the PC should be remembered while using a PC.

2) The IT Department should be contacted via the IT support email for any assistance with the PC hardware or software.

3) Technical support will not be provided for hardware devices or software which are personally purchased, illegal or not included in the standard hardware / software list developed by the IT Department.

4) Software applications evaluated by the IT Department to cause problems with the organization’s PCs will be removed.

4. <u>Internet Usage Policy</u>

a. Objective

The Internet Usage Policy provides guidelines for acceptable use of the organization’s Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the employees.

b. General Guidelines

1) The Internet is a paid resource and therefore, shall be used only for office work.

2) The organization reserves the right to monitor, examine, block or delete any / all incoming or outgoing Internet connections on the organization’s network.

3) The organization has systems in place to monitor and record all Internet usage on the organization’s network including each website visit and each email sent or received. The Management Committee can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.

4) The organization would install an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.

c. Internet Login Guidelines

1) All employees would be provided with a Username and Password to login to the Internet network in the office and to monitor their individual usage.

2) An employee can also get a local static IP address for internet and intranet use. All employees would be responsible for the internet usage through this local static IP.

3) Username and password for a new employee must be requested by the immediate reporting manager.

4) Sharing the username and password with another employee, visitor or guest user is prohibited.

5) A visitor or guest user who wants to use the office Internet will be given a guest username and password.

6) The IT Department will define guidelines for issuing new passwords or allowing employees to modify their own passwords.

7) Any password security breach must be notified to the IT Department immediately.

8) Username and password allotted to an employee will be deleted upon resignation / termination / retirement from the organization.

d. Password Guidelines

The following password guidelines can be followed to ensure maximum password safety -

1) Select a good password:

    a. *Choose a password which does not contain easily identifiable words (e.g. username, name, phone number, house location etc.)*
    b. *Use 8 or more characters.*
    c. *Use at least one numeric and one special character apart from letters.*

d. *Combine multiple unrelated words to make a password.*

2) Keep the password safe:

   a. *Do not share the password with anyone.*
   b. *Make sure no one is observing while entering the password.*
   c. *As far as possible, do not write down the password. If it needs to be written down, do not display it in a publicly visible area.*
   d. *Change the password periodically (every 3 months is recommended).*
   e. *Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.*

3) Other security measures:

   a. *Ensure the computer is reasonably secure in the user's absence.*
   b. *Lock the monitor screen, log out or turn off the computer when not at the desk.*

e. Online Content Usage Guidelines

1) Employees are solely responsible for the content accessed and downloaded using the Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.

2) During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.

3) Employees are not allowed to use the Internet for non-official purposes using the Internet facility in the office.

4) Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

f. *Inappropriate Use*

The following activities are prohibited on the organization's Internet network. This list can be modified / updated any time by the Management Committee as deemed.

Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below -

1) Playing online games, downloading and / or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth.

2) Downloading images, videos and documents unless required to official work.

3) Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work.

4) Accessing pirated software, tools or data using the official network or systems.

5) Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee.

6) Engaging in any criminal or illegal activity or violating law.

7) Invading privacy of co-workers.

8) Using the Internet for personal financial gain or for conducting personal business.

9) Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.

10) Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization’s reputation.

5. <u>Information Security Policy</u>

a. Objective

Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization’s information systems.

b. General Guidelines

1) Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.

2) Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.

3) Appropriate training must be provided to data owners, data users and network & system administrators to ensure data security.

c. Data Classification

1) The organization classifies data into three categories:

    a. *High risk - it includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure (e.g. payroll, personnel, financial, biometric data).*
    b. *Medium risk - it includes confidential data which would not impose losses on the organization if disclosed, but is also not publicly available (e.g. agreement documents, unpublished reports etc.)*
    c. *Low risk - it includes information that can be freely disseminated (e.g. brochures, published reports, other printed material etc.)*

2) Different protection strategies must be developed by the IT Department for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.

3) High risk data must be encrypted when transmitted over insecure channels.

4) All data must be backed up on a regular basis as per the rules defined by the IT Department at that time.

d. Access Control

1) Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.

2) All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.

3) Default passwords on all systems must be changed after installation.

4) Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.

e. Virus Prevention

1) Virus prevention for personal computers and email usage has been described previously.

2) Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.

3) Whenever feasible, system / network administrators must inform users when a virus / other vulnerability has been detected in the network or systems.

f. Intrusion Detection

1) Intrusion detection shall be implemented on all servers and workstations containing high and medium risk data.

2) Operating system and application software logging process must be enabled on all systems.

3) Server, firewall and critical system logs must be reviewed frequently.

6. <u>Email & Chat Policy</u>

a. Objective

This policy provides information about acceptable usage, ownership, confidentiality and security while using electronic messaging systems and chat platforms provided or approved by the organization. The policy applies to all electronic messages sent or received via the above-mentioned messaging systems and chat platforms by all official employees of the organization.

b. General Guidelines

1) The organization reserves the right to approve or disapprove which electronic messaging systems and chat platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for office use only.

2) An employee who, upon joining the organization, is provided with an official email address should use it for official purposes only.

3) Any email security breach must be notified to the IT Department immediately.

4) Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned / provided by the organization.

5) All messages composed and / or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication.

6) Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.

7) All email signatures must have appropriate designations of employees and must be in the format approved by the Management Committee.

c. Ownership

1) The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the organization.

2) The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.

3) The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate.

4) IT administrators can change the email system password and monitor email usage of any employee for security purposes.

d. Confidentiality

1) Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Reporting Manager(s) and / or the Management Committee.

2) Caution and proper judgement should be used to decide whether to deliver a message in person, on phone or via email / electronic messaging systems.

3) Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
4) Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

e. Email security

1) Anti-virus:

   a. Anti-virus software pre-approved by the Department Head - IT should be installed in the laptop / desktop provided to a new employee after joining the organization.
   b. All employees in the organization are expected to make sure they have anti-virus software installed in their laptops / desktops (personal or official) used for office work.
   c. The organization will bear responsibility for providing, installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop provided by the organization. The employee is responsible for installing good quality anti-virus software in their personal laptop / desktop used for office work.
   d. Employees are prohibited from disabling the anti-virus software on organization provided laptops / desktops.
   e. Employees should make sure their anti-virus is regularly updated and not out of date.

2) Safe Email Usage:

Following precautions must be taken to maintain email security -

a. Do not open emails and / or attachments from unknown or suspicious sources unless anticipated by the user.

b. In case of doubts about emails / attachments from known senders, confirm from them about the legitimacy of the email / attachment.

c. *Use email spam filters to filter out spam emails.*

f. Inappropriate use

1) Official email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.

2) Official email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one’s religious, social or political views.

3) Spam / bulk / junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

7. Software Usage Policy

a. Objective

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization-owned computers.

b. General Guidelines

1) Third-party software (free as well as purchased) required for day-to-day work will be pre-installed onto all company systems before handing them over to employees. A designated person in the IT Department can be contacted to add / delete from the list of pre-installed software on organizational computers.

2) No other third-party software - free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Department.

3) To request installation of software onto a personal computing device, an employee needs to send a written request via the IT support email.

4) Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

c. Compliance

1) No employee is allowed to install pirated software on official computing systems.

2) Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.

3) Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization are strictly prohibited. Any such act will be subject to strict disciplinary action.

4) The Procurement Department's procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes. All approved software will be purchased through the Procurement Department unless informed / permitted otherwise.

5) Any employee who notices misuse or improper use of software within the organization must inform his / her Reporting Manager(s)

d. Software Registration

1) Software licensed or purchased by the organization must be registered in the name of the organization with the job role or department in which it will be used and not in the name of an individual.

2) After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the IT Department.

3) After installation, all original installation media (CDs, DVDs etc.) must be safely stored in a designated location by the IT Department.

e. Software Audit

1) The IT Department will conduct periodic audits of software installed in all company-owned systems to make sure all compliances are being met.

2) Prior notice may or may not be provided by the IT Department before conducting the Software Audit.

3) During this audit, the IT Department will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes.

4) The full cooperation of all employees is required during such audits.

INFORMATION TECHNOLOGY STRATEGIC COMMITTEE

(IT Strategic Committee)

TABLE OF CONTENTS:

1. <u>IT Strategy Committee - Objective</u>

KSBCDC Ltd has formed a committee named IT Strategy Committee to advise the board of the company on the Information Technology initiative. This committee is mandatorily required to form as per the master direction - Information Technology Framework for NBFC sector issued by Reserve Bank of India. Strategy Committee generally consists of board members and specialized non-board members. The Committee shall work in partnership with other Board committees and senior management to provide input to them. The Committee shall carry out review and amend the IT strategies in line with the corporate strategies, Board policy reviews, cyber security arrangements and any other matter related to IT governance. Its deliberations may be placed before the Board.

2. Members of the Committee

Members of the Committee includes -

a. *Chairman - an independent director*
b. *Two or three board members*
c. *Chief Information Security Officer (CISO)*
d. *Chief Technology Officer (CTO)*
e. *IT Support Manager*
f. *General Manager - Finance & Accounts*
g. *Company Secretary*

3. Roles and responsibilities of the Committee

The primary role of the IT Strategy Committee is to support and oversee the IT infrastructure team and the IT support team. The Committee ensures that the appropriate departmental structures are in place and functioning to allow for effective communication and to ensure that the teams' own needs are recognized.

a. *Approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place.*

b. *Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.*

c. *Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable.*

d. *Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources.*

e. *Ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.*

f. *Ensuring that all new requirements are communicated to the IT teams in a timely manner.*

g. *Ensuring that mechanisms are in place so the needs of the various users in the Department can be responded to effectively.*

h. *Provide feedback on proposed solutions from a user perspective (but not to formulate solutions). Where appropriate, the IT Strategic Committee will put members of the IT teams in touch with members of the Department who can give technical advice.*

i. *The committee will support the Heads of the business team in making decisions on purchase of new software or equipment and will monitor progress on acquisition and deployment of equipment. It will also support* *the Head of the business team in making decisions about changes in staffing in the IT teams and provide guidance on funding sources and cost recovery.*

4. Frequency of meeting

The meeting of the IT Strategic Committee shall be held at least twice in a year not having a gap of more than 180 days.

5. Agenda and minutes of the Committee

Agenda of the committee meeting and minutes of the meeting shall be prepared and maintained by the Company Secretary of the company.

6. Committee decisions

Committee decisions shall be presented in the Board of the company to get the final approval.

INFORMATION SECURITY POLICY

TABLE OF CONTENTS:

1. Introduction

The information security policy provides an integrated set of protection measures that must be uniformly applied across KSBCDC Ltd to ensure a secured operating environment for its business operations.

Customer information, organizational information, supporting IT systems, processes and people that are generating, storing and retrieving information are important assets of the company. The availability, integrity and confidentiality of information are essential in building and maintaining our competitive edge, cash flow, profitability, legal compliance and respected company image.

This Information Security Policy addresses the information security requirements of:

a. ***Confidentiality****: Protecting sensitive information from disclosure to unauthorized individuals or systems*

b. ***Integrity****: Safeguarding the accuracy, completeness, and timeliness of information*

c. ***Availability****: Ensuring that information and vital services are accessible to authorized users when required*

Other principles and security requirements such as Authenticity, Non-reputation, Identification, Authorization, Accountability and Audit Ability are also addressed in this policy.

2. Scope

This policy applies to all employees, contractors, partners, Interns/Trainees working in the company. Third party service providers providing hosting services or wherein data is held outside the company premises, shall also comply with this policy.

Scope of this Information Security Policy is the information stored, communicated and processed within the company and the company's data across outsourced locations.

3. Objectives

The objective of the Information Security Policy is to provide the company, an approach to managing information risks and directives for the protection of information assets to all units, and those contracted to provide services.

4. Ownership

The Board of Directors of the company is the owner of this policy and ultimately responsible for information security.

5. Responsibility

To avoid conflict of interest, the formulation of policy and implementation/compliance to the policy shall remain segregated. Therefore, the Risk Management committee will be the owner of the Information Security (IS) Policy and Implementation responsibility to rest with the IT Security Department under IT department. The Risk Management Committee consists of the Board of Directors, Chief Information Security Officer and Chief Risk Officer.

The Chief Information Security Officer (CISO) of the company is responsible for articulating the IS Policy that the company uses to protect the information assets apart from coordinating the security related issues within the organization as well as relevant external agencies. General Manager HR acts as CISO of the

Company. The CISO shall not be a member of the IT department and shall be a member of the Risk Management Committee.

Chief Risk Officer shall assess the IT risk of the Company. General Manager (Finance) currently acts as CRO.

All the employees, contractors, partners, Interns/Trainees are responsible to ensure the confidentiality, integrity and availability of the company's information assets.

6. Risk Management Committee

This Committee shall give recommendations regarding the information Security risk and responsible for maintenance/review of the IS Policy and also for formulating/review of all sub policies derived from IS policy.

Information technology risk management is a specific branch of risk mitigation, prioritization, and optimization that focuses on the probabilities and threats that come from enterprise hardware, software, and networks.

Focus areas of risk management include:

a. ***Mitigation*** *— enterprises work to lessen the negative impact of problems that have already occurred*

b. ***Prioritization*** *— enterprises decide which risks are most important for them to handle and which are less critical*

c. ***Optimization*** *— enterprises discover which risks are worth taking so they can reap the benefits if the risks pay off.*

This Committee provides a framework for the operations of the company to track every threat presented by devices, networks, and human users. This Committee would make a risk assessment of all the IT assets, rank their importance, detailing how critical a risk is to business operations and alerting the employees who are responsible for handling it. Without managing information technology and security risks, businesses will rapidly become swamped with compliance tasks, security threats, and endpoint device management.

Since the company has a risk team and an IT department, both the teams shall collaborate in working to set up a successful IT risk management strategy. Working together means these two teams will be increasingly aware of technology threats and prioritize the ensuing risks. For example, if a storage system is breached, IT or infosec teams will discover patterns within the attack and share all relevant information with the risk team.

7. Periodic Review

The policy shall be reviewed every year or at the time of any major change in the existing IT environment affecting policy and procedures, by CISO and placed to the Board for approval.

This policy will remain in force until the next review/revision.

8. Policy Compliance Check

Compliance review of IS policy should be carried out by an internal / external auditor on a periodic basis. Internal Audit Division (IA) is responsible for monitoring compliance of IS policy. The compliance report should be placed by IA to the Audit Committee of the Board.

9. Information Security Governance

Information security governance consists of leadership, organizational structures and processes that protect information and mitigation of growing information security threats.

Critical outcomes of information security governance include:

a. *Alignment of information security with business strategy to support organizational objectives.*

b. *Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level.*

c. *Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved.*

d. *Optimization of information security investments in support of organizational objectives.*

It is important to consider the organizational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security- related events and prevention of catastrophic consequences and improved reputation in the market and among customers.

10. Management Responsibility

a. Approve policies related to information security function.

b. Ownership for implementation of board approved information security policy.

c. Ownership for establishing necessary organizational processes for information security.

d. Ownership for providing necessary resources for successful information security.

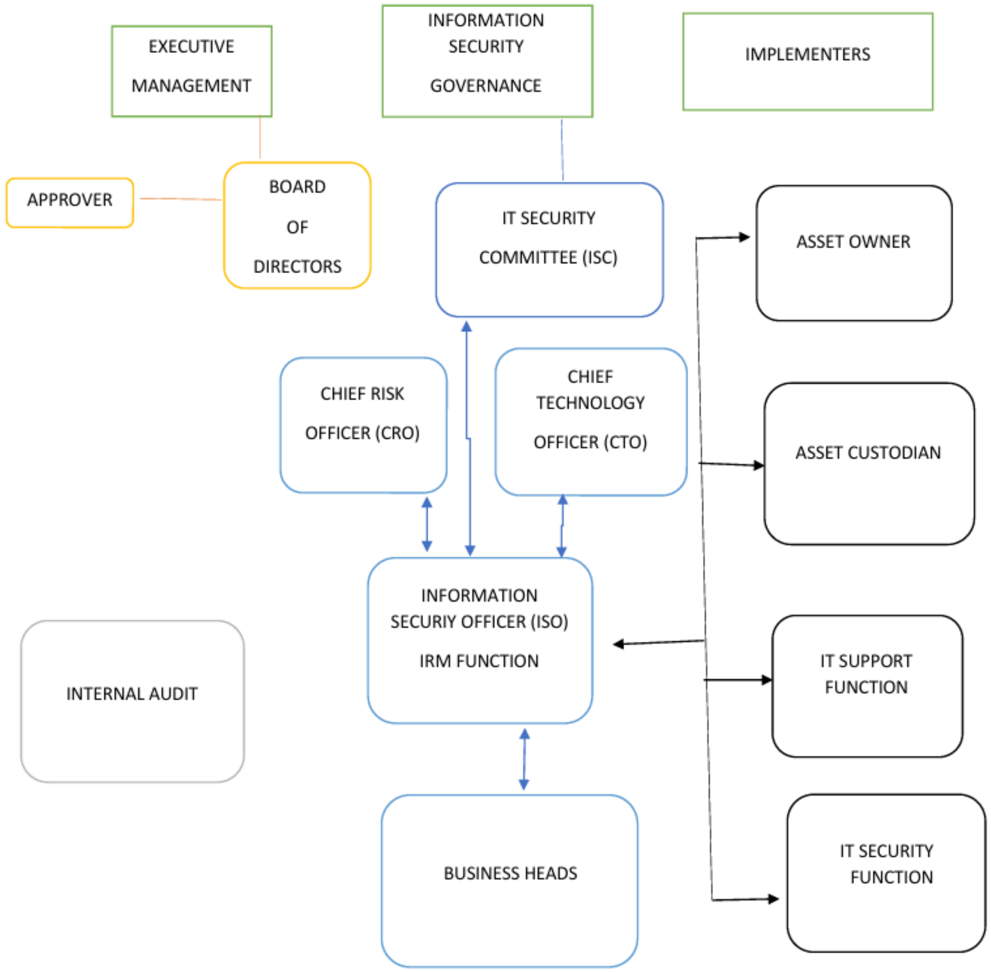
e. Ownership for establishing a structure for implantation of an information security program (framework).

11. Organization Structure

Information security organization shall comprise of the following:

a. Board of Directors
b. Information Security Committee (ISC)
c. Business/Department Heads
d. Information Asset Owner
e. Chief Information Security Officer (CISO)
f. Chief Risk Officer (CRO)
g. Chief Technology Officer (CTO)
h. Asset Custodian
i. IT Security operations
j. IT Operation
k. Internal Audit

INFORMATION SECURITY ORGANIZATION STRUCTURE



The information security organization is divided into 3 sections:

a. ***Executive Management*** *- Implementing effective security governance and defining the strategic security objectives of an organization can be complex tasks. As with any other major initiative, it must have leadership and ongoing support from executive management to succeed.*

b. ***Governance*** *- Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved,* *ascertaining that risks are managed appropriately and verifying that the enterprise resources are used responsibly.*

c. ***Implementer** - Ensuring that initiatives and existing operations adhere to policies is an area that the implementer is expected to manage.*

12. Roles and Responsibilities

The roles and responsibilities of the information Security Organization members are as follows -

a. *Board of Directors*

Approving the Information Security Policy.

b. *IT Security Committee (ISC)*

The chairman of the ISC shall be a Managing director. The ISC shall have the representation from the following Departments:

- ➔ *MD as a Chairman*
- ➔ *Chief Technology officer (CTO) – System Administrator holds the position*
- ➔ *Chief Information Security Officer (CISO)– GM (HRM & ADMIN) holds the position*
- ➔ *Chief Risk Officer – GM (Finance) holds the position*

Members from Internal Audit, HR, Legal, Finance and other departments should be called for the ISC meeting on a need basis.

The ISC roles and responsibilities shall be as follows:

- *Developing and facilitating the implantation of information security policies, and procedures to ensure that all identified risks are managed within a company’s risk appetite.*

- *Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving procedures.*

- *Supporting the development and implementation of a company-wide information security management program.*

- *Reviewing the position of security incidents and various information security assessments and monitoring activities across the company.*

- *Reviewing the status of security awareness programs.*

- *Assessing new developments or issues relating to information security.*

- *Requirement for generating effective metrics for measuring performance of security control.*

- *Reporting to the Board of Directors on information security activities.*

- *Conducting regular ISC meetings (at least quarterly) and maintenance of MOM.*

c. *Chief Information Security Officer (CISO)*

- ➔ Establishing, implanting, monitoring, reviewing, maintaining and improving information Security Management System (ISMS)

- ➔ Reviewing the security policies/procedures and suggesting improvements

- ➔ Coordinating the Information Security Committee (ISC) meetings

- ➔ Providing consultative inputs to the ISC on security requirements

- ➔ Coordinating information security initiatives in the organization

- ➔ Driving and monitoring the ISC directives in the organization

- ➔ Updating ISC about IS initiatives, issues and incidents

- ➔ Facilitating and conducting risk assessments of information assets used and recommend mitigation controls

- ➔ Promote security awareness amongst employees, customers and partners

d. Business Heads

- ➔ Heads of Business Units are ultimately responsible for managing information risk in their respective business as part of their wider risk management responsibilities

- ➔ Nominate Asset Owner

- ➔ Providing resources and support to the Asset Owners for Information security implementation in the business unit

e. Information Asset Owner

Information Asset owners shall be allocated to each information asset and shall ensure that security processes associated with these assets are established. For data and IT systems, they are called application owners. The asset owner or the application owner is usually the business owner. Each application should have an application owner (asset owner) who will typically be part of the concerned business function that uses the application.

Responsibilities would include, but not be limited to:

- ➔ *Assigning initial information classification and periodically reviewing the classification to ensure it still meets business needs under guidance of Risk Management Committee*

- ➔ *Ensuring security controls are in place, as recommended by Risk Management Committee*

- ➔ *Reviewing and ensuring currency of the access rights associated with information assets they own*

- ➔ *Determining access criteria and back-up requirements for the information assets/applications they own*

An information asset owner may delegate authority for the operation and protection of assets under their responsibility to an asset custodian. However, it will remain the responsibility of the asset owner to accept risk and to take appropriate steps to ensure that delegated authority is being responsibly applied.

f. Asset Custodian

- ➔ An asset custodian shall be a member of the information technology team.

- ➔ A custodian shall typically, but not necessarily be confined to, assist the owner in the identification of control mechanisms, ensuring their development /purchase, implementation, maintenance and effective operation, reporting issues that affect the information asset in the operational environment to the owner.

- ➔ Together with the business owner, a custodian shall develop and maintain an information asset inventory including Confidentiality, Integrity and Availability ratings in such a way that the relationship between business process and IT component is documented and known by both parties.

- ➔ A business owner shall not relinquish accountability for risk management of the owned asset by delegation of responsibility.

➔ CTO is the IT asset custodian of the Company.

g. IT Security Function

The IT Security is responsible for the execution of Information Risk policies, framework, guidelines and control process.

The responsibilities of IT Security include, but not limited to:

➔ *Enable Information Security controls*

➔ *Define IT security procedures and guidelines in line with the IS Policies*

➔ *Provide Security Architecture*

➔ *Implement and monitor operational effectiveness of mandatory IT controls*

➔ *Analysis of Security incidences, both internal and external and arriving at Lessons learned*

h. Technology Infrastructure Service Providers

➔ Infrastructure services shall be provided by strategic outsourced partners with Service Level agreements. The service providers are custodians of IT assets on behalf of the company and are responsible for the implementation and operation of the infrastructure as appropriate to meet the Confidentiality, Integrity and Availability ratings specified by the company.

- ➔ Develop Standard Operating Procedures (SOP's), Security Guidelines for the assets managed.

- ➔ Manage IT assets as per the company approved policies and procedures.

i. Application Developers

Application systems (including both business applications and generic supporting software, e.g. middle-ware, databases) may be developed and maintained by an internal IT team or by a third party. These parties are responsible for ensuring that systems are developed and maintained, incorporating user requirements and information security requirements that are in adherence to the company's policies for Information Risk. They are also responsible, in conjunction with the provider of the underlying technology infrastructure, for ensuring that information risk is adequately managed in development and test environments and report to the company IT Security.

j. User Manager

The user manager is the immediate manager or supervisor of an employee. He has the ultimate responsibility for all user IDs and information assets owned by employees. In the case of non-employee individuals such as contractors, consultants, etc., this manager is responsible for the activity and for the company assets used by these individuals. He/she is usually the manager responsible for hiring the outside contractor.

k. End Users

End users are responsible for the following with regard to information security:

- ➔ *Responsible and accountable for activities associated with an assigned account, as well as assigned equipment and removable media*
- ➔ *Protect secrecy of passwords and business information*
- ➔ *Report known or suspected security incidents*

l. Audit Team

Conduct information security audits to check compliance against policies and procedures.

13. Policies, Procedures and Guidelines

At the company considering the security requirements, Information Security policies have been framed based on a series of security principles. All the Information Security policies and their need have been addressed below:

a. Asset Management Policy

Information assets shall be accounted for and have a nominated asset owner. Owners shall be identified and catalogued for all information assets and the responsibility for maintenance of appropriated controls shall be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains accountable for the proper protection of the assets.

Reference: Asset Management Policy of the company

b. *Information Risk Management Procedure*

Detailed risk assessments for Information risks (e.g. application risk assessment, infra risk assessment) shall be undertaken in order to identify pertinent threats, the extent of vulnerability to those threats, the likelihood and the potential impact as a result of the vulnerability. This assessment shall determine acceptable, transferable and avoidable risk and the risk that shall be reduced by risk treatments (control mechanisms). The risk assessment of IT assets is attached.

Reference: Information Risk Management Procedure
Reference: Risk Assessment of IT Assets

c. *Data Classification Policy*

To ensure that confidentiality, integrity and availability of information is maintained, a data classification scheme has been designed. The level of security to be provided to the information will depend directly on the classification of the data.

Reference: Data Classification Policy

d. *Acceptable IT Usage Policy*

This policy has been prepared and implemented to ensure that all the users and staff at the company are aware of their responsibilities towards the IT resources of the company. This policy details the end users aware of their responsibilities and the acceptable use of the IT Resources of the company.

Reference: Acceptable IT Usage policy

e. *Access Control Policy*

Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized. The Access Control Policy addresses this need.

Reference: ISMS-Access Control Policy

f. *E-mail Security Policy*

The company shall implement effective systems and procedures to ensure that e- mails are used as an efficient mode of business communication and implement control procedures so that e-mail facility is not misused by the users. It also needs to ensure that e-mail service and operations remain secure, efficient while communicating within the intranet as well as through the internet. The E-mail Security Policy of the company addresses this.

Reference: ISMS-E-mail Security Policy

g. *Internet & Intranet Security Policy*

The company should utilize the internet as an important resource for information and knowledge to carry on the business more efficiently. Users must also understand that any connection to the Internet offers an opportunity for unauthorized users to view or access corporate information. Towards this direction, the company has developed systems & procedures to ensure that the Internet is used only for business purposes in a secure manner, (without endangering the security of the company's network) with a uniform code of conduct.

Reference: ISMS-Internet & Intranet policy

h. *Password Security Policy*

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of the change. All application software in the company will have to comply with minimum password standards as specified in this document.

Reference: ISMS- Password Security Policy

i. *Information Security (IS) Incident Management Policy*

Incident management is required and needs to be established to ensure a quick, effective and orderly response to security incidents. Such a policy would vary in scope depending on the sensitivity and size of the information systems being managed. A companywide incident management policy has been established for all systems.

Reference: ISMS-IS Incident Management Policy

j. *Application Security Policy*

It may be required to develop and maintain software, applications and add-on modules from time to time. Proper procedures, access controls and security requirements need to be addressed in the entire process. The application security policy has been framed to address these needs.

Reference: ISMS-Application Security Policy

k. Operating System Security Policy

The company shall protect its operating system resources by providing security at a level that is appropriate for the nature of the data being processed. The operating system security policy has been framed for achieving this. The company shall protect all business data, related application systems and operating systems software from unauthorized or illegal access. Access to the operating system must be restricted to those people who need the access to perform their duties.

Reference: ISMS-Operating System Security Policy

l. Network Security Policy

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorized access. The company's network infrastructure needs to be protected from unauthorized access. A range of security controls is required in computer networks to protect these environments. Considering the above, the network security policy has been framed for the company.

Reference: ISMS-Network Security Policy

m. Anti-Virus Policy

Viruses, Trojans, Worms, etc., are malicious programs called malware and can corrupt or destroy data or may spread confidential information to unauthorized recipients, resulting in loss of confidentiality, integrity, availability of the information. Malware detection and prevention measures as appropriate need to be implemented. The basis of protection against Malware should be founded on good security awareness and appropriate system access controls. The Anti-Virus policy has been framed on the above grounds.

Reference: Network Security Policy

n. Backup & Recovery Policy

In order to safeguard information and computing resources from various business and environmental threats, systems and procedures have been developed for backup of all business data, related application systems and operating systems software on a scheduled basis and in a standardized manner across the company. The backup and recovery procedures must be automated wherever possible using the system features and be monitored regularly. The backup & recovery policy that has been framed for the company considers these points.

Reference: ISMS-Backup & Recovery Policy

o. Log and Audit Trail Policy

The log and audit trail policy addresses the framework for logging & auditing operating system events, application events, database events in the local area network and the network events.

Reference: ISMS-Log and Audit Trail Policy

p. *Security Awareness*

All employees of the company and, where relevant, contractor and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

q. *Data Security*

Appropriate physical, technical and organizational security procedures that restrict access to and disclosure of personal data within the company are implemented. The company uses encryption, firewalls and other technology and security procedures to help protect the accuracy and security of sensitive personal information and prevent unauthorized access or improper use.

The Company adapts best practice guidelines for Physical, Technical and Organizational measures to ensure the security of personal data including the prevention of their alteration, loss, damage, unauthorized processing or access.

r. *Remote Access Policy*

The purpose of this policy is to define standards for connecting to company networks from any host. These standards are designed to minimize the potential exposure to companies from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical company internal systems, etc.

Reference: Access Control Policy

s. Exception Handling Procedure

Information security policies and procedures constitute controls for protecting the information assets. While every attempt should be made to comply with the policies and procedures there could be exceptions. The exception handling procedures should be followed for taking exceptions to the Information Security Policy after prior approval of the Chief Information Security Officer and MD of the company.

t. New Technology Adoption

- ➔ Introduction of new technology and deployment of application & infrastructure shall go through risk assessment and sign off process before implementation in production.

- ➔ Procedures and guidelines for new technologies such as cloud computing etc. shall be developed.

- ➔ The risks associated with adoption of new & emerging technologies shall be assessed and approved.

u. Cloud Computing

Cloud computing requirements shall be assessed in detail for data security, privacy, legal requirements, sustainability of the provider, service levels, geographical location of data storage and processing, including trans-border data flows, business continuity requirements, log retention, data retention, audit trials etc., during the risk assessment process.

v. *Social Media*

- ➔ Usage of social media within the company’s network is restricted, unless approved specifically.

- ➔ Employees are personally responsible for the content they publish on-line, whether in a blog, social computing site or any other form of user-generated media.

- ➔ Employees are not authorized to publish or discuss the following on social media -

    - *The company’s confidential or other proprietary information*

    - *To cite or reference customers, partners or supplies without their approval*

    - *To use the company’s logos or trademarks unless approved to do so*

w. *Compliance*

- ➔ **Compliance with regulatory requirements**

    - *Compliance to statutory, regulatory and contractual requirements such as information technology (IT) Act 2008, directives and recommendations given by RBI shall be ensured.*

- *Compliance with terms/conditions and license requirements for the usage of copyrighted software or any other proprietary information/material shall be maintained.*

- *Cross border movement of data shall be in accordance with legal and regulatory requirements.*

➔ *Compliance with Information Security Policy and procedures*

- *Information processing facilities shall be used as per information security policy and acceptable usage policy*

- *While the company respects the privacy of its employees its reserves the right to audit and / or monitor the activities of its employees and information stored, processed, transmitted or handled on any assets / devices / services used by employee*

- *Exceptions to security policy and procedure shall be approved through the exception management process.*

- *Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats, etc.*

- *Violations or any attempted violations of security policies and procedures shall result in disciplinary actions.*

➔ **Information Systems Audit**

- *Audits shall be conducted to ensure compliance with the information security policies, procedures and guidelines.*

- *The use of information systems audit tools shall be controlled and authorized to prevent any possible misuse of tools.*

Asset Inventory - Policy and Procedure

TABLE OF CONTENTS:

1. Goal

To maintain an inventory of information assets so that an appropriate level of protection of organization assets can be achieved. This is done through asset documentation, ownership, and risk rankings.

2. Scope

The Company must maintain inventories of all important information assets. The scope of this policy is inclusive of all IT assets that are owned or hosted by the company, IT assets hosted on behalf of the company by a cloud vendor or is located at a shared data center facility. At this time the current scope for maintaining inventory on assets includes:

a. *End user compute devices (computers, laptops)*
b. *End user applications*
c. *Cloud based (SaaS) applications*
d. *Company provided endpoints for employees*
e. *Company provided endpoints for contractors and/or consultants*
f. *Employee owned (BYOD) endpoints used on premises*
g. *Company owned servers onsite*
h. *Non-company owned servers onsite*
i. *Company owned servers at vendor or partner locations*
j. *Non-company owned servers located at vendor or partner locations*
k. *Company owned servers at offsite data center*
l. *Company owned networking infrastructure onsite*
m. *Company owned access badges*
n. *Company owned mobile devices*
o. *Company access devices (keys to building / elevators)*

3. Requirements for asset inventory

Data required to be collected and retained as part of the asset inventory process is:

a. *Asset name (DNS, hostname, Application name)*

b. *Approval (checkbox field that the asset has been verified as appropriate to the environment)*

c. *Device Type (computer, server, laptop, end user application, cloud application)*

d. *Description (field to provide basic description)*

e. *Asset Location (on premises, mobile, cloud)*

f. *IP Address (any protocol assignment associated with asset, can be IP range)*

g. *Asset Owner (group that owns, maintains, or requires this asset)*

h. *Risk Classification (unknown, low, medium, high)*

i. *Risk Assessment Performed (NA, none, or date)*

j. *Notes / remarks if any*

4. Inventory system

The assets shall be inventoried in a central repository. This source should be independent and regarded as the authoritative source of trust for the inventory is maintained. Procedures will exist to reconcile and update this inventory. No automated processes should update this inventory from a subjective inventory, such as other security management consoles.

5. Asset owners

All information assets must have owners, within the context of the organization. The asset owner is responsible for providing risk classification information consistent with data classification policy levels. If the ownership for a specific type of asset has not yet been clearly assigned to a specific owner, it will be temporarily defaulted to the head of that particular section on which the asset is bought.

6. Asset monitoring

Assets should be continuously monitored, as part of the cyber security vulnerability management program.

Asset Inventory: Management Process

Inputs: Assets will be discovered and ingested from other appropriate technology tools and resources. Data exports, or manual exports can be performed to populate the inventory asset list.

Review: Assets will be reviewed with the asset owner for appropriateness within the environment. Once a single approval is achieved the asset is approved unless the data owner provides written notice the asset is no longer approved.

Discovery: Ongoing processes will be used to detect new, rouge, or malicious assets introduced in the environment.

a. *Utilize Discovery Tools: Utilize active and passive discovery tools such as scanners, Active Directory, and other resources to discover new assets*

b. *Log Sources: Log sources can be used and reviewed to identify previously unknown assets such as DHCP, and DNS logs*

7. Reconcile

Assets identified as part of the discovery process will be reconciled against the source of truth asset inventory list. Assets identified that were not currently previously in the asset list, will be reviewed for ownership assignment and approval by ownership to be included in the asset inventory list.

Maintain: An ongoing governance task will be created and assigned to regularly review the asset inventory list.

This maintains process will ensure the following -

a. *Discovered assets are being added*
b. *Asset ownership and fields are being updated*
c. *Information is accurate and up to date*

Information Security Risk Management Procedure

TABLE OF CONTENTS:

1. Policy Statement

KSBCDC Ltd recognizes information as a critical asset and acknowledges the increasing risks associated with cyber threats, data breaches, and operational disruptions. The NBFC is committed to protecting its information assets by implementing a robust Information Security Risk Management (ISRM) framework.

This policy establishes the principles, governance, and processes for identifying, assessing, treating, and monitoring information security risks in line with:

a. ***RBI Master Direction DNBS.PPD. No.04/66.15.001/2016-17*** *(and subsequent amendments) on IT Framework for NBFCs*

b. ***ISO/IEC 27001 & ISO 27005*** *standards*

c. *Applicable legal requirements, including the* ***Information Technology Act 2000*** *and the* ***Digital Personal Data Protection Act 2023***

2. Objectives

The objectives of this policy are to:

a. Safeguard customer information, financial systems, and operations.

b. Ensure confidentiality, integrity, and availability (CIA) of information assets.

c. Establish a structured and repeatable methodology for risk management.

d. Meet regulatory requirements and expectations of RBI.

e. *Minimize financial, reputational, legal, and operational risks arising from cyber threats.*

f. *Promote risk awareness and accountability across the organization.*

3. Scope

This policy applies to:

a. *All IT systems, applications, infrastructure, and digital channels of the KSBCDC.*

b. *All employees, contractors, service providers, and vendors handling KSBCDC data.*

c. *All branches, head office and data centres.*

4. Governance Framework

a. Board of Directors

- ➔ *Approves this policy and defines KSBCDC’s risk appetite for information security.*
- ➔ *Receives quarterly updates on key risks and risk treatment measures.*

b. IT Strategy Committee / Risk Management Committee (RMC)

- ➔ *Provides oversight of ISRM activities.*

- ➔ *Reviews and approves residual risk acceptance.*
- ➔ *Monitors adequacy of controls and treatment plans.*

c. **Chief Information Security Officer (CISO)**

- ➔ *Owns the ISRM framework.*
- ➔ *Maintains and updates the Information Security Risk Register.*
- ➔ *Reports quarterly to RMC and annually to the Board.*

d. **Business Unit Heads**

- ➔ *Identify risks within their processes.*
- ➔ *Implement controls and ensure compliance.*

e. **Employees & Vendors**

- ➔ *Must adhere to KSBCDC's security policies and report incidents promptly.*

5. Risk Management Approach

The KSBCDC shall adopt the following approach to manage information security risks:

a. Risk Identification

- Maintain an Information Asset Register covering applications, data, infrastructure, and third-party systems.
- Identify threats (cyberattacks, fraud, insider misuse, ransomware, phishing, etc.).
- Identify vulnerabilities (weak access controls, unpatched systems, inadequate vendor security).
- Record all risks in the Information Security Risk Register.

b. Risk Assessment

- Evaluate risks based on likelihood of occurrence and potential business impact (regulatory, financial, reputational, operational).
- Use a standardized Risk Matrix for risk scoring.

c. Risk Evaluation

- Compare assessed risks with KSBCDC’s risk appetite.
- Prioritize treatment of High and Critical risks.

d. *Risk Treatment*

Four treatment options shall be applied:

- ➔ Mitigation – Apply technical and procedural controls (e.g., SOC monitoring, encryption, MFA, vendor audits).
- ➔ Avoidance – Discontinue high-risk activities.
- ➔ Transfer – Outsource to secure vendors or take cyber insurance.
- ➔ Acceptance – Accept residual risk with documented RMC approval.

e. Risk Monitoring

- ➔ Continuous monitoring.
- ➔ Regular Vulnerability Assessment & Penetration Testing (VAPT).
- ➔ Quarterly review of the Risk Register.
- ➔ Annual third-party audit of IT and IS controls.

6. <u>Risk Appetite & Tolerance</u>

a. Risks rated Extreme or Very High must be escalated to the Board with immediate treatment plans.

b. High risks must be reviewed and approved by the RMC.

c. Medium risks may be mitigated or monitored.

d. Low risks may be accepted with business justification.

7. Reporting & Review

a. The CISO shall report quarterly to the RMC and annually to the Board.

b. The policy shall be reviewed annually or earlier if triggered by significant changes in regulations, technology, or after a major incident.

8. Compliance

a. Failure to comply with this policy may lead to disciplinary action, termination of contracts, and regulatory reporting obligations.

Risk Assessment of IT Assets

TABLE OF CONTENTS:

1. Introduction

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to an IT system must be analysed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps, which are described below:

a. Step 1 - System Characterization
b. Step 2 - Threat Identification
c. Step 3 - Vulnerability Identification
d. Step 4 - Control Analysis and Likelihood of Risk
e. Step 5 - Impact Analysis and Control Recommendations

2. System Characterization

In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

The system related information of the company can be classified as follows:

a. *Hardware*
b. *Software – loan software and accounting software*
c. *System interfaces (internal and external connectivity)*
d. *Data and information*
e. *Persons who support and use the IT System*
f. *Processes performed by the system*
g. *System and data criticality*
h. *System and data sensitivity*

Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:

a. *The functional requirements of the IT system*

b. *Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)*

c. *System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)*

d. *System security architecture*

e. *Current network topology (e.g., network diagram)*

f. *Information storage protection that safeguards system and data availability, integrity, and confidentiality*

g. *Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)*

h. *Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)*

i. *Management controls used for the IT system (e.g., rules of behavior, security planning)*

j. *Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)*

k. *Physical security environment of the IT system (e.g., facility security, data centre policies)*

l. *Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).*

3. Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls.

A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human, or environmental.

Common Threat - Sources of the company:

a. *Natural Threats — Floods, earthquakes, electrical storms, and other such events.*

b. *Human Threats — Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network-based attacks, malicious software upload, unauthorized access to confidential information).*

c. *Environmental Threats — Long-term power failure, pollution, chemicals, liquid leakage.*

Kerala is a state in southern India that is prone to floods and landslides due to its topography and heavy rainfall. The state has faced fatal floods in 2018, 2019, and 2022.

The flood had made a very good loss to the whole industry of the State. Some of the branch offices of the company located in Alappuzha, Pathanamthitta and Kottayam have experienced flood issues, as most of the offices are on the ground floor. The IT assets, title deeds, other loan documents and other permanent files of the offices were safely relocated to the offsite at that time.

Recently in 2023, a virus attack to the punching system is another attack faced by the company at its Head office.

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. The table shown below presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack.

Threat Source	Motivation	Threat Actions
Hacker, cracker	Challenge, Ego, Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information, Illegal information disclosure, Monetary gain, Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion

Terrorist	Blackmail, Destruction, Exploitation, Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity, Ego ,Intelligence Monetary gain, Revenge ,Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available. Known threats have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:

a. *Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Centre)*

b. *Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.*

4. Vulnerability Identification

Vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

The below table presents the possible vulnerability / threat pairs of the company.

Vulnerability	Threat Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system.	Terminated Employees	Dialing into the company's network and accessing company proprietary data
Automatic locking of system not enabled when not in use	Employees or contractors	Data manipulation
Loan software is not an open source software (OSS)	Users of the loan software	Currently proprietary software is being used by the company, which is recommended to convert to a Core Financial Service Solution in future.
Backup facility	IT support team	If daily backup of transactions is not captured by the IT support team of the Company, there would be high risk of loss of data, if the third- party server has lost the data in their cloud server and in their mirror back up system.

5. Control Analysis and Likelihood of Risk

This step is to analyse necessary controls have been placed to reduce the vulnerabilities identified, or are planned to implement controls to reduce the vulnerabilities.

Vulnerabilities identified	Controls implemented	Likelihood of risk
Access to company data by unauthorized persons	System logins for employees, contract employees and other management staff are given for authorized persons. The log in access of systems and system data by terminated employees/ employees resigned from the company are inactivated on the day of exit.	Low
Locking of system when not in use	Automatic lock in system to all the systems shall be enabled if the system not working for a few minutes is enabled in the company to control data manipulation by another staff.	Medium

Access to company files and title deeds of the customers by unauthorized persons	Significant files of company / Title deeds of the customers are kept in a safe locker having joint custody of two authorized staff.	Medium
Access to cash in hand of the company	Cash in hand is kept in the joint custody of two authorized staff of the company / units and kept in a cash chest.	Low
Password sharing	Necessary training with regard to consequences of password sharing has been given to staff and would be provided to the new staff who would from time to time.	Medium
Social engineering by hackers	Gathering information from the company staff by the hackers / third parties who desire to attack the company data through casual talk or otherwise is called social engineering. Necessary training shall be provided to staffs to not share company data in any	Medium

	manners.	
Loan software is not an open-source software	No controls initiated in this regard. Currently proprietary software is being used by the company, which is recommended to convert to a Core Financial Service Solution in future.	High
Units located at the ground floor of the leased premises in flood prone area	The second floor of the rental premises shall be preferred for flood prone areas.	High
Lack of sufficient IT support personnel in the H.O and the units	Sufficient IT personnel shall be recruited to meet all the IT related responsibilities.	High

6. Impact Analysis and Control Recommendations

Risk impacts shall be analysed in detail to ascertain how it affects the business functionality of the company.

Vulnerabilities identified	**Impact analysis**	**Control recommendations**

Access to company data by unauthorized persons	Very low chances to occur. However, if happens, loss of data can be expected	Strict access control policy shall be adhered
Locking of system when not in use	Data manipulation may affect the business credibility of the company and questions the integrity of the company data and information.	Automatic lock of systems shall be enabled
Access to company files and title deeds of the customers by unauthorized persons	Loss of important files or theft of title deeds is a serious issue	A powerful and strong locker system shall be enabled. Also an alarming system in the locker shall be made to alert high officials.
Access to cash in hand of the company	Very low risk since there is a cash chest maintained. However, if any fraud done by the cashier and accountant by mutual understanding, then there would be cash loss to the company	Periodical review and surprise physical verification of cash by the GM Finance and Accounts shall be ensured
Password sharing	Generally happens in all organizations in between	Proper training to the staff shall be made to

	staff on account of friendship or trust, that can be misused by a hacker , or a person having rival and ego mentality.	not to share the password and make aware of its effects.
Social engineering by hackers	Loss of company data/ data manipulation	Necessary training shall be provided to staff to not share company data in any manner.
Loan software is not an open-source software	Non compatibility of the software when integrating with other software. Undocumented source code may affect the management of the loan software in case of any emergency of software maintenance by the IT support team.	No controls initiated in this regard. Currently proprietary software is being used by the company, which is recommended to convert to a Core Financial Service Solution in future.
Units located at the ground floor of the leased premises in flood prone area	The offices in the flood prone area may damage the physical files, systems and the title deeds of the borrowers.	The second floor of the rental premises shall be preferred for flood prone areas.
Lack of sufficient IT support personnel in the H.O and the units	Lack of IT personnel may affect the management of the IT	Sufficient IT personnel shall be recruited to meet all the IT related

	support of the H.O and units.	responsibilities.

Data Classification Policy

TABLE OF CONTENTS:

1. Purpose

The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to the organization, so sensitive corporate and customer data can be secured appropriately.

2. Scope

This policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all of the organization's employees, as well as to third-party agents authorized to access the data.

3. Roles and Responsibilities

The company should designate individuals who will be responsible for carrying out the duties associated with each of the roles.

a. *Data owner — The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management. The data owner shall address the following:*

➔ Review and categorization — Review and categorize data and information collected by his or her department or division

➔ Assignment of data classification labels — Assign data classification labels based on the data's potential impact level

➔ Data compilation — Ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data

➔ Data classification coordination — Ensure that data shared between departments is consistently classified and protected

➔ Data classification compliance (in conjunction with data custodians) — Ensure that information with high and moderate impact level is secured in accordance with federal or state regulations and guidelines

➔ Data access (in conjunction with data custodians) — Develop data access guidelines for each data classification label

b. Data custodians — Technicians from the IT department or, in larger organizations, the Information Security office. Data custodians are responsible for maintaining and backing up the systems, databases and servers that store the organization's data. In addition, this role is responsible for the technical deployment of all of the rules set forth by data owners and for ensuring that the rules applied within systems are working. Some specific data custodian responsibilities include:

➔ Access control — Ensure that proper access controls are implemented, monitored and audited in accordance with the data classification labels assigned by the data owner

➔ Audit reports — Submit an annual report to the data owners that addresses availability, integrity and confidentiality of classified data

➔ Data backups — Perform regular backups of state data

➔ Data validation — Periodically validate data integrity

- ➔ Data restoration — Restore data from backup media

- ➔ Compliance — Fulfil the data requirements specified in the organization’s security policies, standards and guidelines pertaining to information security and data protection

- ➔ Monitor activity — Monitor and record data activity, including information on who accessed what data

- ➔ Secure storage — Encrypt sensitive data at rest while in storage; audit storage area network (SAN) administrator activity and review access logs regularly

- ➔ Data classification compliance (in conjunction with data owners) — Ensure that information with high and moderate impact level is secured in accordance with the regulations

- ➔ Data access (in conjunction with data owners) — Develop data access guidelines for each data classification label

c. Data user — Person, organization or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended, and comply with this policy and all policies applicable to data use.

4. Data Classification Procedure

a. Data owners review each piece of data they are responsible for and determine its overall impact level and assign a classification label as follows:

Overall impact level	Classification label
High	Restricted
Medium	Confidential
Low	Public

b. The data owner records the classification label and overall impact level for each piece of data in the official data classification table, either in a database or on paper.

c. Data custodians apply appropriate security controls to protect each piece of data according to the classification label and overall impact level recorded in the official data classification table.

5. <u>Data Classification Guideline</u>

Use this table to determine the overall impact level and classification label for many information assets commonly used in the organization.

Budget Planning Documents
Federal budget planning documents state the potential expenses for the following year. They include data about partners and suppliers, as well as analytical and research data.
Information Types

Funds Control	Funds Control documents include information about the management of the budget process, including the development of plans and use programs, budgets, and performance outputs, as well as information about financing programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other mechanisms.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Unauthorized disclosure of funds control information (particularly budget allocations for specific programs or program elements) can be seriously detrimental to a company's interests in procurement processes.	Funds control activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive obligations or disbursements.	Funds control processes are generally tolerant of delay. Typically, disruption of access to funds control information can be expected to have only a limited adverse effect on agency operations, agency assets or individuals.
Impact Level	Moderate	Moderate	Low
Overall Impact	Moderate		

Level	
Data Classification Label	Confidential

6. Impact Level Determination

Use this table to assess the potential impact to the company of a loss of the confidentiality, integrity or availability of data assets.

Security Objective	Potential Impact		
	Low	**Moderate**	**High**
Confidentiality. Restrict access to and disclosure of data to authorized users in order to protect personal privacy and secure proprietary information.	Unauthorized disclosure of the information is expected to have **limited** adverse effects on operations, organizational assets, or individuals.	Unauthorized disclosure of the information is expected to have a **serious** adverse effect on operations, organizational assets, or individuals.	Unauthorized disclosure of the information is expected to have a **severe or catastrophic** adverse effect on operations, organizational assets, or individuals.
Integrity. Guard against	Unauthorized modification or destruction of the	Unauthorized modification or destruction of the	Unauthorized modification or destruction of the

improper modification or destruction of data, which includes ensuring information nonrepudiation and authenticity.	information is expected to have a **limited** adverse effect on operations, assets, or individuals.	information is expected to have a **serious** adverse effect on operations, assets, or individuals.	information is expected to have a **severe or catastrophic** adverse effect on operations, assets, or individuals.
Availability. Ensure timely and reliable access to and use of information.	Disruption of access to or use of the information or information system is expected to have a **limited** adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have a **serious** adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have a **severe or catastrophic** adverse effect on operations, assets, or individuals.

Acceptable IT Usage Policy

TABLE OF CONTENTS:

1. Purpose

The purpose of these guidelines is to set appropriate acceptable use parameters for the Information Technology systems, to ensure the continued effective and secure operation of those systems and to protect the company from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.

These guidelines should be read in conjunction with the People, Culture and Integrity Policy.

2. Scope

These guidelines apply to:

a. *all users*

b. *any use of the systems, whether or not during business hours, on company premises or through the use of privately owned devices or facilities.*

3. Authorized use

The systems are primarily a company tool, to be used for the company purposes by employees, trainees, consultants taken for contract basis, senior management etc.

a. *Employees and trainees are authorized to access only the data and information of the company for the purposes for which they have been given access to the system, based on their roles and responsibilities designated.*

b. *However, with the permission of the Managing director, Chief Information Security Officer and Chief Technical officer, additional access shall be provided to the staff, if required.*

c. *Outside consultants shall be authorized to provide only read only access to the data and information of the company, required for their work assigned by the senior management of the company. However, they shall not be given permission to edit the data and information of the company until and unless the permission of the MD, Chief Information Security Officer and Chief Technical officer is granted.*

d. *Senior management shall be restricted to give read and write access to the data and information based on the roles and responsibilities fixed by the Board of directors of the company.*

4. Personal use

Any personal use of company equipment and systems should be incidental and not interfere with the user's role within the company.

However, unreasonable or excessive personal use is not permitted. For example, the systems must not be used to conduct a personal business or private commercial activity, gamble, objectionable material or carry out excessive.

5. Ownership of data and intellectual property

The Company is the owner of all data:

a. created by employees as part of their employment; and
b. created, sent or received by users using the systems,

and all such data may be accessed as records of evidence, including in an investigation or in response to other actions such as audit, litigation or criminal investigations.

The company is the owner of all the intellectual properties held in the name of the company.

6. <u>Conditions of access</u>

It is a condition of access to the systems that users must agree to comply with all company policies relating to the use of computing facilities, including the People, Culture and Integrity Policy and these guidelines.

Users:

a. *are presumed to be responsible for all activities undertaken using their accounts*

b. *must take reasonable steps to keep their account secure*

c. *must choose a password that cannot easily be guessed or predicted*

d. *must not share their password with anyone else or record their password in obvious locations*

e. *must change their password regularly (and immediately if it becomes known by another person)*

f. *must not permit other persons to use their account (other than through an email proxy arrangement or unless approved in advance by the CIO* *g. must log out or lock their computers whenever they are left unattended*

h. must protect the security of data held on mobile systems (e.g. phones, laptops, memory sticks and other storage mediums), including by maintaining reasonable virus control measures where possible

i. must not copy or export any official electronic communication or data for non- official purposes and the same must not be retained once the official purpose is fulfilled

j. such data must not be copied to unauthorized devices

k. must not connect unauthorized devices to the network, either via software or hardware that makes this possible (e.g. attaching a personal computer or external storage device)

l. must make sure that important company data that is not included in automatic backups is manually backed up on a regular basis and can be recovered to the latest version in the event of data loss

m. must not use abusive, profane, threatening, racist, sexist, or otherwise objectionable language in any message

n. must not access, send, receive, store, or print pornographic, racist, or otherwise discriminatory, or objectionable material

o. must report actual or suspected security breaches to the IT Service Desk as soon as possible

p. must not defeat or attempt to defeat security restrictions on systems and applications *q. must not remove or disable antivirus and other similar client security agents without approval from the CIO*

r. must not use or install unauthorized or unlicensed software

s. knowingly propagate or disseminate malicious software of any type

7. Unauthorized and illegal uses

Users must not use the systems to engage in offensive, unlawful or illegal behaviour.

8. Email and other electronic communication

Email is an official method of communication for staff, contractors and trainees. Mass electronic communications are moderated by the Chief Technological officer.

9. Privacy

Users must deal with personal information in accordance with the company rules and regulations.

10. Access, monitoring, filtering and blocking

Users:

a. use the systems on the understanding and condition that their use is monitored

b. *acknowledge and consent to the company's right to access, monitor, filter and block electronic communications created, sent or received by any user using the systems*

c. *acknowledge that staff and contractor access is provisioned when commencing at the company, and staff and contractor access will be removed on their last day of employment*

d. *acknowledge that remote access to the company's network may only be made by IT approved VPN clients/services*

Subject to the approval and at the discretion of the Managing Director or other authorized person and for compliance with applicable rules, the Company reserves the right to (without notice):

a. *intercept, access, monitor and use electronic communications created, sent or received by users of the systems in any manner determined by the Company (including as records of evidence in an investigation or in response to other actions such as audit, litigation, criminal investigations or freedom of information requests)*

b. *monitor the use of any device or terminal*

c. *inspect any data residing on any Company-owned resource (regardless of data ownership and including personal emails and other personal communications and data stored in personal file directories)*

d. *capture and inspect any data in any computing infrastructure owned by the Company* *e. delete or modify any data in its network*

f. re-image its desktops and laptops as and when required

g. apply filtering systems to the network that limit use and activity by preventing communications based on size or content.

For example, communications may be blocked if they are suspected:

a. to contain unlawful material

b. to be unsolicited commercial electronic messages

c. establish processes to block access to websites deemed inappropriate

For example, the Company may block access to:

a. websites deemed to be a security risk

b. websites that may cause a negative impact on the systems

c. websites that affect network bandwidth detrimentally

d. websites deemed to contain offensive or unlawful material

e. internet protocols and methods deemed insecure

f. websites that contravene the Company's policies in any way

g. remove any material deemed to be offensive, indecent or inappropriate (including obscene material, defamatory, fraudulent or deceptive *statements, threatening, intimidating or harassing statements, or material that violates the privacy rights or property of others)*

11. Destruction of company data

Users who store Company data on a privately owned device or facility are responsible for ensuring that the Company data is rendered illegible and irretrievable at the time of disposal of that device or facility.

12. Breach of these guidelines

Access to the systems may be suspended or terminated at any time if these guidelines are breached. In addition:

a. *In some exceptional circumstances, subject to the approval of and at the discretion of authorized persons, an exemption may be granted for activities that would otherwise breach these guidelines. Exemptions may be required to be approved in advance by the MD and IT Steering Committee.*

A breach of these guidelines may also be:

a. *a breach of third-party rights (such as an infringement of intellectual property rights)*

b. *a criminal offence (such as serious acts of harassment, bullying and occupational violence and vilification)*

In addition to any disciplinary action by the Company, this may lead to civil or criminal proceedings and penalties, which the Company may report to relevant law enforcement bodies and for which the user will be held personally accountable.

In some exceptional circumstances, subject to the approval of and at the discretion of authorized persons, an exemption may be granted for activities that would otherwise breach these guidelines. Exemptions may be required to be approved in advance by the MD and IT Steering Committee.

13. Complaints

Users who receive an internal or external electronic communication that is offensive or inappropriate, should in the case of staff, contractors and consultants, raise it with their Head of the Unit or if the General manager is the cause of the complaint raise it with the Managing Director.

Access Control Policy

TABLE OF CONTENTS:

1. Scope

This policy applies to the Company’s employees, trainees, contractors and consultants that connect to servers, applications or network devices that contain or transmit company protected data, per the Data Classification Policy. All servers, applications or network devices that contain, transmit or process Company Protected Data are considered “High Security Systems”.

2. Purpose

Access controls are designed to minimize potential exposure to the Company resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the Company’s networks, systems and applications.

3. Policy

Segregation of Duties

Access to High Security Systems will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. All additions, changes, and deletions to individual system access must be approved by the Chief Technical Officer and the Chief Information Security Officer, with a valid business justification. Access controls to High Security Systems are implemented via an automated control system. Account creation, deletion, and modification as well as access to protected data and network resources is completed by the Server Operations group (CTO and IT Consultant).

On an annual basis, the Company’s Chief Information Security Officer will audit all user and administrative access to High Security Systems. Discrepancies in access will be reported to the appropriate supervisor in the responsible unit, and remediated accordingly.

4. User Access

All users of High Security Systems will abide by the following set of rules:

Users with access to High Security Systems will utilize a separate unique account, different from their normal company account. This account will conform to the following standards:

a. The password will conform to the minimum strength according to the Password Protected Policy.

b. Inactive accounts will be disabled after 90 days of inactivity.

c. Access will be enabled only during the time period needed and disabled when not in use.

d. Access will be monitored when the account is in use.

e. Repeated access attempts will be limited by locking out the user ID after not more than six attempts.

f. Lockout duration must be set to a minimum of 30 minutes or until an administrator enables the user ID.

g. If a session has been idle for more than 15 minutes, the user is required to re- authenticate to re-activate the terminal or session.

h. Users will not login using generic, shared or service accounts.

i. Service providers with remote access to customer premises (for example, for support of Point of Service systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

5. Administrative Access

a. System Administrators will abide by the Privileged Access Policy.

b. Users will abide by the above user access guidelines.

c. Administrators will immediately revoke all of a user's access to High Security Systems when a change in employment status, job function, or responsibilities dictate the user no longer requires such access.

d. Administrators must not extend a user group's permissions in such a way that it provides inappropriate access to any user in that group.

e. All servers, applications and network devices shall contain a login banner that displays the following content:

> *"This computer and network are provided for use by authorized users. Use of this computer and network are subject to all applicable company policies, including Information Technology Services policies. Any use of this computer or network constitutes acknowledgment that the user is subject to all applicable policies. Any other use is prohibited. Users of any networked system, including this computer, should be aware that due to the nature of electronic communications, any information conveyed via a computer or a network may not be private. Sensitive*

communications should be encrypted or communicated via an alternative method."

6. Remote Access

All users and administrators accessing High Security Systems must abide by the following rules:

a. *No modems or wireless access points are allowed on high security networks, or other unapproved remote access technology.*

b. *All remote access must be authenticated and encrypted through the company's VPN (Virtual Private Network), Company Secure Access.*

c. *All remote access will be accomplished through the use of two factor authentication; a username and password or PIN combination, and a second method not based on user credentials, such as a certificate or token, provisioned to the user.*

d. *Any machine used for remote access must have antivirus and host-based firewall software installed, running, and enabled. This requirement is enforced by a host checker component of the Company's VPN software, and remote access to the High Security Network is only possible after a machine has passed these configured checks.*

e. *Any third party, non-company affiliate that requires remote access to High Security Systems for support, maintenance or administrative reasons must designate a person to be the Point of Contact (POC) for their organization. In the event the POC changes, the third party must designate a new POC.*

f. All third-party access to High Security Systems must be approved by the Information Security Officer or their designee.

g. Third parties may access only the systems that they support or maintain.

h. All third-party accounts on High Security Systems will be disabled and inactive unless needed for support or maintenance. Requests for enabling access must follow the policies of the company. Requests for access outside of this policy are expressly denied. The server System Administrator will be responsible for enabling/disabling accounts and monitoring vendor access to said systems. All third parties with access to any High Security Systems must adhere to all regulations and governance standards associated with that data. Third party accounts must be immediately disabled after support or maintenance is complete.

i. Data must not be copied from high security systems to a user's remote machine.

j. Access will be disconnected automatically after 24 hours.

k. Users will abide by the above user access guidelines.

7. <u>Physical Access to Datacentre</u>

The data Centre of the company is maintained by Kerala State IT Mission based on the contract between the company and Kerala State IT Mission.

Hence no physical access to the company employees is made available.

8. **Policy Adherence**

Failure to follow this policy can result in disciplinary action against the employees, trainees, contractors etc.

Email Security Policy

TABLE OF CONTENTS:

1. Introduction

An email security policy is a series of procedures governing the use of emails within a network or an establishment. It details how a category of users interacts with messages that are sent and received via email.

2. Purpose

The goal of an email security policy is to secure messages from unauthorized access.

3. Responsibilities of Users

Appropriate Use of E-mail Service:

a) *E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ids should be used for official communication and name-based ids can be used for both official and personal communication.*

b) *Examples of inappropriate use of the e-mail service -*

- ➔ Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.

- ➔ Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

- ➔ Unauthorized access of the services. This includes the distribution of emails anonymously, use of other officers' user ids or using a false identity.

- ➔ Creation and exchange of information in violation of any laws, including copyright laws.

- ➔ Wilful transmission of an e-mail containing a computer virus.

- ➔ Misrepresentation of the identity of the sender of an email.

- ➔ Use or attempt to use the accounts of others without their permission.

- ➔ Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc.

- ➔ Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation of the account. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

4. User’s Role

a) The user is responsible for any data / e-mail that is transmitted using thee-mail system.

b) All e-mails / data sent through the mail server are the sole responsibility of the user owning the account.

c) Sharing of passwords is prohibited.

d) The user’s responsibility shall extend to the following:

- ➔ *Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.*

- ➔ *The ‘reply all’ and the use of ‘distribution lists’ should be used with caution to reduce the risk of sending e-mails to wrong people.*

- ➔ *Back up of important files shall be taken by the user at regular intervals.*

5. Deactivation

In case of threat to the security of the company, the e-mail id being used to impact the service may be suspended or deactivated immediately by the Chief Technology Officer.

Subsequent to deactivation, the concerned user and the competent authority of that respective organization shall be informed.

Internet And Intranet Policy

TABLE OF CONTENTS:

1. <u>Purpose</u>

The purpose of the internet policy is to protect the confidentiality and integrity of the information of the company as required by law, professional ethics, and accreditation requirements. All employees of this practice must comply with this policy.

2. <u>Assumptions</u>

This Internet Security Policy is based on the following assumptions:

a) *Our office benefits from access to and use of the Internet and its resources.*

b) *The resources, services, and interconnectivity available via the internet provide significant resources to improve the efficiency of this practice.*

c) *Use of the internet also involves more risks than an intranet.*

d) *Improper use of the internet puts this practice and its employees at risk.*

e) *The content of all web pages under this practice's jurisdiction must comply with local, state, and federal laws and its own policies and procedures.*

f) *A policy is necessary to clarify the proper use of the internet to maintain the accuracy, security, and confidentiality of individually identifiable health information and other sensitive data.*

g) *This company's system used to access the internet is the property of the practice and is subject to the office's control of such use.*

h) Data users have no expectation of privacy when using the office's system to access the internet.

3. Policy

This policy applies to all officers, employees, and independent contractors of this office who use its system for internet access and governs all internet access, communications, and storage using this practice's system.

All data users must strictly observe the following rules when using the internet:

- ➔ Users may not access or use the internet for personal business or personal commercial gain.
- ➔ Users must have a proper medical or business purpose for any access and use of the internet.
- ➔ Users may not access pornographic or other offensive websites (including, but not limited to, sexist, racist, discriminatory, hate, or other sites that would offend a reasonable person in the same or similar circumstances). If the user has any doubt whether access to a specific site is proper, he or she should seek approval from the Security Officer.

4. Access control

a) Users may not use any other user's ID, password or other identification to access the internet.

b) Users attempting to establish a connection with this office's computer system via the internet must authenticate themselves at a firewall before gaining access to its internal network.

c) Users may not establish modems, internet, or other external network connections that could allow unauthorized users to access this practice's system or information without the prior approval of the Security Officer.

d) Users may not establish or use new or existing internet connections to establish new communications channels without the prior approval of the Security Officer.

e) Users may not transfer business information or any information of the company via the internet without prior approval of the Security Officer.

f) Users may not download and/or install software without prior permission from the Security Officer.

g) Users must not open any email attachments they are not expecting to receive. Questionable emails should be referred to the appropriate compliance officer.

5. Enforcement

All employees are responsible for adhering to and enforcing this policy. Employees who violate this policy are subject to disciplinary action up to and including termination.

Password Security Policy

TABLE OF CONTENTS:

1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

2. Scope

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

3. Policy

a) Policy Statements

I. For users having accounts for accessing systems/services

- ➔ Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.

- ➔ All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.

- ➔ Passwords shall be enforced to be of a minimum length and comprising a mix of alphabets, numbers and characters.

- ➔ Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.

- ➔ All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.

- ➔ All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.

- ➔ Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.

- ➔ Passwords shall not be revealed on questionnaires or security forms.

- ➔ Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.

- ➔ The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. a separate password to be used for a Windows account and an UNIX account should be selected. The "Remember Password" feature of applications shall not be used.

- ➔ Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

- ➔ First time login to systems/services with administrator created passwords, should force changing of password by the user.

- ➔ If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

- ➔ The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

Ii. For designers/developers of applications/sites

- ➔ No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.

- ➔ The backend database shall store hash of the individual passwords and never passwords in readable form.

- ➔ Passwords shall be enforced to be of a minimum length and comprising a mix of alphabets, numbers and characters.

- ➔ Users shall be required to change their passwords periodically and not be able to reuse previous passwords.

- ➔ For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

b) Policy for constructing a password:

All user-level and system-level passwords must conform to the following general guidelines described below -

- ➔ The password shall contain more than eight characters.

- ➔ The password shall not be a word found in a dictionary (English or foreign).

- ➔ The password shall not be a derivative of the user ID, e.g. 123.

- ➔ The password shall not be a slang, dialect, jargon etc.

- ➔ The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.

- ➔ The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.

➔ The password shall not be based on birthdays and other personal information such as addresses and phone numbers.

➔ The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.

➔ The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).

➔ The password shall be a combination of upper- and lower-case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., @# $%^&*() _+|~-=\`{}[]:";'<>? /).

➔ Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

c) Suggestions for choosing passwords:

Passwords may be chosen such that they are difficult-to-guess yet easy-to remember.

Methods such as the following may be employed -

➔ String together several words to form a pass-phrase as a password.

➔ Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.

- ➔ Combine punctuation and/or numbers with a regular word.

- ➔ Create acronyms from words in a song, a poem, or any other known sequence of words.

- ➔ Bump characters in a word a certain number of letters up or down the alphabet.

- ➔ Shift a word up, down, left or right one row on the keyboard.

4. <u>Responsibilities</u>

a) All individual users having accounts for accessing systems/services in the domain, and system/network administrators of servers/ network equipment shall ensure the implementation of this policy.

b) All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

5. <u>Compliance</u>

a) Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.

b) Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.

Information Security Incident Management Policy

TABLE OF CONTENTS:

1. **Background**

a) All information security incidents, actual or suspected, must be reported, documented, assessed, mitigated and communicated as appropriate.

b) Detection controls, including procedures and tools must be in place to detect and escalate as soon as possible any occurrence of a security incident.

c) When occurring, security incidents must be effectively addressed to contain and mitigate negative impacts and return to a normal situation in a timely manner.

2. **Policy Objective**

a) The objective of this policy is to ensure the Institution has reasonable security controls in place to prevent, detect and address information security incidents.

3. **Scope**

This policy applies to:

a) All employees, consultants, contractors, agents and authorized users accessing company's IT systems and applications

b) All IT systems or applications managed by the company that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems

4. Definitions

a) “Information Security Incidents” are unplanned events which affect the confidentiality and integrity of data and the availability of IT systems. Examples of an information security incident include: confidential data breach, privacy breach, unauthorized access to applications and network, malware contamination, web site defacement, etc. Security incidents that have a high probability of being exploited and that will highly impact the Institution (i.e. risk of operation disruption, data breach, etc.) are often labelled as “Critical” or “High”.

b) “Critical Security Incidents” are security incidents that present the highest probability of being exploited and that have a high impact on the Institution.

c) “Users” are persons accessing an IT system or application.

5. Guiding Principles - General Requirements

All users must immediately report any observed or suspected event that potentially presents a security risk or is in violation of the company’s security policies, such as:

a) Suspicious behaviour of a company system or application

b) Suspicious behaviour of a user

c) Security weakness in company technology, systems or services

d) *When an information security incident occurs, the IT Help Desk must be immediately informed. The IT Help Desk is the first point of contact for such an incident.*

e) *The company will take appropriate actions in response to information security incidents to:*

- ➔ Immediately contain the information security incident and prevent any further impact where possible

- ➔ Remediate the incident and return to a normal situation in a timely manner

- ➔ Communicate internally with stakeholders impacted by the incident, as well as with necessary directors of the company to contain and remediate the incident

- ➔ Communicate with external stakeholders, including the public, business partners and law enforcement authorities, where applicable

- ➔ Document in a formal incident report the details of the incident, including:

    - *Timeline of the information security incident*

    - *How the incident was detected*

    - *How the incident occurred, and if any gap in the security controls in place facilitated the occurrence of the incident*

    - *The impact of the incident (e.g. as cost to remediate and loss of data)*

    - *How the incident was contained and remediated*

    - *The lessons learned from the incident, to prevent the re-occurrence of such an incident in the future*

➔ The Institution will maintain and regularly update incident response plans for common security threats

➔ Operational procedures must be maintained and regularly reviewed for the operation of security and system monitoring services, such as:

    - *Security log monitoring and Security Information and Events Management (SIEM)*

    - *Intrusion Detection and Prevention systems (IDS/IPS)*

    - *Network firewalls*

    - *Web application firewalls*

    - *Anti-malware software*

    - *Email and web filtering systems*

    - *Network performance monitoring tools*

- *Procedures and tools to monitoring the usage of the company’s technology (such as network, email, web access and applications)*

6. Roles and Responsibilities

Board of directors - Approve and formally support this policy

Managing Director - Review and formally support this policy

Chief Technology Officer - Develop and maintain this policy, Review and approve the incident reaction plans as well as the security monitoring procedures, Review and approve any exceptions to the requirements of this policy, takes proactive steps to reinforce compliance of all stakeholders with this policy.

GM Admin / HRM - Support all employees and other trainees in the understanding of the requirements of this policy, immediately assess and report to the IT service desk any non- compliance instance with this policy

Company Secretary - Ensure that the responsibilities and obligations of each party to the contractual relationship are outlined in the contract executed between the Institution and the contractor/sub-contractor

GM Admin / HRM - Present each new employee or contractor with the existing company policies, upon the first day of commencing work with the company, Support all employees in the understanding of the requirements of this policy

All users (Employees and contractors, Visitors and or Volunteers) - Report all non- compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible

7. <u>Exceptions to the Policy</u>

a) Exceptions to the guiding principles in this policy must be documented and formally approved by the Chief Information Security Officer.

b) Policy exceptions must describe:

- ➔ *The nature of the exception*
- ➔ *A reasonable explanation for why the policy exception is required*
- ➔ *Any risks created by the policy exception*
- ➔ *Evidence of approval by the Chief Information Security Officer*

Application Security Policy

TABLE OF CONTENTS:

1. Purpose

The purpose of this policy is to enforce that web applications maintain the security posture, compliance, risk management, and change control of Company IT Resources.

2. Scope

This IT policy, and all policies referenced herein, shall apply to all the employees, independent contractors, trainees etc. who use, access, or otherwise employ, locally or remotely, the Company's IT Resources, whether individually controlled, shared, stand-alone, or networked.

3. Policy Statement

a) Web application security assessments must be performed to identify potential or realized weaknesses (e.g., insecure coding, inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage).

b) Web applications must follow regular security or out-of-band assessments if one of the following criteria are met:

➔ *New or significant application releases are subject to the Secure Software Development Life Cycle before approval of the change control documentation or release into the live environment.*

➔ *Third-party or acquired web applications (i.e., commercial applications for which source code is not available) must be scanned when installed or upgraded. The vulnerabilities must be* *reported to Information Security and Assurance (ISA) and the vendor for correction.*

c) Shared accounts are prohibited, except where it is not technically possible to individually provision accounts.

d) All Internet-facing web applications should deploy the Information Security and Assurance approved technical controls (e.g., Web Application Firewall (WAF) or Intrusion Prevention System (IPS)).

e) Other security controls include but are not limited to, the following:

- ➔ *Access controls*
- ➔ *Configuration changes (you must submit non-agreed upon configuration changes to Information Security and Assurance for review)*
- ➔ *Authentication (multi-factor authentication must be used for except where it is not technically possible)*
- ➔ *Data protection (e.g., encryption, data masking)*
- ➔ *Error handling and logging*
- ➔ *Input and output handling*
- ➔ *Session management*

4. Definitions

IT Resources include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

Web Application Security is a branch of information security that deals specifically with the security of websites, web applications, and web services.

Operating System Security Policies

TABLE OF CONTENTS:

1. Introduction

The operating system is the physical environment where your application runs. Any vulnerability in the operating system could compromise the security of the application. By securing the operating system, you make the environment stable, control access to resources, and control external access to the environment.

The physical security of the system is essential. Threats can come through the Web, but they can also come from a physical terminal. Even if the Web access is very secure, if an attacker obtains physical access to a server, breaking into a system is much easier.

2. Scope

This policy is applicable to all employees, trainees, consultants, those who have access to operating systems of the company.

Policies and procedures to be followed by the users those who have access to Operating System of the company are detailed below:

a) User Accounts

➔ Limit the number of user accounts on the server computers.

- *Unnecessary and legacy user accounts increase system complexity and may present system vulnerabilities.*

- *Fewer user accounts reduce the amount of time administrators spend on account administration.*

➔ Ensure that only a few trusted users have administrative access to the server computers.

- *Fewer administrators make it easier to maintain accountability. The administrators must be competent.*

➔ Assign the minimum required access permissions for the account that runs the application.

- *If attackers obtain access to the application, they have the permissions of the user who runs the application.*

b) Account Policies

➔ Password policies that promote operating system security shall be followed.

- *Examples of such policies are the strong password rule and the password change schedule.*

- *Refer: the password policy of the company*

➔ Test the strength of users' passwords by breaking the passwords.

- *The users who do not comply with the strong password rule shall receive a notification to update their passwords according to the organization password policy.*

c) File System

➔ Grant the users read-only permissions for required directories.

- *If attackers obtain access to an application, they have the user permissions.*

➔ Deny access by default.

- *Access to resources shall be denied for everyone except for the users to whom access is granted explicitly.*

- *The Company shall deny read and write permissions for all directory structures for all users. Only users to whom these permissions are granted explicitly have access to the directories and files. This policy also protects any resources that were overlooked by an administrator.*

d) Network Services

➔ Provide the minimum number of required services on the server computer.

- *Use only the services that the company needs to run the application. Each service is a potential entry point for a malicious attack. Reducing the number of running services also makes the system more manageable.*

- *For example, the company may not need the ftp, rlogin, or ssh services.*

➔ Reduce the level of access permissions for the network services users.

    - *Network services are exposed to the public.*

➔ Ensure that the user accounts that have access to the Web server do not have access to the shell functions.

➔ Ensure that unused services are not running, and that they do not start automatically on Microsoft Windows operating systems.

➔ Reduce the number of trusted ports specified in the /etc/services file.

    - *Delete or comment out the ports that the users do not plan to use to eliminate possible entry points to the system.*

➔ Protect the system against NetBIOS threats associated with ports 137, 138, and 139.

    - *These ports are listed in the /etc/services file.*

➔ Use wrapper services, such as iptables.

➔ Ensure that the services are current by checking often for security updates.

➔ Avoid using services that have a graphical user interface (GUI), if possible.

    - *Such services introduce many known security vulnerabilities.*

e) System Patches

- ➔ Run the latest, vendor-recommended patches for the operating system.

  - ● *The patches may be core OS patches, or patches required by additional applications.*

- ➔ Schedule regular maintenance of security patches.

f) Operating System Minimization

- ➔ Remove nonessential applications to reduce possible system vulnerabilities.

- ➔ Restrict local services to the services required for operation.

- ➔ Implement protection for buffer overflow.

g) Logging and Monitoring

- ➔ Log security-related events, including successful and failed logons, logoffs, and changes to user permissions.

- ➔ Monitor system log files.

- ➔ Use a time server to correlate time for forensics.

- ➔ Secure the system log files by restricting access permissions to them.

- *Logs are important for daily maintenance and as a disaster recovery tool. Therefore, they must be protected from system failures and user tampering.*

➔ Use IPF logging to build a more sophisticated logging system.

- *To increase the security of the log file system, the users shall*

    ★ place all log files in one location, on one server

    - *This simplifies the administration of log files.*

    ★ set up multiple logging servers for redundancy

    ★ use a remote server for logging

    - *This protects the logs if the system is compromised and, for example, the hard drive is destroyed.*

    - *Because an IPF server is accessed through the network, it can be located anywhere in the world.*

➔ Secure the logging configuration file.

- *The configuration file contains settings that, if changed, can compromise the reliability of the log system. For example, setting the log level incorrectly may cause some failures not to be logged.*

➔ Enable logging of access requests on the Web server.

- *This can be useful in identifying malicious activity.*

h) System Integrity

➔ Build production systems from a known and repeatable process to ensure the system integrity.

➔ Check systems periodically against snapshots of the original system.

➔ Use available third-party auditing software to check the system integrity.

➔ Back up the system resources on a regular basis.

3. <u>Exception to the policy</u>

Any deviation from the procedure of operation / use of the operating system shall be sought special permission / approval from the Chief Information Security Officer and Managing Director.

4. <u>Compliance</u>

Any breach of the operating system security policy by the users shall be treated as a punishable offence and the company shall have every right to expel that person from employment.

Network Security Policy

TABLE OF CONTENTS:

1. Purpose

The Company resources, such as Internet/Intranet/Extranet-related systems, are to be used for company business purposes in serving the interests of the company. The participation and support of every employee, trainee, consultants etc. who deals with information and/or information systems is necessary to achieve effective security. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. The purpose of this policy is to delineate acceptable use of technology resources. These rules are in place to protect the user of these resources and the company. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues.

2. Scope

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

3. Maintenance

This Policy will be reviewed by the Company's Information Security Office annually or as deemed appropriate based on changes in technology or regulatory requirements.

4. Enforcement

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

5. Exceptions

Exceptions to this Policy must be approved by the Information Security Office. All exceptions will be formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

6. Policy on data network

The data network is a shared resource used by the entire employees of the company in support of the business processes and academic missions. Business units and community members 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 the company.

This policy is established under the provisions of the Company's Information Security Policy Program.

The following rules define the policy regarding access to the Company network:

a) *Only authorized people can gain access to the company'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 company-owned computers.*

b) *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.*

c) Use of service accounts for local log-ins by any individual is prohibited. This rule is designed to prevent unauthorized changes to production data by accounts that allow groups of users to employ the same password.

d) Access controls required for remote systems connecting to production systems. All computers that have remote real-time dialogs with Company's IT production systems must run an access control package approved by the Chief Information Security Officer.

e) Multiple simultaneous remote external network connections prohibited. Unless special permission has been granted by the Chief Information Security Officer.

f) All log-in banners must include security notice. Every log-in screen for multiuser 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.

g) Security notice in log-in banner must not disclose system information. All log-in banners on network-connected computer systems must simply ask the user to log-in, 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.

h) 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.*

7. <u>Server</u>

This policy applies to all servers that the company is responsible to manage.

Policy

Servers must be registered within the Enterprise Management System.

At a minimum, the following information is required to positively identify the point of contact:

a) Server contact(s) and location, and a backup contact

b) Hardware and Operating System/Version

c) Main functions and applications, if applicable

d) Information in the Enterprise Management System must be kept up-to-date

e) The device must be guarded by an up-to-date and active firewall set to protect it from unauthorized network traffic

f) Current operating system and application software with current security patches must be installed

g) *The device must be protected against malicious or undesired software such as viruses, spyware, or adware*

h) *Access to the device must require appropriate authentication controls such as account identifiers and robust passwords*

i) *The device must be certified and registered as equipment that has met all security criteria, prior to connecting to the network*

8. <u>Server general configuration guidelines</u>

a) Services and applications that will not be used must be disabled where practical.

b) Access to services should be logged and/or protected through access-control methods such as Transmission Control Protocol (TCP) Wrappers.

c) 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.

d) 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.

e) 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).

f) Servers should be physically located in an access-controlled environment.

g) Servers are specifically prohibited from being operated in uncontrolled cubicle areas.

9. Internal network addresses

a) Internal network addresses must not be publicly released.

b) The internal system addresses, configurations, and related system design information systems and users outside the internal network cannot access this information.

10. Internet web server

All Internet Web servers must be firewall protected.

All connections between Company’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 the Chief Information Security Officer.

11. Public servers

Public Internet servers must be placed on subnets separate from internal networks. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

12. Malware protection

The Chief information security office is entrusted with the responsibility to provide professional management of the company’s servers as outlined in this policy.

Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover. This policy applies to all servers that the company is responsible to manage.

Policy

a) Anti-virus

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

➔ Non-administrative users have remote access capability

➔ The system is a file server

➔ Microsoft Share access is open to the server from systems used by no administrative users

➔ HTTP/FTP access is open from the Internet

➔ Other “risky” protocols/applications are available to this system from the Internet at the discretion of the IT Security Administration.

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- ➔ Outbound web access is available from the system

b) Mail server anti-virus

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local antivirus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

c) Anti-spyware

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- ➔ Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet

- ➔ Any system where non-technical or non-administrative users have the ability to install software on their own

d) Notable exceptions

An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions applies to this system:

- ➔ The system is a SQL server Database
- ➔ The system is used as a dedicated mail server
- ➔ The system is not a Windows based platform

e) Enforcement

The responsibility for implementing this policy belongs to all the staff of the company. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the company Information Security Officer. Any employee, visitors, consultants or contractors found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

13. Router

This policy describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the company.

All routers and switches connected toIT production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the Internet DMZ Equipment Policy.

Policy

All routers within the company IT Enterprise must meet the following configuration standards:

a) No local user accounts are configured on routers.

b) 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 IT Enterprise must disallow the following:

a) IP directed broadcast Incoming packets at the router sourced with invalid addresses such as RFC1918 address

b) TCP small services

c) UDP small services

d) All source routing

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

14. Firewall

The firewall policy dictates how the firewall should handle application traffic such as web, email, or telnet. The policy describes how the firewall is to be managed and updated.

a) Real-time external network connections require firewalls

Before reaching a log-in banner, all in-bound real-time external connections to the company IT 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 set up 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 company network.*

b) Firewall configuration change requires CISO 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 the Chief Information Security officer.

- ➔ *The Board must monitor incident response team reports and security websites for information about any 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 Board must ensure that administrators receive regular training in order to stay current with threats and vulnerabilities.*

15. Internet DMZ equipment

This Policy defines the standards to be met by all equipment owned and/or operated by the company that is located outside the company’s Internet firewalls (the demilitarized zone or DMZ). These standards are designed to minimize the potential exposure to the company from the loss of sensitive or confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of IT resources.

Devices that are Internet facing and outside the company’s firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the company’s firewalls.

The policy defines the following standards:

a) *Ownership responsibility*
b) *Secure configuration requirements*
c) *Operational requirements*
d) *Change control requirement*

All equipment or devices deployed in a DMZ owned and/or operated by the company (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by the company must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "howard.edu" domain or appears to be owned by the company.

All new equipment that falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from the Chief Information Security Officer. All existing and future equipment deployed on Company's un-trusted networks must comply with this policy.

Policy

a) Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by Information Security for DMZ systems, application, and/or network management. Support groups will be responsible for the following:

- ➔ Equipment must be documented in the company-wide enterprise management system. At a minimum, the following information is required:
    - *Host contacts and location*
    - *Hardware and operating system/version*
    - *Main functions and applications*
    - *Password groups for privileged passwords*

- ➔ Network interfaces must have appropriate Domain Name Server records.

- ➔ Immediate access to equipment and system logs must be granted to members of Information Security upon demand, per the Audit Policy.

- ➔ Changes to existing equipment and deployment of new equipment must follow and the company changes management processes / procedures.

To verify compliance with this policy, the Information Security team will periodically audit DMZ equipment per the Audit Policy.

16. <u>General configuration policy</u>

All equipment must comply with the following configuration policy:

a) Hardware, operating systems, services and applications must be approved by the Chief Information Security Officer as part of the pre-deployment review phase.

b) Operating system configuration must be done according to the secure host and router installation and configuration standards.

c) All patches/hot-fixes recommended by the equipment vendor and Chief Information Security Officer must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

d) Services and applications not serving business requirements must be disabled.

e) Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by the Chief Information Security Officer.

f) Services and applications not for general access must be restricted by access control lists.

g) Insecure services or protocols must be replaced with more secure equivalents whenever such exist.

h) Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one- time passwords (DES/SofToken) must be used for all access levels.

i) All host content updates must occur over secure channels.

j) Security-related events must be logged and audit trails saved to approved logs. Security-related events include (but are not limited to) the following:

- User login failures
- Failure to obtain privileged access
- Access policy violations

k) Chief Information Security Officer will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

17. <u>New installations and change management procedures</u>

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

a) New installations must be done via the DMZ Equipment Deployment Process.

b) Configuration changes must follow the Company Change Management (CM) Procedures

c) Chief Information Security Officer (CISO)must be invited to perform system/application audits prior to the deployment of new services.

d) CISO must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

18. <u>Equipment outsourced to external service providers</u>

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.

19. Network management / access requirements

a) All networks on the company are installed and maintained by Company Technology Services.

b) To assure the integrity and availability of network services, no other network communications (with the exception of commercial cellular telephony networks) shall be permitted on company facilities.

c) No networking equipment (routers, managed switches, DHCP servers, DNS servers, WINS servers, VPN servers, remote access dial-in servers/RADIUS, wireless access points, hardware firewalls – shall be permitted without a written exception from CISO.

d) All devices connected to Company networks shall be registered with the Information Security Office register when initially attached to the network. This applies to printers, computing systems, laboratory equipment, and communications devices that use TCP/IP network protocols. The registrant must be an employee, consultant, or contractor with a valid and active Network ID. Information on how to register a network device can be obtained by contacting the System Administer. Unregistered devices are subject to disconnection from the Network, without notice, whether or not they are disrupting network service.

20. Remote access

a) Secure remote access must be strictly controlled. Control will be enforced via one- time password authentication or public/private key with strong passphrases.

b) At no time should any employee provide his or her login or email password to anyone, not even family members.

c) Employees and contractors with remote access privileges must ensure that their company 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.

d) Employees, contractors and students with remote access privileges to the enterprise network must not use non-company email accounts or other external resources to conduct company business.

e) Routers for dedicated Integrated Services Digital Network (ISDN) lines configured for access to the company's network must meet minimum authentication requirements.

f) Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time.

g) Frame relay must meet minimum authentication requirements of Data Link Connection Identifier (DLCI) standards.

h) Third party connections must comply with requirements as stated in the Third-Party Agreement.

i) Personal equipment that is used to connect to the network must meet the requirements of company-owned equipment for remote access.

j) Organizations or individuals who wish to implement non-standard Remote Access solutions to the production network must obtain prior approval from CISO.

k) Direct network connections with outside organizations must be approved. The establishment of a direct connection between the Company'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 CISO.

l) Inventory of connections to external networks must be maintained. CISO must maintain a current inventory of all connections to external networks including telephone networks, EDI networks, extranets, the Internet.

21. 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.

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

a) *When actively connected to the enterprise network, the VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.*

b) *Dual (split) tunnelling is NOT permitted; only one network connection is allowed.*

c) *VPN gateways will be set up and managed by CISO.*

d) *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 computers.*

e) *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.*

f) *Users of computers that are not owned by the company must configure the equipment to comply with VPN and Network policies.*

g) *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 company's owned equipment, i.e., their machines must be configured to comply with company's Security Policies.*

22. Definitions

a) **Server**: For purposes of this policy, a server is any computer system residing in the physically secured data centre owned and operated by the cloud server (Kerala IT Mission). In addition, this includes any system running an operating system specifically intended for server usage as defined by the CISO that has access to internal secure networks. This includes, but is not limited to, Microsoft Servers and all permutations, any Linux/Unix based operating systems that external users are expected to regularly connect to.

b) **Malware**: Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

c) **Spyware**: Broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

d) **Anti-virus Software**: Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

e) **Production Network**: The "production network" is the network used in the daily business. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to company employees or impact their ability to do work.

f) **Lab Network**: A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, research, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to the company nor affect the production network.

g) **DMZ (de-militarized zone)**: Any un-trusted network connected to, but separated from, Company's IT network by a firewall, used for external (Internet/partner, etc.) access from within the company, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.

h) **Secure Channel**: Out-of-band console management or channels using strong encryption. Non-encrypted channels must use strong user authentication (one-time passwords).

i) **Un-Trusted Network**: Any network firewalled off from the company network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

Backup and Recovery Policy

TABLE OF CONTENTS:

1. Overview

In accordance with mandated organizational security requirements set forth and approved by management, KSBCDC Ltd has established a formal Data Backup and Recovery policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the company's needs and goals.

2. Purpose

This policy and supporting procedures are designed to provide the company with a documented and formalized Data Backup and Recovery policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of the company I.T. system resources and all supporting assets. Backups are a critical process for any organization, especially considering today’s growing regulatory compliance mandates and the ever-increasing cyber security threats for which businesses face on a daily basis. Yet even without compliance mandates, a well-though out, efficient, and reliable backup and recovery is a must for ensuring the confidentiality, integrity, and availability (CIA) of critical data.

3. Scope

This policy and supporting procedures encompass all system resources and supporting assets that are owned, operated, maintained, and controlled by Company and all other system resources, both internally and externally, that interact with these systems.

a) *Internal system resources are those owned, operated, maintained, and controlled by Company and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (and the operating systems and applications that reside on them, both physical and virtual servers) and any other system resources and supporting assets deemed in scope.*

b) *External system resources are those owned, operated, maintained, and controlled by any entity other than Company, but for which these very resources may impact the confidentiality, integrity, and availability (CIA) of Company system resources and supporting assets.*

4. Policy

Company is to ensure that the Data Backup and Recovery policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

a) Backup environments

A critical component of any data backup and recovery initiatives is to properly identify all environments – and the associated data – that required backup procedures. While critical environments, such as those relating to production, development, and staging require backups, it’s the platforms and the supporting systems within these environments that are to be identified, with applicable backup procedures in place. This would include, but not limited to, the following platforms and supporting systems:

➔ *Network device backups, such as configuration file, rulesets, and other critical data.*

- ➔ *Servers, (both virtual and physical stand-alone) such as all operating systems, and associated applications (i.e., databases, web server applications, etc.) for all Microsoft Windows, UNIX, Linux, and any other type of other operating systems.*

- ➔ *Critical servers, such as all production facing servers, DNS servers, email servers, FTP servers, and all other systems associated with such servers.*

- ➔ *Voicemail, PBX, Telephone Systems.*

b) Backup Utilities and Supporting Tools

All backup processes undertaken by the Company are to utilize approved hardware, software, and other supporting tools for ensuring the confidentiality, integrity, and availability (CIA) of the entire backup platform. Backup utilities are to consist of, but are not limited to, the following:

- ➔ *Backup software*
- ➔ *Backup tapes and tape devices*
- ➔ *Backup library*
- ➔ *Backup disks*
- ➔ *Hard drives*
- ➔ *CDs*
- ➔ *DVDs*
- ➔ *Compact flash drives, SD*
- ➔ *Dynamic Random Access Memory (DRAM)*
- ➔ *Read-Only Memory (ROM and the different variations thereof)*
- ➔ *Random Access Memory (RAM)*
- ➔ *Flash cards*

- ➔ *USB drives, removable media, memory sticks*

As for the backup processes performed, the following are considered acceptable by Company when conducting backups of all necessary data:

- ➔ ***Manual** – Manual backups are those performed by choosing what data to back up, when to backup, and to what device – all in a manual process. Though it creates great flexibility and customization, it's not recommended as a viable long-term solution for any type of environment.*

- ➔ ***Semi-Automated** – Semi automated backups are those performed using backup tools and software, but still require somebody to initiate and launch the backup process itself. The disadvantage of these backups is that they are prone to human error, such as missing a critical time for backups, etc.*

- ➔ ***Completely Automated** – Completely automated backup processes have fast become the norm in many environments, as they effectively ensure the backup process is run on a regular scheduled time, complete with reporting metrics and other critical information.*

c) Types of Backups and Default Backup Scheduling

It's critically important to design and deploy a backup process that's comprehensive, efficient, and includes backups on a regular basis for ultimately ensuring the confidentiality, integrity, and availability (CIA) of organizational data. The following types of backups are to be utilized for Company's backup process:

- ➔ ***Full*** *– A full backup is simply a complete backup of all data. It's the most comprehensive and time-consuming type of data, yet it ensures a complete backup of everything has been undertaken.*

- ➔ ***Differential*** *- A differential backup provides a backup of files that have effectively changed since the last full backup was performed. A differential backup typically saves only the files that are different or new since the actual last full backup, but this can vary in different backup platforms.*

- ➔ ***Incremental*** *– An incremental backup is essentially a backup of all the files, or parts of files that have changed since the previous backup was conducted, regardless of the type of backup (Full, differential, or incremental).*

Additionally, backup activities for full, differential, and incremental are to take place on an as-needed basis, such as in the following manner:

- ➔ *Full: At a minimum, once a week.*
- ➔ *Differential: At a minimum, daily.*
- ➔ *Incremental: As necessary.*

d) Backup Exceptions

Any exceptions to the types of backups and the default backup scheduling are to be approved by authorized personnel, with a valid and justified reason. Additionally, such exceptions – which are ultimately changes to the backup process – are to be submitted with a formal change request, reviewed and approved by authorized personnel. Furthermore, changes to any of the tools and utilities used for the backup process also require the use of a documented change request, initiated by select personnel only.

The backup platform is a critical component of the organization's information technology infrastructure, thus great care and due diligence must be enacted when involving changes to its process.

e) *Backup Reporting Metrics*

Backup reporting activities, for all types of backups (i.e., Full, Differential, Incremental, etc.) are to be monitored on a regular basis for ensuring the success of the backup process itself. Specifically, all backups conducted are to generate reporting metrics for which authorized personnel are to review in a timely manner. Such reporting metrics include, but are not limited to, the following:

- ➔ *E-mails confirming the current status and final result – such as success or failure – of the backup.*

- ➔ *Reports generated confirming the current status and final result – such as success or failure – of the backup.*

- ➔ *Portals for which authorized employees can log into for reviewing and confirming the current status and final result – such as success or failure – of the backup.*

Backups that are successful are to be recorded as such, yet backup failures and exceptions are to be handled immediately, with all appropriate steps undertaken for ensuring the timely backup of such data.

Failures and exceptions are delivered via email reports or metrics from the backup utilities notifying authorized employees of such issues. Depending on the nature, severity, and urgency of the backup itself and the resolution for correcting the issue, a thorough analysis is to be undertaken for correcting the issue in a timely manner and for helping mitigate the issue in the future.

f) Backup Storage and Security

Appropriate security measures are to be implemented for backups, which includes all necessary physical security controls, such as those related to the safety and security of the actual backup media – specifically – disks, tapes, and any other medium containing backup data. This requires the use of a computer room or other designated area (facility) that is secured and monitored at all times and whereby only authorized personnel have physical access to the backups. Thus, "secured" and "monitored" implies that the facility has in place the following physical security and environmental security controls:

- ➔ *Constructed in a manner allowing for adequate protection of backups.*

- ➔ *Security alarms that are active during non-business hours, with alarm notifications directly answered by a third-party security service or local police force.*

- ➔ *The use of cages, cabinets, or other designated, secured areas for securing backups.*

- ➔ *Access control mechanisms consisting of traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e. iris, palm, fingerprint scanners/readers). Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are retained for a minimum of [180] days.*

- ➔ *Adequate closed-circuit monitoring, video surveillance as needed, both internally and externally, with all video kept for a minimum of [30] days for purposes of meeting security best practices and various regulatory requirements.*

- ➔ *Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.*

- ➔ *Appropriate power protection devices for ensuring a continued, balanced load of power to the facility for where the backups reside.*

g) Media Management and Quality Control

All backup media is to be clearly labelled, logged accordingly, and rotated as necessary for ensuring all retention periods are adhered to, while also utilizing existing mediums (i.e., tapes, disks, etc.) for writing over and copying as necessary for future backups. Additionally, media management practices for backups also required that strict policies be in place for transporting media to and from the off- site approved facility being used by the Company. As such, an authorized list is to be kept that includes only select personnel allowed to transport and recall media, with no exceptions.

Either in manual form or electronic format, the following information is to be recorded regarding backups:

- ➔ *Name and unique identifying number of backup medium*
- ➔ *Contents of the backup*
- ➔ *Data classification of backup*
- ➔ *Location of where it is being stored*
- ➔ *Origination of backup – where the medium initially came from.*

If backups are being transported, the following is to be recorded:

- ➔ *Purpose*
- ➔ *Name of individual requesting backup*
- ➔ *Intended destination*
- ➔ *Date of release*
- ➔ *Date of return*
- ➔ *Any other information deemed relevant*

As for quality control initiatives, backups are to be used until they reach a point far in which the quality of the data may come into question, ultimately to avoid media failures. At any time, if the quality of media becomes an issue, the data is to be immediately removed to another medium, with the compromised medium being disposed of in accordance with company policy.

h) Transporting of Media

Transporting backup media is vital for ensuring its safety and security at all times during movement. The following best practices are to be adhered to at all times, when applicable:

- ➔ *Backup media is to be properly packed and stored for ensuring its safety during movement, which means using approved cases and other protective devices.*

- ➔ *Backup media is to be kept away from extreme temperatures, both heat and cold, during movement.*

- ➔ *Backup media is never to be left alone or unsupervised during transportation.*

- ➔ *Only approved transport methods and vehicles are to be utilized.*

- ➔ *Transport is to be in as direct a manner as possible, with no unnecessary stops or deviations from the intended route.*

- ➔ *When necessary, transport of media is to also include additional security precautions as required.*

i) Backup Requests and Retrieval

Backups are to be available in a timely manner for any such requests for restoration. Such requests require written approval by authorized personnel detailing the request, along with all applicable information as necessary. A change request is to be opened for such requests, and approved by authored personnel. As for the restore process, it is to be conducted by authorized personnel who will test for ensuring a complete restoration was achieved, along with conducting any user-acceptance and system testing. Lastly, the restore media is to be promptly returned to the physically secured area for safe storage.

j) Backup Retention Periods and Disposal Procedures

Backup retention periods – regarding backups - are those specifically identified for purposes of restore and recovery of Company data. Thus, it is the responsibility of authorized personnel to ensure the applicable backup retention periods meet all necessary needs of the organization, while also promoting best practices. Conversely, retention periods, such as those defined by contractual, legal and regulatory compliance mandates, are specifically detailed within the Company Data Retention and Disposal Policy, which outlines policies and procedures regarding data retention length and disposal of the actual data itself.

Additionally, please note that when referring to disposal procedures in the context of backups, this specifically applies to the physical devices used for storing such data, and not the actual data itself. Policies regarding disposal of data – the actual information – are also outlined in the Company Data Retention and Disposal Policy. Thus, for purposes of disposal for the actual physical devices used for storing such data, they consist of the following:

- ➔ *Disintegration*
- ➔ *Shredding (disk grinding device)*
- ➔ *Incineration by a licensed incinerator*
- ➔ *Pulverization - Please note that prior to physically destroying any of the actual devices used for storing data, all data must be electronically removed (i.e., wiped, formatted, etc.) as the primary layer of security before being destroyed*

k) Backup Recovery Abilities

On a regular basis, such as quarterly, and no less than twice a year, authorized personnel are to examine, and report on the ability to effectively restore and recover data in the event of such a request. This required examining the facility for which data is being stored for ensuring its overall safety and security. Furthermore, all backup mediums, such as tapes, disks, and other supporting hardware and software utilities, are to be examined for ensuring proper function. Such information and all relevant findings are to be reported upstream to management, with recommendations for improving upon or correcting any issues or concerns.

l) Business Continuity and Disaster Recovery Planning (BCDR)

Documented Business Continuity and Disaster Recovery Planning (BCDRP) is vital to protecting all Company assets along with ensuring rapid resumption of critical services in a timely manner. Because disasters and business interruptions are extremely difficult to predict, it is the responsibility of authorized Company personnel to have in place a fully functioning BCDRP process, and one that also includes specific policies, procedures, and supporting initiatives relating to the safety and security of backups, and supporting systems for which to restore backup data on.

m) Continuous Monitoring of Backup Environment

It's also vitally important to undertake continuous monitoring practices over the entire backup environment for ensuring its confidentiality, integrity, and availability (CIA). As such, authorized personnel are to ensure the following:

➔ *All applicable environments requiring backups have been readily identified.*

➔ *The backup types (full, differential, and incremental) along with the default backups scheduling, is commensurate with the needs of Company.*

➔ *Backup results are being sent to, reviewed, and assessed by authorized personnel.*

➔ *All backup infrastructures – both hardware and software – are performing and function as expected, with no exceptions or deviations regarding performance, accuracy, and other critical measures deemed relevant. Infrastructure, includes, but is not limited to, the following:*

- Backup software
- Tapes
- Tape and library drives
- Other storage and connectivity apparatus

Log and Audit Trail Policy

TABLE OF CONTENTS:

This Log and Audit Trail Policy is intended to ensure that computers and network devices have proper logging to detect, investigate, and remedy events that may be a security hazard or a threat to the organization or personnel.

1. Overview

This Log and Audit Trail Policy is an internal IT policy which provides guidance about what events on computer systems should be logged, how long logs should be retained, who can access the logs, what kind of access to logs should be granted.

2. Purpose

This Policy is required to help ensure the security of servers and the network by providing guidance about the events to be logged, how long logs should be retained, and what access to logs should be granted.

3. Scope

This Policy applies to all servers, network devices, and network security devices which are capable of producing event logs. This policy is effective as of the issue date and does not expire unless superseded by another policy.

4. Audit Log Requirements

a) Security related activity on all servers, firewalls, routers, and workstations must be logged. Examples include:

- ➔ *Unsuccessful login including details such as IP address where the login was attempted from.*

➔ *Successful login including details such as IP address where the login was done from.*

➔ *Account management events when accounts are added, modified, renamed, or deleted.*

➔ *Changes to policy.*

➔ *System shutdown, system startup, or other system security events.*

➔ *User privilege use and attempted use of privileges not granted.*

➔ *Object access. If possible, the user name or ID should be recorded, time of the event, computer or IP address the action was performed from, and success or failure of the action or event.*

b) Audit logs must be retained on all firewalls, routers, and servers for a minimum of six months and recommended for one year. Where laws or regulations apply, logs may need to be retained longer. Business managers are responsible for informing IT management about any laws that apply to data stored on their servers. On workstations, audit logs should be allowed sufficient space to be retained for six months if possible.

c) Audit logs are normally reviewed daily as a part of normal maintenance on servers. This especially applies to firewalls, routers, and servers with sensitive data on them. Servers that have publicly available data may be audited less often with permission but this is not recommended since any compromised server is a serious security threat.

d) All suspicious activity found in logs shall trigger the incident response plan according to policy and shall be investigated.

e) All activity that indicates violation of policy shall be investigated.

f) Audit logs shall not be accessible to users and shall only be writeable by programs with valid reason to write to them. Where possible programs should be able to amend the logs but not delete entries.

g) Permissions on audit logs must be set to prevent unauthorized access to them. The distribution of audit files, in electronic form or printed form is limited to only those who require access and have clearance to view the information.

h) Sensitive information such as social security numbers, credit card numbers, and passwords should either not be retained in logs or should be masked so they cannot be read.

i) Where possible without reducing security, tools should be used to automate auditing and locate patterns in audit files which would point to something requiring attention.

j) Only administrators of the systems and their management should be able to review logs. In the event of a security incident, investigators may be granted full or partial access. Auditors may also be granted access to logs.

k) Sufficient storage must be made available to keep audit logs for the required times at the level of detail specified.

l) All security events that should be invested are to be included in the audit log and include enough information to properly investigate the event including but not limited to the time of the event and the process associated with the event.

Audit logs must be sufficient to support investigations of inappropriate use, intrusions. or any security incidents. Auditing of printer access for forensic investigation of inappropriate use is recommended.

5. Enforcement

Since audit logs are important to check events that affect the security of the organizational network and prevent unauthorized data disclosure, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

6. Other Requirements

a) Procedures for ensuring that automated tools comply with security requirements and auditing requirements must be developed.

b) More detail about what is audited for each system type must be provided. This includes what system, security, and application events are logged on each type of server such as mail server, print server, file server, web server, and others.

c) Additional detail about the level of access for the business need and based on system type and interoperability must be created.

Cyber Security Policy

TABLE OF CONTENTS:

1. Purpose & Background

This Cyber Security Policy is formulated in line with the RBI Master Direction DNBS.PPD. No.04/66.15.001/2016-17 dated June 08, 2017, which mandates NBFCs to implement a robust IT and Cyber Security Framework.

The objective of this policy is to:

a. *Strengthen the information and cyber security posture of KSBCDC.*
b. *Safeguard customer information, corporate data, financial records, and IT infrastructure.*
c. *Ensure compliance with applicable laws, regulations, and RBI directions.*

2. Applicability

This policy applies to:

a. *All employees, directors, contractual staff, consultants, interns, and third-party vendors accessing KSBCDC information systems.*

b. *All computing devices including desktops, laptops, servers, mobile devices, cloud resources, and network equipment owned or operated by KSBCDC.*

All users are collectively referred to as “Users” under this policy.

3. Information Security & Cyber Security

1. Data Protection

   ➔ *Copying of company data into external USB drives or personal devices is prohibited unless approved.*

   ➔ *Storage of customer data on personal cloud storage (Google Drive, Dropbox etc.) is strictly disallowed.*

2. Access Control

   ➔ *User access shall follow the Principle of Least Privilege (POLP).*

   ➔ *Each employee shall use a unique ID and password, never shared with others.*

   ➔ *Users must lock screens when away from desks.*

3. Email & Internet Security

   ➔ *Email services are hosted in a secure manner with anti-phishing, anti-spam, and malware protection.*

   ➔ *Internet access shall be role-based; unwanted websites (gambling, adult, streaming, P2P) are blocked by IT.*

4. Network & System Security

   ➔ *KSBCDC maintains a firewall with intrusion detection/prevention.*

➔ *Regular patch updates and antivirus scanning are mandatory.*

5. Incident Management

➔ *All suspected security incidents (malware, phishing, unauthorized access) must be reported immediately to the IT Officer.*

➔ *A formal incident response process shall be followed, and significant incidents reported to the CISO/MD and Board.*

4. <u>Digital Signature Certificates (DSC)</u>

a. DSCs shall be used only by authorized officers for statutory filings, banking, MCA, GST, PF, DGFT, and other official purposes.

b. Each DSC is password protected and must be securely stored by the assigned officer.

c. Misuse or sharing of DSC is strictly prohibited.

5. <u>Mobile Computing Policy</u>

a. Employees provided with laptops, tablets, or mobile devices are responsible for safeguarding them against loss or theft.

b. Employees are not allowed to bring personal laptops / tablets to the office premises.

c. Devices must have password/PIN/biometric protection.

d. Company-approved antivirus and encryption tools must be installed.

6. Social Media Usage

a. Use of social media platforms via the company network is restricted unless approved.

b. Employees shall not publish:

   ➔ *KSBCDC's confidential information.*
   ➔ *References to customers, partners, or suppliers without approval.*
   ➔ *KSBCDC's logo, trademark, or branding without authorization.*

c. Personal opinions expressed on social media must not be represented as company views.

7. Compliance with Information Security Policies

a. All IT systems shall be used in line with the Information Security Policy and Acceptable Usage Policy.

b. Any exceptions must be approved.

c. Policy exceptions shall be reviewed annually or when new threats emerge.

d. Violations will attract disciplinary action, up to and including termination.

8. Network Level Security

a. KSBCDC network (LAN/WAN) shall not connect to unauthorized external systems without prior approval.

b. Any external connection (e.g., vendor support via VPN) requires management authorization.

c. Wireless access shall be secured with encryption and monitored regularly.

9. <u>Review & Approval</u>

This Cyber Security Policy shall be:

a. Reviewed annually by the Information Security Committee / Risk Management Committee.

b. Updated in response to regulatory changes, emerging threats, or business needs.

c. Approved by the Board of Directors of KSBCDC.

Cyber Crisis Management Plan

TABLE OF CONTENTS:

1. Purpose

The Cyber Crisis Management Plan (CCMP) aims to ensure KSBCDC can effectively respond to and recover from cyber security incidents that could disrupt operations, compromise customer data, or damage reputation. It provides a structured incident response and crisis management framework aligned with RBI’s Master Direction on IT Framework for NBFCs.

2. Scope

This plan applies to:

a. *All KSBCDC employees, contractual staff, consultants, and third parties handling information assets.*

b. *All IT systems, networks, applications, databases, cloud resources, and communication channels.*

c. *All categories of incidents including data breaches, ransomware attacks, phishing, malware outbreaks, denial of service, unauthorized access, insider threats, and IT infrastructure failures.*

3. Crisis Management Objectives

a. **Rapid Detection** – Identify cyber incidents in a timely manner.

b. **Containment** – Limit the spread and impact of the incident.

c. **Eradication & Recovery** – Remove threats and restore normal operations quickly.

d. **Communication** – Ensure timely reporting to regulators, stakeholders, and customers where required.

e. **Learning** – Document incidents, analyse root causes, and strengthen defences.

4. Incident Classification

Incidents will be classified into 3 levels based on severity:

a. ***Level 1** – **Low Impact**: Malware infection on a single PC, spam emails, minor policy violations.*

b. ***Level 2** – **Medium Impact**: Unauthorized access attempts, phishing attacks affecting multiple users, partial service disruption.*

c. ***Level 3** – **High / Critical Impact**: Large-scale data breach, ransomware, full system outage, compromise of customer financial data.*

5. Incident Response Team (IRT)

The Cyber Crisis Response Team (CCRT) shall be activated in case of Level 2 or 3 incidents.

Team Composition:

a. ***Chief Information Security Officer (CISO) / IT Head** – Incident Commander*

b. ***Managing Director (MD)** – Strategic Oversight*

c. ***Business Heads*** *– Assess impact on operations*

d. ***HR & Legal Officer*** *– Ensure compliance, handle disciplinary/legal matters*

e. ***Communication Officer / PRO*** *– Handle customer and media communication*

f. ***External Experts / CERT-In empanelled auditors*** *(if required) – For forensic analysis*

6. Incident Response Process

a. Detection & Reporting

➔ *All employees must immediately report suspected incidents to the IT Officer / CISO.*

➔ *Automated alerts from firewall, IDS/IPS, SIEM, antivirus, or email security must be monitored.*

b. Assessment & Classification

➔ *CISO evaluates severity (Level 1/2/3).*

➔ *If Level 2 or above → CCRT is activated.*

c. Containment

➔ *Isolate affected systems (e.g., disconnect from network).*

➔ *Block malicious IPs, accounts, or emails.*

➔ *Suspend compromised user credentials.*

d. **Eradication & Recovery**

➔ *Remove malware, patch vulnerabilities, restore from backups.*

➔ *Verify integrity of data before restoring systems.*

➔ *Resume services in a phased manner with monitoring.*

e. **Communication & Escalation**

➔ *Inform MD and Risk Management Committee.*

➔ *For critical incidents (Level 3), notify RBI & CERT-In within prescribed timelines.*

➔ *Communicate with impacted customers, if required, in a transparent manner.*

f. **Post-Incident Review**

➔ *Document root cause, lessons learned, financial and reputational impact.*

➔ *Update security controls, policies, and training programs accordingly.*

7. Communication Process

a. **Internal Reporting**: Employees → IT Officer → CISO → MD.

b. **Regulatory Reporting**: RBI, CERT-In, law enforcement (where applicable).

c. **External Communication**: Customers, media, third-party vendors – only through authorized spokesperson (PRO/MD).

8. Business Continuity & Disaster Recovery Linkage

a. This CCMP shall be executed in coordination with KSBCDC's Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

b. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be adhered to.

c. Backup and alternate data centre arrangements must be validated periodically.

9. Training and Awareness

a. All employees shall undergo cyber awareness training on phishing, safe email practices, and incident reporting.

b. Mock cyber drills shall be conducted at least once a year to test preparedness.

10. Review and Approval

a. This plan will be reviewed annually by the IT & Risk Management Committees.

b. Updated based on new threats, vulnerabilities, and RBI/CERT-In advisories.

c. Approved by the Board of Directors of KSBCDC.

BUSINESS CONTINUITY PLAN

TABLE OF CONTENTS:

1. About the company

KSBCDC Ltd is a private limited company fully owned by the Government of Kerala, registered under the Companies Act 1956 on 28-02-1995.

> *Mission: "Freedom from Poverty and Backwardness" of the targeted communities.*

KSBCDC is the State Channelizing Agency of three National Agencies – National Backward Classes Finance Development Corporation (NBCFDC), National Minorities Development Finance Corporation (NMDFC) and National Safai Karamcharis Finance & Development Corporation (NSKFDC).

KSBCDC's Registered Office is at Thiruvananthapuram and the Corporation has 14 District Offices and 20 Sub District Offices.

2. Scope

The Business Continuity Plan is limited in scope to recovery and business continuance from a serious disruption in activities due to non-availability of the Company's facilities. The Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Strategy of this document. This plan is separate from the Company's Disaster Recovery Plan, which focuses on the recovery of technology facilities and platforms, such as critical applications, databases, servers or other required technology infrastructure (see Assumptions below). Unless otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations. The scope of this plan is focused on localized disasters such as fires, floods, and other localized natural or man-made disasters. This plan is not intended to cover major regional or national disasters such as regional earthquakes, war, or nuclear holocaust. However, it can provide some guidance in the event of such a large-scale disaster.

The plan will illustrate how the business can reduce the potential impact of an incident by being prepared to maintain services in the event of the:

- Loss of key premises
- Loss of key staff
- Loss of IT / data
- Loss of telecommunications
- Loss of hard data / paper records
- Loss of utilities (electricity, water, gas)
- Loss of a key partner or supplier
- Disruption due to industrial action
- Disruption due to severe weather

Assumptions:

The viability of this Business Continuity Plan is based on the following assumptions -

1. That a viable and tested IT Disaster Recovery Plan exists and will be put into operation to restore data centre service at a backup site within seven to fourteen days. The business continuity plan will cover three scenarios: for the first 24 hours following an incident and for both 2 - 7 days and 8 - 14 days following an incident. (Recovery plans needed to cover longer periods would normally be developed during the first fourteen days of an incident.)

2. That the Organization’s facilities management department has identified available space for relocation of departments which can be occupied and used normally within two to five days of a facilities emergency.

3. That this plan has been properly maintained and updated as required.

4. The functions and roles referenced in this plan do not have to previously exist within an organization; they can be assigned to one or more individuals as new responsibilities, or delegated to an external third party if funding for such services can be arranged and allocated.

Detailed planning assumptions:

1. In the event of a major incident existing business premises would be out of use for more than 7 days.

2. In the event of a less significant disruption, some of the existing premises would remain in use.

3. Where a generator is not available, loss of electricity supply across a region could last for up to 1-2 days.

4. The mains water supplies and sewerage services may be interrupted for up to 1-2 days.

5. Availability of the IT network historically runs at over 99%. In the event of a partial failure of a server the network could be unavailable for up to 2-8 hours.

6. If the server suite were to be completely lost it could take up to 2 days to restore a limited desktop service (Microsoft package, E-mail and Internet access). Other software could take even longer to restore.

7. Availability of the internal telephone network historically runs at 85 %. In the event of a failure of the iSDX there could be loss of service for up to 3-8 hours.

8. Access to the public telephone network and mobile communications could be lost for up to 1-3 days.

9. In a pandemic 25% - 30% of staff could be off work at any one time. This will include those who are sick, those caring for others and the ‘worried well’ who are simply too scared to come to work. On average people will be absent for 5-8 days, but some may never return.

10. In a fuel crisis only staff involved with delivering critical services are likely to have priority access to fuel.

3. Goals and objectives

The objective of the Business Continuity Plan is to provide a reference tool for the actions required during or immediately following an emergency or incident that threatens to disrupt normal business activities and also to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities (office building) disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters and also now the pandemic situations like COVID-19.

An emergency is an actual or impending situation that may cause injury, loss of life, destruction of property, or cause the interference, loss or disruption of an organization’s normal business operations to such an extent it poses a threat.

An incident is any event that may be, or may lead to, a business interruption, disruption, loss and or crisis.

A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization’s ability to deliver essential business services.

The priorities in a disaster situation are to:

1. *Ensure the safety of employees and visitors in the office buildings.*

2. *Mitigate threats or limit the damage that threats can cause.*

3. *Have advanced preparations to ensure that critical business functions can continue.*

4. *Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.*

The plan will help to include an adequate level of detail used to maintain the business and:

1. *To ensure a prepared approach to an emergency/incident.*

2. *To facilitate an organized and coordinated response to an emergency / incident.*

3. *To provide an agreed framework within which people can work in a concerted manner to solve problems caused by an emergency / incident.*

The plan will also help to identify actions that could be taken in advance of an emergency or incident to reduce the risk of it happening.

The company's Business Continuity Plan includes procedures for all phases of recovery as detailed in the below sections.

4. Key business functions and recovery priorities

Information listed here is used to recover essential business processes. Information should include key processes, IT systems, and data backups.

Key business functions of the company:

1. Receipt of application forms for various types loans along with basic documents of proofs in physical form.

2. Data entry of loanee particulars, scrutiny and data entry of security documents including obtaining legal report and valuation of property.

3. Processing fee collection and execution of hypothecation agreement.

4. Disbursement of loans by District/Sub District offices.

5. Making entries of transactions of collection and disbursements in the Loan software.

Critical assets of the company include:

1. Employees, management personnel and visitors of the company such as customers, consultants etc.

2. IT systems and accessories.

3. Cash-in-hand held at the office.

4. Application software such as bcdconline (a loan management software which is maintained in cloud server at Kerala IT Mission) and tally an accounting software.

5. Office building.

6. Major manual documents such as loan documents and other critical permanent files of the company.

Recovery priorities:

1. The safety of employees and visitors in the office buildings within a few minutes of the incident occurred.

2. Mitigate the threats / vulnerabilities affecting the IT systems and application software by having an offsite centre as back up site within 2- 5 days.

3. Safely shifting of manual files to an offsite centre within 1- 2 hours’ time.

4. Other safety measures such as equipping the fire alarms / fire extinguishers and sprinklers in case of fire in the office premises.

5. <u>Business impact analysis</u>

Business Impact Analysis team (BIA team) shall be formed under the direction of Board of Directors / senior management of the Company. The Board has to fix the maximum allowable downtime depending upon the risk tolerance that can be afforded by the Company on critical assets and to bring back the facilities to the normal site for normal functioning of the business.

BIA team shall assess severe business impacts on accounts of any disaster / disruption of normal operations such as:

1. *Cash flow interruption*
2. *Increase in customer dissatisfaction*
3. *Loss of income*
4. *Loss of Equipment or data*
5. *Delay or loss of new business*
6. *Inoperative financial controls*
7. *Increases in liability*
8. *Loss of Public image*
9. *Regulatory fines etc.*

6. An overall plan to maintain operations

This section is a more comprehensive area of the company's business continuity plan. The operations shall be broken down into three strategies -

a. Preventive strategies
b. Response strategies
c. Recovery strategies

a. Preventive Strategies:

The company’s preventive measures that should be taken before a disruption occurs are as follows:

- ➔ Creating a remote work solution for the employees.
- ➔ Having backup utility providers
- ➔ Alternative network resources
- ➔ Data backups / cloud facility
- ➔ Server backups

b. *Response Strategies:*

This is the strategy where a plan of action is needed when an emergency or sudden disruption of business occurs. All the employees and management personnel shall be responsible in this stage. The response measures include:

- ➔ Evacuation of human life
- ➔ Evacuation of critical assets such as cash and other permanent manual files, hard disks, forms, regulatory documents etc.
- ➔ Safety protocols
- ➔ Effective staff communications on the disaster occurred

c. *Recovery strategies:*

In this strategy, the company shall ensure that all critical business processes are restored after an emergency event or major disruption in business. The detailed recovery plan and action with team responsibilities in each phase have been already mentioned in the below sections.

7. Recovery priorities

Recovery priorities matrix for critical business functions and assets:

Assets	**Priorities**	**Maximum allowable downtime**
IT systems	*Critical*	*1-2 days*
Loan software	*Critical*	*1-2 days*
Loan collection process	*Medium*	*3-4 days*
Disbursement process	*Medium*	*3-4 days*
Human life	*Very critical*	*Within minutes*
Permanent manual records	*Critical*	*Within hours*

8. <u>Recovery teams</u>

The recovery team consists of members who will participate in the recovery process for the business continuity plan. The participants are organized into one or more teams. Each team has a designated team leader and an alternate for that person. Other team members are assigned either to specific responsibilities or as team members to carry out tasks as needed.

a. Team roles:

Recovery team consists of the following:

1. Team leader - Managing Director of the company would be the recovery team leader. He / she would co-ordinates the overall actions of the recovery team.

2. Branch team leader: Unit head of the branch would be responsible for the recovery functions in a branch.

3. Team members: two or three staff reporting under General Manager (HRM/ADMIN)/ Unit Head of Branch shall do recovery functions as directed by the respective team leader.

4. Personnel notification on disaster: Employee telephone list has been prepared to notify the team members about the disaster and to allocate their responsibility according to the disaster effect. Additionally, the contact list of outside agencies has been prepared and updated to call based on the criticality of disaster occurrences such as ambulance, fire force, nearest police station, other emergency force etc.

b. Team responsibilities:

1. Business continuity coordinator - General Manager (HRM / ADMIN) / unit head branch of the company shall act as Business Continuity coordinator. The responsibilities of Business Continuity coordinator are to ensure the following activities are successfully completed:

   ➔ *Works with the Emergency Management Team to officially declare a disaster, and start the Disaster Recovery/Business Continuation process to recover the business functions at an alternate site.*

   ➔ *Alert the Company's Senior Management that a disaster has been declared.*

➔ *Assist in the development of an official public statement concerning the disaster. He is authorized to make public statements about organization affairs upon senior management's / directors' approval.*

➔ *Monitor the progress of all Business Continuity and Disaster Recovery teams daily.*

➔ *Present Business Continuity Plan recovery status reports to Senior Management on an hourly basis until critical assets are shifted and after that on a daily basis until back to normal operations.*

➔ *Interface with appropriate work management personnel throughout the recovery process.*

➔ *Communicate directions received from Senior Management to the Emergency recovery team and Business Continuity Team Leaders and members.*

➔ *Provide on-going support and guidance to the Business Continuity teams and personnel.*

➔ *Review staff availability and recommend alternate assignments, if necessary.*

➔ *Work with Senior Management to authorize the use of the alternate recovery site selected for re-deploying critical resources of the Company.*

- ➔ *Review and report critical processing schedules and backlog work progress, daily.*

- ➔ *Ensure that a record of all Business Continuity and Disaster Recovery activity and expenses incurred by the Company is being maintained.*

2. Emergency recovery team - General Manager (HRM / ADMIN) / Unit head branch shall act as the team leader of the emergency recovery team, who acts as an intermediary between senior management and team members. This team is responsible for:

    - ➔ *The safety of all employees.*

    - ➔ *Inspecting the physical structure and identifying areas that may have sustained damage.*

    - ➔ *Expanding on and/or revising the findings of the Preliminary Damage Assessment.*

    - ➔ *Providing management with damage assessment reports and recommendations.*

3. IT recovery team - System Administrator/ IT Consultant shall act as the team leader of this team. This team is responsible for:

    - ➔ *Managing the IT disaster response and recovery procedures.*

    - ➔ *Mobilizing and managing IT resources.*

➔ *Coordinating all communications related activities, as required, with telephone & data communications, PC, LAN support personnel, and other IT related vendors.*

➔ *Assisting, as required, in the acquisition and installation of equipment at the recovery site.*

➔ *Ensuring that cellular telephones, and other special-order equipment and supplies are delivered to teams as requested.*

➔ *Participating in testing equipment and facilities.*

➔ *Participating in the transfer of operations from the alternate site as required.*

➔ *Coordinating telephone setup at the Emergency Operation Centre and recovery site.*

➔ *Coordinating and performing restoration or replacement of all desktop PCs, LANs, telephones, and telecommunications access at the damaged site.*

➔ *Coordinating Disaster Recovery / IT efforts between different departments in the same or remote locations.*

➔ *Training Disaster Recovery / IT Team Members.*

➔ *Keeping Senior Management and the Business Continuity Coordinator appraised of recovery status.*

c. Team contact details:

Recovery team contact list has been prepared and circulated to all employees at Head Office and branches.

9. Recovery plan and actions

This section of the plan describes the specific activities and tasks that are to be carried out in the recovery process of the Company assets. This section transforms business continuity strategies into a very specific set of action activities and tasks according to the recovery phase. All plan activities are completed by performing one or more tasks. The tasks are numbered sequentially within each activity, and this is generally the order in which they would be performed.

a. PHASE I - Disaster Occurrence

1. **First Activity**: Emergency response

   Responsibility of the emergency response immediately after disaster: All the employees and personnel in the office shall take this responsibility as there is only a second's time for this phase. This phase will remain for an hour / two hours after the disaster occurs.

   Tasks:

   - ➔ After a disaster occurs, quickly assess the situation to determine whether to immediately evacuate the building or not, depending upon the nature of the disaster, the extent of damage, and the potential for additional danger.

- ➔ Quickly assess whether any personnel in your surrounding area are injured and need medical attention. If you are able to assist them without causing further injury to them or without putting yourself in further danger, then provide what assistance you can and also call for help. If further danger is imminent, then immediately evacuate the building.

- ➔ Check in with your department manager for a roll call. This is important to ensure that all employees are accounted for.

2. **Second Activity**: Notify the senior management

   Responsibility: Managing Director / Unit Head of Branch

   Tasks:

   - ➔ Team leader informs the members of the management team and notifies the senior management if they have not been informed.

   - ➔ Depending upon the time of the disaster, personnel are instructed what to do (i.e. stay at home and wait to be notified again, etc.)

3. **Third Activity**: Preliminary Damage Assessment

   Responsibility: Unit Head of Branch/ Managing Director at H.O

   Tasks:

➔ Contact the Organization Emergency Response Team Leader to determine responsibilities and tasks to be performed by the Management Team or employees.

➔ If the Organization Emergency Response Team requests assistance in performing the Preliminary Damage Assessment, caution all personnel to avoid safety risks as follows:

- *Enter only those areas the authorities give permission to enter.*

- *Ensure that all electrical power supplies are cut to any area or equipment that could possess a threat to personal safety.*

- *Ensure that under no circumstances is power to be restored to computer equipment until the comprehensive damage assessment has been conducted, reviewed, and authority to restore power has been expressly given by the Emergency Management Team.*

- *Inform all team members that no alteration of facilities or equipment can take place until the Risk Management representatives have made a thorough assessment of the damage and given their written agreement that repairs may begin.*

- *Instruct the Organization Emergency Response Team Leader to deliver the preliminary damage assessment status report immediately upon completion.*

- *Facilitate retrieval of items (contents of file cabinets — petty cash box, security codes, network backup tapes, control books, etc.) needed to conduct the preliminary damage assessment.*

- *Arrange a meeting with the Emergency Management Team and Management Teams from other GROUPS/DEPARTMENTS in the facility (location) to review the disaster declaration recommendation that results from the preliminary damage assessment and to determine the course of action to be taken. With this group, determine the strategy to recommend to Senior Management (the Emergency Management Team Leader will be responsible for communicating this to Senior Management).*

4. **Fourth Activity**: Declaration of Disaster

   Responsibility: Managing Director of the company

   Tasks:

   ➔ Actual declaration of a disaster is to be made by the Emergency Management Team, after consulting with senior management. The Management Team should wait for notification from the Emergency Management Team that a disaster has been declared and that groups/departments are to start executing their Business Continuity Plans and relocate to their Alternate Business Site Location.

- ➔ The person contacted verifies that the caller is someone who is authorized to do the notification.

- ➔ The person contacted notifies the Senior Management, if they have not yet been contacted.

- ➔ In the event the Emergency Management Team cannot be assembled or reached, the Team Leaders from each Management Team at the location should assemble, gather appropriate information, consult with senior management, and make the decision whether to declare the disaster.

- ➔ Because of the significance, disruption, and cost of declaring a disaster, appropriate facts should be gathered and considered before making the decision to declare a disaster. Management Teams should not unilaterally make a decision to declare a disaster. This is the responsibility of the Emergency Management Team.

b. PHASE II - Plan Activation

1. **First Activity**: Notification and Assembly of Recovery Teams and Employees

Responsibility: Unit Head of Branch / Managing Director

Tasks:

- ➔ The team leader calls each member of the management team, instructs them of what time frame to assemble at the Emergency Operations Centre (to be decided at the time), and to bring their copies of the Plan. The EOC may be temporarily set up at any one of several optional locations, depending on the situation and accessibility of each one. Once the Alternate site is ready for occupancy the EOC can move to that location, if preferred.

- ➔ Review the recovery strategy and action plan with the assembled team.

- ➔ The Management Team contacts critical employees and tells them to assemble at the alternate site. If the alternate site is a long distance from the primary site, then individuals should make their own travel arrangements to the alternate site. Non- critical employees should be instructed to stay at home, doing what work is possible from home, until notified otherwise.

- ➔ In the event of a disaster that affects telecommunications service regionally, the Management Team should instruct critical employees to proceed to the alternate site even if they have not been contacted directly. Delays in waiting for direct communications can have a negative impact on the company's ability to recover vital services.

2. **Second Activity**: Relocation to alternate site

   Responsibility: All critical personnel such as Unit Head of Branch/ Managing Director

   Tasks:

   ➔ When instructed by the Management Team, make arrangements to commute or travel to the alternate site.

   ➔ The Management Team needs to consult with the Emergency Management Team and the Organization Emergency Response Team to determine if access can be gained to the primary (damaged) site to retrieve vital records and other materials. The Organization Emergency Response Team will only allow access to the primary site if the authorities grant access. This will be dependent upon the nature of the disaster and the extent of damage.

   ➔ If allowed access to the primary site to retrieve vital records and other materials, perform some pre-planning to determine what is most important to retrieve. This may be necessary since the time you may be allowed access to the primary site may be minimal.

   ➔ Depending on the number of vital records and other materials you are able to retrieve from the primary site, make arrangements to transport this material to the alternate site. If the material is not too great, this could be accomplished by giving to employees to carry along with them. If the material is a large amount, then make arrangements for transport services and/or overnight courier services.

➔ Management and critical employees travel to alternate sites.

3. **Third Activity**: Implementation of interim procedures

   Responsibility: Unit Head of Branch / Managing Director

   Tasks:

   ➔ After arrival at the alternate site, map out locations that can be used for workspace. This should include unused offices and cubicles, conference rooms, training rooms, lunch/break areas, and open space in hallways or in other areas.

   ➔ Obtain additional tables and chairs, either from the office or from outside rental agencies to provide additional workspace. Place in any available open areas, but be cautious of not blocking exits for fire evacuation purposes.

   ➔ Gather vital records and other materials that were retrieved from the primary site and determine appropriate storage locations, keeping in mind effectiveness of workgroups.

   ➔ Develop prioritized work activities, especially if all staff members are not available.

4. **Fourth Activity**: Restoring data processing and data communication with primary or secondary data centres

Responsibility: IT Consultant / System Administrator

Tasks:

- ➔ Contact the Organization Disaster Recovery/IT Team to determine when the data centre is to be recovered, if affected by the disaster. Also, discuss when data communications will be established between the primary or secondary backup data centre and your alternate site.

- ➔ If your alternate site is another entity office, determine if that site has access to the computer systems that the company uses. If so, work with local office management to determine how workstations can be shared between personnel. This may involve using flexible hours.

- ➔ Discuss with the Organization Disaster Recovery/IT Team when and how replacement PC's and/or terminals will be provided to you at the alternate site and when they will be connected.

- ➔ Discuss with the Organization Disaster Recovery/IT Team when the files from your normal PC/LAN servers and applications will be restored and how you can access those files. Also, work with other entity's management at your alternate site to discuss using their LAN servers.

- ➔ Discuss with the Organization Disaster Recovery/IT Team your normal application report distributions, such as when you can expect to receive standard computer reports and how they will be distributed to your alternate site.

- ➔ Communicate the IT recovery status to all personnel who regularly use the systems.

c. *PHASE III - Alternate Site Operations*

1. **First Activity**: Alternate Site Processing Procedures

   Responsibility: Alternate site operation team

   Tasks:

   - ➔ Communicate with customers regarding the disaster and re-solicit phone contacts (in conjunction with the Organization Communications Team)
   - ➔ Acquire needed vital documents
   - ➔ Access missing documents and files and reconstruct, if necessary
   - ➔ Set up operation

d. *PHASE IV - Transition to Primary Operations*

1. **First Activity**: Changing telephone and data communication back to primary site

   Responsibility: IT Consultant / System Administrator

Tasks:

- ➔ Coordinate with the Organization Disaster Recovery/IT Team to determine when it will be relocating back to the primary site. Verify that they have a schedule to ensure that telephone and data communications are rerouted accordingly.

- ➔ Discuss when and how PC's, terminals, and printers, if brought into the alternate site, will be de-installed, moved back to the primary site and re-installed.

2. **Second Activity**: Terminating Alternate Site Procedures

   Responsibility: Unit Head of Branch / Managing director

   Tasks:

   - ➔ Determine which alternate site operating procedures will be suspended or discontinued and when.

   - ➔ Communicate the changes in procedures to all affected staff.

   - ➔ Determine if additional procedures are needed upon return to the primary site, such as to continue resolving work backlogs.

3. **Third Activity**: Relocating personnel, records and equipment back to original site

Responsibility: Unit Head of Branch/ Managing director

Tasks:

- ➔ In conjunction with the Emergency Management Team and the Organization Emergency Response Team, determine when the team will be scheduled for relocating back to the primary site.

- ➔ Communicate this schedule to all personnel.

- ➔ Inventory vital records, equipment and assets that need to be transported from alternate site to the primary site.

- ➔ In conjunction with the Organization Administration Team, make arrangements for a moving company or courier service to transport the boxes back to the primary site.

10. <u>IT system resources</u>

The Company's IT system resources include the following:

1. *Computer and accessories that comprise desktop, keyboard, CPU, UPS, Mouse etc.*
2. *Back up utilities such as hard disk, pen drive etc.*
3. *Network switches/ Router, that enables the network communication within the Head office and Branches*
4. *Internet devices such as Ethernet net cards, Fax /Modems etc.*
5. *Application software such as Tally Accounting software*
6. *Web based software such as Loan software.*

7. *Other devices such as secondary memory devices such as hard disks, pen drives, Bluetooth etc.*

11. Maintenance protocols

In a fast-changing environment, business continuity plan maintenance is an essential part of the business continuity programme and a key component of organizational risk management. Businesses must test, review and adapt the plan regularly to meet emerging risks and challenges. It is an ongoing process, not a point-in-time exercise.

a. *Establishing a Business Continuity Plan Review Schedule that fits the business*

As a broad rule of thumb, the senior management lead for the business continuity management (BCM) programme shall conduct a high-level check every six months on whether the plan still meets its desired objectives. The board and executive team should review the plan annually against the organization’s risk appetite and recovery time objectives. A comprehensive update, including a reassessment of risks and a refreshed business impact assessment, should be undertaken every two years. The business continuity plan should be reviewed when there is any significant change such as a new risk or a significant merger, acquisition or change in personnel to make sure it is still fit for purpose.

b. *Design and Implement a Business Continuity Plan Testing Calendar*

The company shall test IT system backup and disaster recovery regularly. Good backup and disaster recovery service providers will facilitate this and deliver reports detailing performance against recovery time objectives (RTOs) and recovery point objectives (RPOs). Operational management activities such as Employee safety drills like fire alarm testing shall be initiated every six months to train the employees themselves on how to respond when a real fire incident occurs in the office premises.

c. ***Conduct Education and Awareness Training to Business Continuity Management team and the employees***

The company shall initiate the business continuity training programme to the Business Continuity Management team and the company employees at least once a year. Any gaps between what they know and what they need to know should be addressed with education, including refresher sessions as required.

Further the Company shall be alert to the natural changes in personnel and job roles, to ensure that responsibilities don’t fall through the gaps and the corporate memory is maintained when employees leave or change roles.

12. Employee contact list

Employee contact list has been prepared in the Head office and in respective branch offices for duly notification of any important matters with regard to business continuity / disaster recovery.

13. Emergency Operations Centre locations

The location of the Emergency Operations Centre would be in the same city. The alternate place can be a house taken for rental for a limited period until the primary site is back to original form.

14. Insurance coverage to mitigate financial loss

The Company shall take Business Interruption insurance or general insurance coverage to cover any material financial loss occurred due to an abnormal / natural disaster. This is one of the preventive measures that can be taken by the company to compensate for the financial loss that occurred during business disruption.

15. Basic matters to be considered to mitigate the business continuity risk

a. *Offices of the company shall be taken at least at the second floor for the flood prone areas of the building to mitigate the critical assets loss from floods since the company's branch offices have already experienced the difficulties when the 2018 floods came.*

b. *A fire extinguisher and sprinkler shall be placed and regular mock tests shall be made to train and experience how it works when actually a fire occurs at the office premises.*

c. *Regular backup of loan software (even though maintained in cloud server) and tally shall be taken to mitigate the risk of data and information.*

d. *Critical manual files such as sale deeds and other permanent files shall be kept in a fireproof steel cabinet and shall be easily movable when fire or any disaster occurs.*

e. *Strict policy on disabling USB drives and USB Storage devices in the system by all people working in the company’s system.*

f. *Email usage policy shall mitigate inappropriate use of company emails by the employees.*

g. *Unauthorized entry to the company premises and unauthorized access to systems and software or even access to manual documents shall be strictly avoided.*