Cyber Security Policy

Index

Cyber Security Policy

1. Introduction

RBI issued its Master Direction DNBS.PPD.No.04/66.15.001/2016-17 dated June 08, 2017, as part of which it mandated NBFCs to implement IT Framework in accordance with the requirements of the same with effect from June 30, 2018. Additionally, NBFCs need to perform System Audits to assess the effectiveness of this framework annually.

Like all NBFCs, KSIDC is also exposed to variety of operational and transactional risks, including crime, employee fraud, and natural disasters. On account of the large amount of information on the financial transactions gathered from its customers and extensive use of technology to process this information, KSIDC is exposed to specific information and technology and cyber security risk.

To comply with regulatory guidelines, KSIDCs cyber security program should be designed in general to:

- Ensure the security and confidentiality of customer information
- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The NBFC’s cyber security program should be designed specifically to address the following:

- Security compliant IT Architecture / Framework
- Cyber Crisis Management Plan
- Organizational Arrangements
- Cyber Security awareness among Top Management/Board / other concerned parties
- Ensuring protection of customer information
- Supervisory reporting framework

The Board of Directors of the KSIDC is required to be involved in the development and implementation of the Cyber security policy.

In addition to developing a cyber security framework, the KSIDC must train staff to implement the KSIDC's cyber security framework. Further, KSIDC may regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the KSIDC's risk assessment. Tests should be conducted, or results reviewed by independent third parties or staff independent of those who develop or maintain the security programs.

2. Cyber security Policy

The KSIDC is committed to implementing and maintaining an effective cyber security framework, in compliance with the requirements of all relevant laws and regulations. KSIDC is committed to safe and sound NBFC'S operating practices, to properly safeguarding both customer information and proprietary KSIDC information and to preventing unauthorized or inadvertent access to or disclosure of such information

Key focus in Cyber security Policy

2.1 Information security

Protecting information from unauthorized access, use, disclosure, disruption, modification or destruction.

2.2 Cyber security

The protection of connected systems and networks, and the data stored on those systems and transferred via those networks, from attack, damage, or unauthorized access.

2.3 Security controls

Specified measures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

2.4 Critical Infrastructure (CI)

Systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, information security, cyber security, or any combination of those matters.

2.5 Critical information infrastructure (CII)

Information and communication systems on KSIDC's premises as well as in external managed hosting environment, forming part of CI (see above) whose maintenance, reliability and safety are essential for the proper functioning of the CI and / or the KSIDC as a whole.

2.6 Security baselines

The minimum-security standards required for information security systems.

2.7 Cyber security norms

Agreed expectations for the behavior of state actors in cyberspace at an international level - e.g., the need for states to cooperate in preventing international cybercrime.

2.8 Internal threats

Critical & sensitive data compromise, password theft, internal source code review, etc.

2.9 External threats

Denial of service attack (DoS) Distributed denial of service (DDoS), Ransom ware, Malware, Phishing, Spear Phishing, Whaling, Vishing, Drive-by downloads, Browser Gateway frauds, Ghost administrator exploit etc.

The definitions specified in the applicable guidelines by RBI shall be applicable to this policy.

3 Purposes and Objectives of Policy

The primary purposes of KSIDC's cyber security policy are to ensure that the KSIDC, the Board of Directors and Management:

- Understand the risks and threats to which information systems are exposed,
- Evaluate the potential exposures to such risks / threats
- Implement appropriate information security systems and administrative, technical and physical security controls to mitigate such risks, threats and exposures, and
- Test the efficacy of information security systems and controls

Specific objectives of this Policy are to:

- Ensure the accuracy, integrity, security, and confidentiality of customer information received, processed, and maintained by the KSIDC.

- Ensure that such information, and proprietary KSIDC information, is adequately protected against anticipated threats or hazards to its security or integrity.
- Protect against unauthorized access to or use of customer and proprietary KSIDC information that might result in substantial harm or inconvenience to any customer or present a safety and soundness risk to the KSIDC.
- Provide for the timely and comprehensive identification and assessment of vulnerabilities and risks that may threaten the security or integrity customer and proprietary KSIDC information.
- Document process for managing and controlling identified risks.
- Provide standards for testing the Policy and adjust on a continuing basis to account for changes in technology, sensitivity of customer information, and internal or external threats to information security.
- Specify the various categories of Information Systems data, equipment, and processes subject to comprehensive cyber security procedures.
- Ensure the KSIDC complies with all relevant regulations, common law, explicit agreements, or conventions that mandate the security and confidentiality of customer information.
- Ensure protection of the hardware and software components that comprise the KSIDC's Information Systems.
- Protect against the use of the KSIDC's assets in a manner contrary to the purpose for which they were intended, including the misallocation of valuable organizational resources, threats to the Company's reputation or a violation of the law.
- In connection with this general cyber security Policy, KSIDC is conscious of cyber security of the following issues:

o Internet Usage

o Network (i.e., LAN) Configuration Security

o Intrusion, Detection and Response

o Logging and Data Collection

o Threat and Vulnerability Management

o Malicious Code Protection

o Patch Management

- Logical and Administrative Access Control
- Physical Security

3.1 Training

The KSIDC will ensure that all employees of KSIDC, its Board members and management, receive training in the regulatory guidelines and laws governing customer information security and the KSIDC's cyber security procedures, as appropriate to their position at the KSIDC and job responsibilities.

The KSIDC IT department will ensure that the training systems are in place to address

- Initial training for new personnel,
- Continuing review sessions for existing personnel and
- Updated sessions for all affected personnel when any significant revisions are made to the cyber security framework.

3.2 Risk Assessment & Management

KSIDC will implement a comprehensive risk assessment process, including classification, or ranking, of information systems, both electronic and non-electronic, based on the following criteria:

- Nature and sensitivity of information contained in the system, whether non-public customer or proprietary KSIDC information
- Quantity or volume of such information contained in the system
- Impact of the loss of integrity of such information
- Impact of the loss of confidentiality of such information
- Impact of the loss of accessibility of such information
- The risk assessment process will consider for each appropriate information system, the likelihood of occurrence of certain threats and the potential exposure to such threats, and document the existence of administrative, technical, and physical security controls implemented by the KSIDC to mitigate the occurrence and/or potential severity of risks and exposures.
- The data classification and risk assessment will be updated at least annually, and the results of the assessment used in an evaluation of the adequacy of the

KSIDC's information security policies and programs. Results of the data classification and risk assessment will be reviewed with senior management, the Audit Committee, and the Board of Directors.

4. Roles & Responsibilities

The following are integral to the successful execution of KSIDC's cyber security framework and will have the following responsibilities:

4.1 IT Steering Committee

IT Steering Committee needs to be created with representations from various IT functions, HR, Legal and business functions as appropriate. The role of the IT Steering Committee would be to assist the Executive Management in the implementation of the IT strategy approved by the Board. Further,

- Ensure that an appropriate cyber security policy is developed and implemented.
- Review periodic information regarding breaches of cyber security.
- Ensure that annual assessments of risks and threats are prepared, information systems and related data are risk rated and that appropriate reviews are made of related risk management strategies and controls.
- Review regulatory examinations of cyber security and ensure that appropriate action is taken to address comments and recommendations of regulators.

4.2 Audit Committee

- Ensure that appropriate tests and audits of cyber security systems are performed.
- Review reports of cyber security tests and audits and ensure that appropriate action is taken to address identified weaknesses in control.
- Review assessments of outsourced technology vendor performance and controls and ensure that appropriate action is taken to address identified weaknesses in vendor cyber security controls.

4.3 IT department

- Department of the KSIDC responsible for ensuring overall compliance with the cyber security policy, the efficacy of the KSIDC's information security procedures and practices and the assessment of information Security risks and the related adequacy of information security policies and procedures.

- Report any breaches of Information Security to the Chief Executive officer/ Deputy General Manager, Board of Directors, and any applicable regulatory and law enforcement agencies.
- Primarily responsible for the execution of significant elements of the cyber security program, including the maintenance and review of information systems and related reports.
- Responsible for ensuring that the network and network based / accessible systems are secured to protect customer information.
- Responsible for reporting any attempted or successful breaches of security systems to the management.
- Ensure the appropriate installation, maintenance and monitoring of intrusion detection systems and intrusion response procedures.
- Coordinate the implementation of changes and patches to information system software and / or hardware to improve cyber security and maintain appropriate records of such changes and related testing/review documentation and approvals.
- Responsible for the implementation of the KSIDC's cyber security policy and the maintenance of appropriate physical security devices and procedures.
- DGM of the KSIDC and IT Department should function as Cyber Crisis Management Team.
- Head of IT Department will act as Chief Information Security Officer (CISO) of the KSIDC.

4.4 Human Resources Department / Establishment Section

- Responsible for ensuring appropriate cyber security orientation is provided for new employees.
- Ensure new hires and contract personnel are properly vetted and agree to follow KSIDC's cyber security policies.

4.5 Department Heads

- Ensure employees are performing due diligence in protecting customer information.
- Provide input into cyber security policy reviews / updates.

- Responsible for reporting any breaches of cyber security to the IT department.

4.6 KSIDC Employees

- Ensure that customer information is protected on a day-to-day basis.
- Responsible for reporting any breaches of cyber security to their respective business unit manager, the Security Officer and / or the KSIDC IT department

5. Availability and Maintenance of the Cyber security Policy

The cyber security Policy is accessible to all members of the KSIDC staff through either the Human Resources or IT Department. All users of KSIDC's IT resources should be familiar with relevant sections of the policy. Relevant sections of this Policy, and other related policies, as described above, will be available to all employees over the KSIDC's Intranet, along with other relevant Human Resources policies (i.e., confidentiality).

This cyber security Policy is a "living" document that will be revised as required to address changes in the KSIDC's technology, applications, procedures, legal and social imperatives, perceived threats, etc. All revisions to the cyber security Policy will be submitted to, reviewed, and approved by the Information Technology Steering Committee. The KSIDC's Board of Directors must subsequently ratify / approve all changes to the Information Security Policy.

5.1 Compliance with Policy

To ensure compliance with this Policy, KSIDC has developed a comprehensive Cyber security Framework, commensurate with and appropriate for the threats and risks faced by the KSIDC and the nature and scope of its operations. KSIDC's IT department shall ensure compliance with this Policy. In addition, KSIDC will appoint as required from time-to-time appropriate personnel / consultants, to be responsible for the day-to-day execution of the cyber security program, investigation and reporting attempted or successful security breaches and other aspects of the information security program and applicable KSIDC' policies and legal and regulatory requirements.

5.2 Breach of Security

All breaches and attempted breaches of the KSIDC’s cyber security systems and controls will be reviewed by the IT department, documented, and reported to the DGM / CEO and the Board of Directors, as prescribed in this Policy and as required to the appropriate legal and regulatory authorities. If appropriate, a Suspicious Activity Report will also be filed.

5.3 Independent Testing and Audit

KSIDC's information security policies and programs will be independently tested in accordance with the procedures adopted by KSIDC (e.g., internal audit approved by the Audit Committee) and/or agreed upon with an independent third-party (e.g., IS Audit). Cyber security testing (i.e., vulnerability assessments and external penetration testing) and audit procedures will be performed no less often than annually. The specific scope and timing of such testing and audit procedures will be reviewed and approved by KSIDC Audit Committee. The results of testing and audits will also be reviewed by the Audit Committee.

5.4 RBI Guidelines

As per RBI Master Direction on Information Technology Framework for the NBFC Sector, (RBI/DNBS/2016-17/53 Master Direction DNBS.PPD. No.04/66.15.001/2016-17), it is recommended that NBFCs having asset size below INR 500 crore shall have a Board approved Information Technology policy/Information system policy.

NBFCs having asset size more than INR 500 crores shall comply with directions provided under section A of RBI/DNBS/2016-17/53 Master Direction DNBS.PPD. No.04/66.15.001/2016-17.

Report of the working group for setting up of computer emergency response team in the financial sector (CERT-FIN)

6. Cyber security Framework

6.1 Scope of Security

The KSIDC defines an effective level of cyber security as "the state of being free from unacceptable levels of risk or exposure to threats and vulnerabilities." In that regard, the KSIDC will adopt controls and other risk mitigation practices and procedures it believes are appropriate in the circumstances to provide reasonable control and eliminate unacceptable risks. It has, therefore, become essential to enhance the security of the KSIDC from cyber threats by improving the current defense system in addressing cyber risks.

Cyber security risks, threats, vulnerabilities, and exposures of concern to the KSIDC may be summarized in the following categories:

- **Confidentiality of information**
    - This refers to the concerns of privacy of personal and corporate information.
- **Integrity of information**
- This refers to the accuracy of customer information maintained in the KSIDC's information systems.
- **Security of information**
- This includes security of:
    - Computer and peripheral equipment
    - Communications equipment
    - Computing and communication premises
    - Power, water, environmental controls, and communication utilities
    - System software (computer programs) and documentation
    - Application software and documentation
    - Customer and KSIDC Information, both electronic and non-electronic
- **System availability and information accessibility**
    - This area of concern is with the full functionality of systems and the KSIDC's ability to recover from short and long-term business interruptions.

- The potential causes of losses, or breaches of security, are termed "threats." Threats to the KSIDC's information systems may be human or non-human, natural, accidental, or deliberate

6.2 Domains of Cyber security

This policy specifically addresses the following domains, or areas, of cyber security:

- Administrative practices: including information security, cyber security, antivirus, e-mail, Internet access and others.
- Technical systems security: including those securing access to the KSIDC's primary processing equipment, peripheral devices, and operating systems. These include hardware and software security, such as firewalls, network intrusion monitoring systems, network configuration and protocol use, etc.
- Physical security: including the premises occupied by the Information Systems personnel and equipment.
- Operational security: including environmental controls, power back-up, equipment functionality, and other operations activities.
- Security over third-party: technology providers, vendor, management personnel, as well as end users.
- Data communications security: including security over electronic access to communications equipment such as hubs, routers, patch panels, lines, etc.

Many of these features are documented in the KSIDC's general information security policy. Wherever a special emphasis is needed, those are specifically dealt with in this cyber security policy.

7. Program

7.1 Critical Information Infrastructure (CII)

CII may be owned and operated by KSIDC, or they may be owned and operated by another entity or a third party with whom KSIDC has established a business relationship. The following components comprise KSIDC's strategic systems:

- Servers

- Firewalls, Routers, Switches & Modems
- Core banking Software
- Database

7.2 Management of CII

Oversight and management of CII is primarily the responsibility of the IT Department. For in-house CII, day-to-day operations and daily coordination of data input from CII outside the institution are performed by the IT Department. The IT Department is also primarily responsible for the management of third-party technology service providers.

7.3 Physical Access

It is expected that CII not under the direct control of KSIDC, such as those operated by service providers of the KSIDC, will adhere to similar standards as the KSIDC.

7.4 Data Integrity

Input of data to CBS must be subject to appropriate reconciliation and transaction review procedures to ensure that data was input correctly, and that resulting output is correct.

7.5 Data Accessibility

All strategic systems will be backed-up daily to minimize data loss in the event of a system failure or disaster situation. The backup strategy must determine the frequency complete daily backups including redundant backup copies. Daily backups must be stored offsite in a secure environment. At no time should all backup copies of any strategic system reside at a single location. Backup media should be validated on a periodic basis (at least annually) to ensure proper operation.

7.6 Backup Plan

Data backup is the process of backing up – copying into an archive file of computer data so it may be used to restore the original after a data loss event.

- Backup shall be scheduled optimally for frequency as well as timing of each backup.

- The IT Department shall ensure that scheduled periodical backups are regularly carried out.
- Offsite backup shall be taken and preserved away from data center.
- Restoration tests shall be carried out as per prescribed frequency to ensure data integrity of backup files.
- Backup should be systematic as prescribed in KSIDC's backup policy.
- Based on the IT head Approval vendor shall share the backup files through FTP/ Other Secured method.

7.7 Password Controls

Each strategic system should incorporate a comprehensive password control strategy as prescribed in the password policy.

All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards lay down in this IT Framework. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this IT Framework. The Complexity Requirements for setting passwords are as follows:

- A strong password must be at least 8 (Eight) characters long
- It should not contain any of the user's personal information—specifically his/her real name, username, or even company name
- It must be unique from the passwords used previously by the users
- It should not contain any word spelled completely
- It should contain characters from the four primary categories i.e., uppercase letters, lowercase letters, numbers, and characters
- To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change the password every 30 (Thirty) days
- Passwords must not be stored in readable form in computers without access control systems or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them

- Immediately upon assignment of the initial password and in case of password “reset” situations, the password must be immediately changed by the user to ensure confidentiality of all information
- Under no circumstances, the users shall use another user’s account or password without proper authorization
- Under no circumstances, should the user share his/her password(s) with other user(s), unless the said user has obtained from the Digital head the necessary approval in this regard. In cases where the password(s) is shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password was shared

7.8 Virus Protection

The management of KSIDC recognizes the threat computer viruses present to its computer systems and networks. As a result, several steps should be implemented to prevent infection:

- Network protection — KSIDC shall use virus protection software to constantly check for viruses. A complete system scan shall be conducted on a regular, periodic basis
- Desktop protection — KSIDC shall install and use virus protection software for individual desktop protection from viruses.
- User training — The best tool used to prevent a virus attack is using caution when opening email and downloading anything from the Internet. Occasionally, guidelines may be given to all staff containing instructions regarding virus threats.
  IT department should provide for continuous updates of current releases of new virus signatures.

7.9 Disaster Recovery and Business Continuity Planning

The KSIDC must develop and maintain a comprehensive IT disaster recovery plan. A hot-site DR site must also be maintained and be tested annually. Comprehensive Business Continuity Plans for all business units of the KSIDC, in addition to those for IT, must be prepared and updated annually.

- Application Server – Will be taking the snapshot of VM after initial setup and whenever there is a change in dependent.
- Application / Software – Any issues restore the application server with last snapshot.
- Snapshot will be taken and kept in configured retention period

8. Data communication

8.1 Network Access Areas

Network access at KSIDC can be divided into two major areas:

- Local Area Networks (LAN)
- External Access via modems etc.

8.1.1 Local Area Networks

KSIDC uses the term Local Area Network or LAN to refer to a collection of computers physically located together and connected in such a way to allow them to share resources such as printers, disk drives, Internet, and fax connections. A combination of routers and switches may be used to segment the network. LAN equipment is considered part of the CII.

The primary location for most of the LAN equipment at KSIDC is at the KSIDC's Data Center. LAN equipment located in the IT department area should be a secure area. Access to this area should be restricted to authorized personnel from the IT Department and authorized vendor personnel only. Access to server and communications equipment in branch offices must also be secured.

8.1.2 External Access via Modem

Access to certain KSIDC systems shall be available for authorized users through a standard Internet service via the KSIDC's secure telecom network connection.

9. Vulnerability Assessment and Penetration Testing (VAPT)

Vulnerability Assessment is a rapid automated review of network devices, servers, and systems to identify key vulnerabilities and configuration issues that an attacker may be able to take advantage off. It is generally conducted within the network on internal devices. A Penetration Test is an in-depth expert-driven activity focused on identifying various possible routes an attacker could use to break into the network. In-addition with the vulnerabilities it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter. Vulnerability Assessment focuses on internal organizational security, while Penetration Testing focuses on external real-world risk.

The KSIDC shall incorporate VAPT in cyber security processes. This will ensure genuine cyber security as opposed to an illusion of being secure.

10. Cyber Crisis Management Plan

The KSIDC shall have a detailed **C**yber **C**risis **M**anagement **P**lan. The plan will be drawn up with primary focus on the following attributes:

- **Identification**: A detailed record of all known threats based on their media reports publication shall be maintained so as to enable immediate detection of such attacks as and when they occur. The record should, apart from identifying the threat as internal or external, rate them as low, medium, high and very high from a risk perspective.

- **Protection** : Strategy shall be devised to put in protective measures against all identified threats which are known in public domain

- **Detection**: Based on the strategy devised to identify and protect the ecosystem of the KSIDC from all identified and emerging threats appropriate plans shall be drawn to install solutions that detect at a very short notice such attacks as and when they occur.

- **Respond:** An action plan, with clear identification of roles and responsibilities with regard to designations and appropriate escalation matrices, detailing the response mechanism against such attacks shall be drawn up and implemented in letter and spirit.

- **Recover:** A detailed plan with implementation strategy to recover data which was subject to cyber hacks shall be made and put in to effect.

11 Preparation of Inventory of Business IT Assets

11.1 Maintenance of IT assets Inventory

KSIDC should maintain an Inventory register showing the details of all the Business IT assets. The register should be updated on a constant basis in accordance with the purchase and sale of hardware/software solutions. The head of the IT Department is responsible for the upkeep of the said register. However, it is the responsibility of the **CISO** to verify and ascertain the accuracy of the said Inventory register. The inventory registers for business IT assets should consist of the following.

- **Details of all IT assets**: The purchase and sale details of all hardware/software/network devices shall be recorded. Movements of such IT assets within the various branches of the KSIDC shall be recorded in the asset registers.

- **Details of systems containing customer data**: If the customer data is stored in systems other than the CBS server then detailed a record of such systems and servers shall be made in the inventory register. The inventory should also record the time stamp of the user id of the KSIDC personnel who access such systems and servers.

- **Maintenance of associated business applications**: All business applications purchased by the KSIDC with the intention of running parallel to the CBS or for independent execution in order to extract data to be submitted to the regulator or for the own use of the KSIDC shall be recorded in the said inventory register. The purchase license and AMC agreements of such application shall also be recorded and filed in proper order.

- **Criticality of the IT asset:** Appropriate risk rating levels (High, Medium, and Low) should be specified for all IT assets and business applications of the KSIDC. Protocols shall be observed strictly while granting user access to assets whose critical risk rating is high.

11.2 Classification of data/information based on information sensitivity criteria

KSIDC shall practice a classification procedure of data as per Data classification and access control policy wherein data related to the customers or that of the KSIDC.

11.3 Management and protection of Information

KSIDC shall practice a procedure wherein firewalls installed should be upgraded on a constant basis in order to ensure protection to the CBS ecosystem of the KSIDC from external threats.

12 Prevention of access of unauthorized software

12.1 Maintenance of software inventory

A centralized inventory detailing the authorized software(s) and approved applications that have been installed in the KSIDC shall be maintained. In the event of discovery of a suspicious application/software, the centralized inventory will help in identifying whether such application/software was installed with proper authorization or not.

12.2 Control mechanism to block/prevent unauthorized software / application installation

Implement a mechanism to control installation of software / applications on end-user PCs, laptops servers, mobile device etc. Allow user tights only to end user PCs and block any installation of software/application in the PCs without permission from IT department. Adequate firewalls up gradation should be done to prevent installation of unauthorized software and applications through network.

12.3 Auto setting of web browser settings

The web browser settings shall be set to auto update and controls of scripts of networking languages like Java script, Java, ActiveX and .Net shall be disabled when they are not used for running any programs.

12.4 Restriction on internet usage

Usage of internet at KSIDC branch / Head office level on end user PC's, Desktops & laptops that are connected to the KSIDC network should be strictly restricted and all browser activities shall be monitored through the firewall. Access to all restricted /suspicious sites should be blocked in the firewall. A branch shall be allotted only one Email ID on the mail server of the KSIDC for communicating with the head office and for communicating with the customers of the KSIDC on behalf of the KSIDC. The branch manager and in his absence the officer operating in capacity as the manager shall be solely responsible for the Emails sent / receiving on behalf of the KSIDC and should be very careful while receiving mails from unknown source. Necessary directions should be issued to end users regarding operations of the systems having internet access.

13. Environmental Controls

13.1 The KSIDC should ensure that all the critical IT assets are properly secured and installed or stored in places that are safe from natural and man-made threats. As part of ensuring such safety following controls should be implemented. The servers and network accessories should be kept in a protected area such as data center / network racks. Access to the datacenter should be strictly controlled by using biometric access, lock and key, etc. security cameras and fire alarm systems should be installed at all critical areas including branches.

13.2 KSIDC should put in place mechanisms for monitoring breaches / compromises of environmental controls of IT assets in the following manner.

- The temperature variation of the data Centre shall be constantly monitored by IT Department. Automatic SMS should be sent to members of IT Department as and when temperatures in the server room breach tolerable limits.

- The IT Department should ensure that support commitments spelt out in the AMC agreements for data Centre maintenance shall be honored by the companies to whom the AMC contract has been awarded.

- A separate visitors' ledger should be maintained to record the details of entries to data Centre other than IT allowed persons.

- Routine inspection with regard to UPS, Battery water, fire and smoke alarm shall be carried out by the IT Team and malfunctioning with regard to any of these shall be recorded and steps shall be taken to rectify the issues in the shortest time possible.

- The **EDP/DC** shall be a non-smoking zone and any instance of any employee/user smoking within the **EDP/DC** must be severely dealt with.

- Adequate fire extinguishers must be placed at all vantage points and the premises must be kept clean and free of combustible materials all the time.

- Branch Managers or other staff members deputed by managers should ensure the proper functioning of batteries, UPS, systems, CCTV cameras, fire alarm / security systems and should be reported to IT department in case of any fault in functioning

14. Network Management and Security

1. The IT Department should ensure that all network devices for e.g. routers, firewall, switches etc. are configured properly and that such configurations are securely maintained. Access controls should be defined in the firewalls with clear privilege definitions about users who access systems and other applications installed and identified as business IT assets of the KSIDC.

2. The default passwords of all the network devices and systems connected to CBS network or any other critical network offering access to delivery channels or digital payments must be changed immediately after installation. The new password shall remain in the custody of **CISO,** or other team leaders identified by the **CISO** and should be stored in a safe locker.

3. The IT Department shall consider disabling all WLAN /WAP/WACS networks and devices at branch levels and ensuring effective monitoring of such networks and devices though firewall at Data Centre.

The end users at branch level and also the HO should not be allowed to access the server or interface server network of payment delivery channels like RTGS/NEFT/ATM or digital products like Wallet / Mobile App solutions or the CBS network as such. The access to such critical infrastructure should be extended only to members of the IT Department / Application support team on a need basis. Such access should be closely monitored, and an appropriate log must be maintained for effective monitoring.

15. Secure Configuration

1. The firewalls of all critical business IT assets of the KSIDC must be set to the highest levels and evaluations of such configurations must be carried out at periodic intervals. While configuring firewalls, the IT Department should adopt the following practices.

- Initiate an assessment process with which the firewall team analyzes the risk and determines the best course of action to balance the KSIDC's needs with security needs.
- Initiate a testing process to ensure that changes to the firewall have the desired effect.
- Initiate a deployment process for moving the new rule into production after it has been tested.
- Initiate a validation process to ensure that the new firewall settings are operating as intended.
- Initiate a process of reviewing firewall rules at periodic intervals.
- Remove overlapping firewall rules in order to ensure efficiency in the working of firewalls.
- Ensure installation of the latest patches into the firewall as part of up gradation of the firewall.

To reduce the risk exposure of networks, software applications, database servers etc. the IT Department must consider dedicating such infrastructure depending upon their critical rating exclusively for the purpose for which they have been set up.

16. Anti-Virus and Patch management

The IT Department shall evolve a comprehensive Anti –Virus management procedure wherein the following steps shall be taken as part of execution of the procedure.

- Disable all existing end user USB and PS/2 ports and CD drives at branch user levels to discourage the plug-in of secondary memory devices thereby eliminating the threat of virus attacks due to installation of unapproved software/hardware solutions which are not properly scanned.
- In cases where installation of any software or hardware tools is required at branch user level, the said installation must be carried out by the **IT Department** after scanning for viruses in the said tools.
- All end users' systems should be installed with anti-virus solutions and such installed solutions have to be upgraded on a periodic basis.
- Program disks should not be loaned out as these may be returned with virus. If however, it becomes unavoidable, only a copy and not the original disk should be loaned.
- Computer games and other Trojan programs could be one of the main carriers of computer viruses and an unsuspecting easy medium for an intruder to break into the computer system. Playing computer games must not be allowed.
- Incident report must be documented and communicated as per established procedures.
- All employees should be strictly adhered with the guidelines on Antivirus with this document.

17. User Access Control/ Management

For the effective implementation of User access control or management of user access, the IT Department should follow the under mentioned steps.

1. End users working in the branches shall be provided with user rights only.
2. The administrator login should be strictly restricted to IT department people, or the people permitted by them for need to basis.
3. The role level permissions should be defined in the CBS to access various programs and the roles should be assigned to each user in need to basis.
4. KSIDC should put in place a Data Access Control policy.
5. KSIDC should put in place a Password Policy with clear instructions to use complex and lengthy passwords and to use different passwords for different applications.
6. All user Ids related to retired employees and employees who are on long leaves must always remain in disabled status and they must be monitored to see for unauthorized enabled status.
7. Remote Desktop access by Any Desk, Ammy Admin, Team Viewer etc., should be always disabled and should be enabled only with the approval of the authorized officer from IT Department.
8. All such access by using remote control should be recorded and the logs for such access shall be monitored for suspicious activities.

18 Securing mail and messaging systems

The IT Department shall follow the following procedures for securing mail and messaging systems of the KSIDC.

- Employees of the KSIDC shall not be allowed to use the official email IDs of the KSIDC for sending or receiving personal messages.

- All the email IDs of the KSIDC shall be constantly monitored for suspicious email messages.

- The mail server of the KSIDC shall be hosted on a third-party website offering cloud solutions.

- Sufficient awareness shall be imparted to the employees regarding malicious mails like phishing, malware, WannaCry etc. and the dangers involved in the opening of such mails and responding to them.

  Purchase sufficient security certificates and protect KSIDC website.

19 Removable Media Management

The following procedures shall be adopted for managing all removable media.

- As a general rule of this policy, usage of all removable media and secondary memory devices like pen drive, external hard disks etc. shall be strictly prohibited. In case of use in unavoidable circumstances, it shall be done subject to prior approval of the KSIDC IT Department.

- USB ports of the end user systems should be blocked to prevent the usage of removable media.
- Usage of such removable devices for which approval has been received shall be only after scanning of virus or other malware.
- Ensure deletion of data on the removable media after use except the backup media.

20 Cyber security awareness among the Users/ Employees/ Management

- Awareness programs shall be conducted among the employees/Users of the KSIDC with regard to Cyber security crimes and the threats. The employees shall be made aware of all the latest cybercrime related incidents, they shall also be made aware of various cyber threats like malware, phishing, fishing etc. The staff shall be trained to understand the concepts of basic information security controls like preparation of inventory, configuration of firewalls, and regulation with regard to installation of pirated/unauthorized software and also with regard to misuse of removable media. The importance of following appropriate protocols and regulatory compliance shall be stressed upon in particular during such training sessions.

- Cyber security awareness program shall be conducted on half yearly/ annual basis for updating the board members on the basic tenets of IT/Cyber security

21 Customer Education and awareness

Customer should have well aware regarding safe usage of digital products launched by KSIDC, various chances of cyber-attacks, precautions to be taken while using mobile app, ATM cards, E-Com, POS etc., risks involved in sharing of MPIN, TPIN, OTP etc., fraud calls / emails /SMS in the name of KSIDC. To aware the customer KSIDC shall adopt the following procedures.

- Conduct awareness programs.
- Send SMS to customers.
- Send email to customers.
- Paper advertisement / bit notices etc.

22 Backup and restoration

Backups should be taken on a daily basis for restoration purpose in the event of a breakdown. Such backups shall be stored in a separate disk.

KSIDC should prepare a backup policy.

23 Vendors / Outsourcing Risk Management

All agreements related to purchase of hardware /Software solutions must be scrutiny. The responsibility of the KSIDC and that of the service/solution providers must be spelt out in clear terms. The payment terms mentioned in such agreements must be free from any ambiguity whatsoever. The terms related to UAT testing if any and that of AMC must be singled out and they must be strictly adhered to.

- The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints.

- The agreements must be reviewed periodically to ensure compliance of terms mentioned therein.

24 Incident Response Policies

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handling various security incidents. This document discusses the considerations required to build an incident response plan.

This policy is designed to protect the organizational resources against intrusion.

24.1 Incident Response Goals

- Verify that an incident occurred.
- Maintain or Restore Business Continuity.
- Reduce the incident impact.
- Determine how the attack was done in the incident happened.
- Prevent future attacks or incidents.
- Improve security and incident response.
- Prosecute illegal activity.
- Keep management informed of the situation and response.

24.2 Incident Definition

An incident is any one or more of the following:

- Loss of information confidentiality (data theft)
- Compromise of information integrity (damage to data or unauthorized modification).
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Damage to physical IT assets including computers, storage devices, printers, etc.
- Denial of service.
- Misuse of services, information, or assets.
- Infection of systems by unauthorized or hostile software.
- An attempt at unauthorized access.

- Unauthorized changes to organizational hardware, software, or configuration.
- Reports of unusual system behavior.
- Responses to intrusion detection alarms.

24.3 Incident Planning

- Define roles and responsibilities
- Establish procedures detailing actions taken during the incident.
- Detail actions based on type of incident such as a virus, hacker intrusion, data theft, system destruction.
- Procedures should consider how critical the threatened system or data is.
- Consider whether the incident is ongoing or done.

24.4 Incident Response Life cycle

1. Incident Preparation

- Policies and Procedures
  - Incident Response Procedures
  - Backup and Recovery Procedures
- Implement policies with security tools
- Post warning banners against unauthorized use at system points of access.
- Establish Response Guidelines by considering and discussing possible scenarios.
- Train users about computer security and train IT staff in handling security situations
- Establish Contacts
- Test the process.

2. Discovery

- Helpdesk
- Intrusion detection system
- A system administrator
- A firewall administrator
- A business partners
- A monitoring teams
- A manager
- The security department or a security person.

- An outside source.

3. **Notification** - The emergency contact procedure is used to contact the incident response team.

4. **Analysis and Assessment** –

   Many factors will determine the proper response including:

- Is the incident real or perceived?
- Is the incident still in progress?
- What data or property is threatened and how critical is it?
- What is the impact on the business should the attack succeed? Minimal, serious, or critical?
- What system or systems are targeted, where are they located physically and on the network?
- Is the incident inside the trusted network?

5. **Response Strategy**

   Determine a response strategy.

- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker and do we care?

6. **Containment** - Take action to prevent further intrusion or damage and remove the cause of the problem. May need to:

- Disconnect the affected system(s)
- Change passwords.
- Block some ports or connections from some IP addresses.

7. **Prevention of re-infection**

- Determine how the intrusion happened - Determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, and attack due to unpatched system or application.
- Take steps to prevent an immediate re-infection which may include one or more of:
  - Close a port on a firewall
  - Patch the affected system

- Shut down the infected system until it can be re-installed
- Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
- Change email settings to prevent a file attachment type from being allow through the email system.
- Plan for some user training.
- Disable unused services on the affected system.

8. **Restore Affected Systems** - Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following

- Re-install the affected system(s) from scratch and restore data from backups if necessary. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.
- Make users change passwords if passwords may have been sniffed.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real time virus protection and intrusion detection is running.
- Be sure the system is logging the correct items

9. **Documentation** - Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective.
10. **Evidence Preservation** - Make copies of logs, email, and other documentable communication. Keep lists of witnesses.
11. **Notifying Police** - Notify the police if prosecution of the intruder is possible.
12. **Notifying proper external agencies** - Notify The Reserve KSIDC of India, as required by the regulatory guidelines from time to time.
13. **Assess damage and cost** - Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
14. **Review response and update policies** - Plan and take preventative steps so the intrusion can't happen again.

- Consider whether an additional policy could have prevented the intrusion.
- Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident responses procedures detailed and cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?

25. Data Classification and Access Control Policy

25.1 Overview

1. **IT Department Responsibility**: All IT Department employees who come into contact with sensitive internal information of the KSIDC are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily business activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, IT Department employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for IT Department for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications

2. **Addresses Major Risks:** The IT Department data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and

demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect the KSIDC's information from unauthorized disclosure, use, modification, and deletion.

3. **Applicable Information:** This data classification policy is applicable to all electronic information for which IT Department is the custodian.

25.2 Procedure

25.2.1 Access Control

1. Need to Know: Each of the policy requirements set forth in this document is based on the concept of need to know. That is to say that information must be disclosed only to those people who have a legitimate business need for the information.

2. System Access Controls: Proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to the KSIDC's systems and resources. Remote access shall be controlled through identification and authentication mechanisms.

3. Access Granting Decisions: Access to the KSIDC's sensitive information must be provided only after the written authorization of the Data Owner has been obtained. Access requests will be presented to the data owner using the Access Request template. Custodians of the involved information must refer all requests for access to the relevant Owners or their delegates. Special needs for other access privileges will be dealt with on a request-by-request basis. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by the relevant Data Owner in accordance with a system review schedule approved by the Deputy General Manager.

25.2.2 Information Classification

1. Owners and Production Information: All electronic information managed by IT Department must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners should be at the manager level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the KSIDC's management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

2. **Restricted**: This classification applies to the most sensitive business information that is intended for use strictly within the KSIDC. Its unauthorized disclosure could seriously and adversely impact the KSIDC or its customers, its business partners, and its suppliers.

3. **Confidential**: This classification applies to less-sensitive business information that is intended for use within the KSIDC. Its unauthorized disclosure could adversely impact the KSIDC or its customers, suppliers, business partners, or employees.

4. **PUBLIC**: This classification applies to information that has been approved by the KSIDC management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information, and it may be disseminated without potential harm.
5. **Owners and Access Decisions:** Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. IT Department must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

25.2.3 Object Reuse and Disposal

Storage media containing sensitive (i.e., restricted, or confidential) information shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the Deputy General Manager.

25.2.4 Special Considerations for Restricted Information

If restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must conform to data access control safeguards approved by IT Department and KSIDC senior management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information. The KSIDC's employees and vendors must not install encryption software to encrypt files or folders on their own without the express written consent of IT Department Security.

25.2.5 Information Transfer

1. Transmission over Networks: If restricted data of the KSIDC is to be transmitted over any external communication network, it must be sent only in encrypted form as approved by the IT department. Such networks include electronic mail systems, the Internet, etc. All such transmissions must use a virtual public network or similar software as approved by the IT Department.

2. Transfer to another Computer: Before any restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

25.2.6 Software Security

1. Secure Storage of object and source code: Object and source code for any software shall be securely stored when not in use by the developer. Developers must not have access to modify program files that actually run-in production. Changes made by developers must be implemented into production by Technical Operations. Unless access is routed through an application interface, no developer shall have more than read access to production data. Further, any changes to production applications must follow the change management process.

2. **Testing**: Developers must at least perform unit testing. Final testing must be performed by the Quality Assurance team or the target user population.

3. **Backups**: Sensitive data shall be backed up regularly, and the backup media shall be stored in a secure environment.

26 Employee Confidentiality Policy

26.1 Overview

Employee confidentiality policy refers to the disclosure of important information that the KSIDC holds. During the course of everyday business, employees will unavoidably receive and handle personal and private information about customers, partners, and the KSIDC. This policy is designed to set the rules that will protect this information from exposure.

26.2 Scope

This policy affects all employees and others that may have access to confidential information, such as board members, investors, contractors and volunteers.

26.3 Policy Elements

Information that the KSIDC considers confidential and proprietary is undisclosed, valuable, expensive and / or easily replicated. More specifically, information that is classified as confidential includes:

- Customer information (existing and prospective)
- Data of customer transactions
- Unpublished financial information
- Processes, methods, and credit details
- Product / marketing and other undisclosed strategies
- Unpublished forecasts or initiatives that are marked as confidential

- Data entrusted to the KSIDC by external parties
- Documents, processes, or other elements explicitly marked as confidential
- Any other knowledge acquired by employees during their employment

All these types of information must be protected for different reasons – some may be legally binding (e.g., sensitive data) and some constitute the backbone of the business and give it a competitive advantage (e.g., business processes). The disclosure of some kinds of information may expose the KSIDC to increased risk.

In the course of their employment, employees will have various levels of authorized access to confidential information so as to conduct their business. When they do so, the following rules strictly apply:

1. No amount of information will be disseminated to anyone outside of the organization.
2. The disclosure of information inside the organization will be limited to those with authorized access and legitimate reason to require that information.
3. The information will not be used for the personal benefit or profit of the employee or any other except the KSIDC.
4. The employee will have access only to the amount and type of information required for the completion of their job responsibilities and no more.
5. Employees must limit to a minimum the occasions when they take confidential information out of the office
6. When perusing or sharing information through electronic means, all precautionary safety measures must be in effect
7. Confidential information must not be left unattended or unlocked
8. Unauthorized replication of information is prohibited
9. All copies of confidential documents must be shredded when no longer needed

10. Upon separation of employment all confidential information must be returned or deleted from the employee's electronic devices

The KSIDC will take measures to ensure that confidential information is well protected. Those measures include but are not limited to:

- Electronic information will be encrypted
- Databases will be protected with all available security measures
- Paper documents will be safely stored and locked
- Authorization of access will be carefully controlled, usually by senior management
- Employees may need to sign non-compete and/or non-disclosure agreements (NDAs**)**

Confidential information as described above may occasionally have to be disclosed for legitimate reasons, e.g., upon request of the regulator or government. In such cases, a strict procedure must be followed that includes the explicit consent of parties involved (unless they are faced with criminal charges) and the disclosure of only relevant information and no more.

26.4 Disciplinary Consequences

The KSIDC places great importance in this policy. Any non-conformity will bring about disciplinary and, possibly, legal action. The KSIDC may terminate any employee who willfully or regularly breaches the confidentiality guidelines for personal profit. Grave offenses such as theft of information, illegal disclosure of sensitive data etc. will be grounds for immediate for-cause dismissal and may also involve legal consequences.

Any unintentional breach of this policy will be thoroughly investigated and will be punished appropriately depending on its magnitude and seriousness.

This policy is binding even after separation of employment.

27 Guidelines on Anti-Virus Process

A Recommended processes to prevent virus problems:

- Always use the corporate standard, supported anti-virus software installed and centrally administered by IT Department. IT Department should download and update the current virus signatures; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a pen drive or a storage device from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software and run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.