CAPRI GLOBAL

Capri Global Capital Limited

Information & Cyber Security Policy

Policy Document – Ver 1.4

Document No.: CGCL/IT/POL/002

This document is reviewed and approved by "Members of Company Board"during board members meeting held on ________

Purpose

The ‘Information & Cyber Security’ policy serves as the primary IT policy. Its aim is to establish a framework and offer direction to the Information Technology team. This guidance ensures the security of corporate IT systems and applications, in line with regulatory standards. The ultimate goal is to safeguard and uphold the confidentiality, integrity & availability of the company information technology services, applications & data.

Legal Framework

The Reserve Bank of India has vide circular RBI/2023-24/107DoS.CO.CSITEG/SEC.7/31.01.015/ 2023-24 dated November 7, 2023. The NBFC shall set the IT framework which covers IT Governance, IT Policy, Information & Cyber Security, IT Operations, IS Audit, Business Continuity Planning. Capri Global Capital Limited has adopted this document in accordance with RBI Master Direction. This document should be reviewed annually by the Board.

Revision Control

Version	Description	Action	Date
1.2	Included sections for MDM, DLP and SOC	Amendment	15-Apr-2024
1.3	Amendments incorporated based on gap assessment.	Amendment	
1.4	Annual Review(No Changes Made)	Review	Sept-2025

Reviewed By

Version	Name	Designation	Sign
1.4	Sandeep Kumar Jain	CISO	Sandeep Jain Digitally signed by Sandeep Jain Date: 2025.09.18 15:38:11 +05'30'
1.4	Paromesh Chatterjee	CIO	Paromesh Chatterjee Digitally signed by Paromesh Chatterjee Date: 2025.09.08 20:07:01 +05'30'

Approved By

Version	Name	Designation	Sign
1.4	Varun Malhotra	CTO	Varun Malhotra Digitally signed by Varun Malhotra Date: 2025.10.18 10:50:36 +05'30'

Next Review Schedule

Version	Review Interval	Last Review	Next Review
1.4	1 Year	Sept 2025	Sept 2026

Summary of Changes

Version	Change Description
1.3	Included Objectives, Ownership, Straight Through Processing, Remote Access, Audit Trial, Cryptographic controls, Physical Security, CCMP and policy statements basis Gap assessment in accordance with RBI’s Master Direction dated Nov 7, 2023.
1.4	Annual Review (No Changes Made)

Table of Contents

1 Introduction

Information Security, often abbreviated as InfoSec, is the practice of safeguarding information by mitigating information risks. It involves the protection of both physical and electronic information from unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction.

Key aspects of Information Security include:

1) **Confidentiality**: Ensuring that information is accessible only to those authorized to have access.
2) **Integrity**: Safeguarding the accuracy and completeness of information and processing methods.
3) **Availability**: Ensuring that authorized users have access to information and associated assets when required.

Cyber Security refers to the practice of protecting computer systems, networks, devices, and data from digital attacks, theft, damage, and unauthorized access. It encompasses a range of techniques, technologies, processes, and controls designed to safeguard the confidentiality, integrity, and availability of information.

Information Security spans across all verticals and covers every aspect of IT Systems. It requires a comprehensive approach that considers all aspects of the information environment, including technology, policies and procedures, and people. It also requires ongoing monitoring, assessment, and adaptation to address emerging threats and vulnerabilities.

The goal of Information Security is to protect valuable information assets from a wide range of threats, including theft, espionage, and cybercrime. It is necessary to ensure the confidentiality, integrity, and availability of information, whether it is stored digitally or in other forms such as paper documents.

Effective Information Security helps protect sensitive information from being accessed, disclosed, or modified by unauthorized individuals. This includes personal information, financial data, and trade secrets, as well as confidential government and military information. By implementing Information Security measures, organizations can mitigate the risks associated with cyber threats and other security incidents.

This 'Information & Cyber Security' policy is a declaration of managerial intent that establishes a framework and guidelines through rules and procedures for the security of the Company's IT systems and company data. This policy serves as a roadmap for the Company IT team in the design, implementation, and management of IT systems and services. It enables the access, processing, and storage of information vital to the Company's business operations, in compliance with relevant standards, laws and regulations.

1.1 Objectives

1. To create a secure cyber ecosystem for the employees, partners, suppliers, and customers of the Company, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all functions of the company.
2. To ensure that the IT infrastructure deployed for enabling Company's business is adequately protected.
3. To create an assurance framework for the design of security policies and enabling actions for compliance to industry security standards and best practices by way of assessment of people, process and technology
4. To comply with the regulatory requirements under which the Company operates.
5. To enable protection of information while processing, handling, storage & transit to safeguard Company's customer data and for reduce economic losses due to cybercrime or data theft.

6. To maintain an appropriate Security Program including:
    - Conducting regular assessments of the threats, vulnerabilities, and risks to Company's data, applications, networks and operating platforms, including those associated with operational control systems; and
    - Implementing appropriate security controls to address the identified threats vulnerabilities, and risks, consistent with the types of data and systems to be protected and the nature and scope of the Company. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 24 (a)]***

1.2 Scope

The 'Information & Cyber Security' policy is enforced across all IT systems. This includes, but is not limited to, end-user systems, mobile devices, data center services, cloud platforms such as SaaS, PaaS, IaaS, networking equipment, and application servers. Any individual, whether an employee, contractor, or third-party resource, who has either direct or indirect access to the company's IT systems or data, is governed by this policy and are required to adhere to this policy. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 24 (a)]***

1.3 Policy Statement

The Company's IT is required to establish and enforce controls for information security that are technical, procedural, administrative, and operational across all levels. The aim is to safeguard the Confidentiality, Integrity, and Availability of data that is stored and processed within company IT systems. It is also crucial to guarantee that such information is accessible to those who are authorized, whenever necessary.

1.4 Cyber Security Governance

- Company shall identify a Chief Information Security Officer (CISO) responsible for the security of information, information processing systems and cyber security efforts and initiatives.
- Company shall identify a team focused on the management of information security.
- Company shall identify a team responsible for the identification and appropriate response to a cyber-threat / security breach

1.5 Responsibility of Information Security

Although the CISO function of the Company spearheads the operations of Information Security, the obligation to uphold data security and integrity is shared by every person who has direct or indirect access to company data or is involved in the planning, design, implementation or operation of the Company's IT systems and data storage locations.

This responsibility extends to all full-time employees, external contractors, and other third parties associated with the Company's IT function.

1.6 Compliance with IS policy

Leaders of business verticals, owners of IT applications and technology shall participate or facilitate regular audits, at least annually, to ensure the systems and processes comply with the Information & Cyber Security policy. As necessary, additional sections or guidelines may be issued and will be integrated into the Information Security policy document during its renewal periods.

All staff, including employees, contractors, dealers, vendors, third parties, and any other personnel who are part of a service agreement with the Company, are obligated to ensure that customer data, personal data, and the organization's data are not susceptible to data leakage, theft, unauthorized access, or the introduction of viruses and malware into the organization's network.

Non-compliance or violation of the information security policy could lead to punitive action or penalties, depending on the context and severity of the breach. These actions may include, but are not limited to, warnings, suspensions, terminations, or legal proceedings.

2 Information and Cyber Security Policy

As Information security touches every function of business and IT department, information security policy has various sections to address specific requirements of individual functions security areas and together, all these sections form a consolidated and comprehensive Information Security Policy.

2.1 Document Control

Documents are major source of information in any enterprise and the Company is no exception to it. Many documents are being formulated or have been created to record very unique and sensitive information about companies' business model and strategy, underline IT systems and security configurations. If not protected properly, loos documents could lead to major risk to information security.

- Roles and responsibility of formulating/managing/authorizing information sensitive documents must be clearly defined and approved by Senior management of the Company.
- A document must contain relevant information to quantify its existence and relevance into the Company. Document must have details like Title, Classification, Owner, Author, Approver, Reviewer, Date of Publishing, Version details, Approval Status, Circulation List and References.
- Wherever possible, important documents shall have unique document ID assigned and tracked under the document register.
- All these fields are mandatory and must be filled with relevant and correct information.
- Documents must be classified / stored and circulated according to the 'Document Classification Policy'.
- Unclassified and Untagged documents must not be published or circulated. Such documents shall not be considered as authentic under Document Control process.
- Document author cannot be reviewer or approver; the Company must identify individuals or committee to review and approve documents. All approvals must be recorded on document in digital or physical signed format.
- Approved document contents cannot be changed unilaterally; all amendments/changes must be tracked and recorded under document revision control and should undergo re approval process before publishing amendments as final document.
- Every document must have defined review period, not exceeding one year. Reviewed document must be re-signed by approving authorities to affirm reviewed copies.
- All signed documents must be published and made accessible to targeted audiences only.
- Document which became irrelevant or inapplicable shall be taken out from document repository.
- Approved copies of documents must be made available to internal / external auditors during auditperiod or as situation demands.
- Record of all documents, approved as well as discarded must be maintained for document governance and tracking purpose.
- Physical copies of documents must not be left unattended; all such documents should be shreddedimmediately after use.

- Unauthorized access, download, share of secured documents from repository is strictly prohibited. Identified individuals violating this policy will face strict action.
- There are three general categories for technology documents i.e Policy, Process and SOP.
  - Policy- This is high level statement document about management expectations.
  - Process- This document is elaborative or detailed document explaining approach orframework or methodology to achieve policy objective.
  - SOP- The SOP is more of a technical document which is affiliated to process document and follows guidelines issued by policy document.

2.2 Approval Matrix

- For any document to become a policy, approval from Company Board Committee is mandatory.
- For process to be enforced approval from Departmental Head is essential.
- For SOP to be effective, it needs to be reviewed and approved by functional managers with gradeabove VP.

2.3 Password Security

Passwords are very sensitive and critical components under Information Security. Weak or unregulated passwords could lead to severe security risk like system compromise, intrusion, or data theft. Password of any user account including but not limited to Employee id, application id, network devices id, database user, used in the Company network must meet Password Policy of Information Security.

2.3.1 Password policy

- Passwords should be consisted of minimum eight characters.
- Passwords must be complex and should include alphanumeric and mixed case characters i.e., at least one integer (0-9) and one special character (! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , ./) as well as both upper- and lower-case letters of the alphabet.
- The password should not contain the user's name or user-ID or other easily guessable combinations.
- A password must not be created or have common, guessable strings such as @123, @2015, birth date or name of self, family, pet.
- System must maintain password history and shall not the same password to be repeated within a cycle of 13 password changes.
- Password must have max age of 90 days, before forcing users to change password.
- System must notify users about password expiry or IT team shall setup communication channel to made users aware about password expiry.
- Password for any user account must not be changed unless formal request received from authentic user. IT team must maintain record of all requests for change / reset password.
- Initial password shared by IT administrator or help-desk personals must be change as soon as possible by user.
- System must have capability to allow users to change their account password on the login interface (after authentication) and the session must be re-authenticated with the new password.
- Both user-ID and password must be authenticated before allowing access to the Company systems and / or applications.
- Authentication failure message to user shall be indicative such as "Incorrect login" or “Incorrect user-id or password” and not exact such as "Incorrect password".
- Ideal sessions on desktops and servers should be lock-out at 15 minutes and 5 minutes of inactivity

respectively.

- While entering a password it should be masked/hidden and not be visible on the screen.
- User account ID should be locked after the 3 unsuccessful login attempts and should be unlocked by the system administrator manually on approvals.
- User passwords can be shared via a text message on a mobile number to user or to the immediate Reporting Manager on Reporting Manager's official email account in one-on-one communication.
- Sharing and disclosing passwords in open email or other group channels is violation of password policy and strictly prohibited and such exposed account passwords must be changed immediately.
- System account passwords must not be hard coded in software/application/utility in clear text or in human readable format.
- User must maintain complete secrecy about their account passwords and must not share, post, write, or otherwise divulged it in any manner to anyone.
- One user account & password must not be used by multiple users, for any reason. Shared use for credentials is not permitted and is violation of this policy.
- Any user suspecting that their password may have been compromised should immediately change the password and report it to the Information Security officer.
- Audit trails should be maintained by the administrator for all events related to password management. The audit trail must be periodically reviewed for anomalies and resolved promptly.

2.4 Malware Protection

Malware protection is essential and mandatory for all systems including endpoints/laptops/desktops. The Company's IT systems and its data must be protected from any kind of risk involving threats like but not limited to virus, Trojans, spyware, ransomware etc.

2.4.1 Malware detection & prevention

- All internal/ external clients and servers connected physically or remotely to Organization's network shall have anti-malware software installed, configured, activated and updated with the latest version of the malicious code definitions before or immediately upon connecting to the network.
- Anti-malware software on all endpoints must be centrally managed and configured according to this policy.
- Anti-malware software should be capable of detecting, containing, removing, and protecting the Company data against any forms of malicious software, including spy ware, ransomware etc.
- New definition signature updates should be applied to all endpoints as soon as, released by vendor. There should be proper monitoring of the updating of the signatures on servers and clients.
- Antivirus should be configured to perform a full scan on all endpoints at least once a week; it should be properly scheduled, preferably during the lean period of office hours.
- Antivirus must be configured to perform real time scan of all the files as and when they are opened,copied or moved.
- All the emails and its attachments must be scanned as it enters the Company network and before it leaves the server.
- If malicious code is found, the email should be quarantined for investigation by IT team without any notification to the recipients.
- Anti-malicious code solutions shall be installed on the internet gateways for scanning the internet requests for malicious code, software, applets, Active X etc. downloaded from Internet.

- Users should report to system administrator / help desk for any abnormal behavior of the system or in the event virus is not getting cleaned by the anti-virus agent.
- Disabling / deactivating malware protection is strictly prohibited; IT team must configure security control to prevent disabling or uninstall of malware protection software without proper authorization.
- The Company IT team must practice techniques and tools to detect/report/protect unprotected endpoints automatically.
- Any detection of malicious activity on endpoints must be recorded under cyber security incident and tracked according to its impact or affected endpoints.
- The Company IT shall configure IT systems and networks to prevent lateral movement malware infection; any infected system must be isolated from the Company network immediately and reconnected only after completely cleaned or formatted.
- Statistical report on malware protection must be published and shared with IT leadership team at periodic interval.

2.5 Secure Configuration Policy

IT systems are backbone of modern corporate world. While there are immense benefits of running business through digital platform, but it also has its own security risks which could lead to severe threats like but not limited to data theft, identity theft, malware attack which could result into loss of reputation and revenue for any organization.

Secure configuration policy deals with risk areas of IT systems security to reduce attack surface and avoid weak configuration.

2.5.1 Objective

The goal of secure configuration policy is to ensure installed IT systems including servers, databases, network devices meet minimum security parameters to avoid security lapse/weakness in the Company's IT services.

2.5.2 Policy Details

- Installation and management of all IT equipment/applications in the Company must comply to "IT System & Operations" policy.
- Only required and necessary services to be allowed to run on production servers. All servers must be hardened according to approved server hardening process to reduce threat surface attack.
- Production servers must be fire walled and separated from non-production server workload. Only necessary ports should be allowed from external network to sub nets running production servers and databases.
- Any alteration/change in network access rules for production workload must be reviewed and authorized by Information Security Officer or IT Infra head followed by change management process.
- Internet access on servers must be restricted. By default, no server will be allowed to connect internet directly. If required, only specific URL/IP must be allowed to connect after thorough review and approval Information Security Officer / IT Infra Head.
- Removable storage access on all servers must be disabled. If situation demands, such access can beactivated for temporary period only after approval from IT Head / CTO.

- Unsecured web servers/APIs should not be allowed to run on the Company's network; there must be SSL/TLS level protection to secure these services.
- Weak SSL/TLS protocols & chippers must not be actively disabled / removed to enforce strong encryption for in-transit traffic.
- Data on-rest must be encrypted to prevent unauthorized access. This is applicable to in-use production data as well as backup copies.
- Any threat detection / suspicious activity on corporate devices must be tagged under cyber security incident and must be investigate thoroughly to inspect and envisage impact on the Company's IT.
- Default ID/password on servers / network devices must be renamed/disabled. Only delegatedadmin ID must be used to manage/operate IT tasks.
- Privileged IDs/access must be strictly governed and tracked for access to production systems.
- Corporate network must be secure to deny access to unauthorized/unknown devices.
- Broadcasting insecure Wi-Fi on the Company's network is strictly prohibited. IT team must set policies/processes to prevent configuration of insecure Wi-Fi/wireless hotpots.
- Any access to IT systems management console must be controlled; it must be limited to and allowed from identified secure workstations only.
- The Company's IT team and Information security officer must review the configuration of IT systems at periodic interval to identify and fix security gaps.
- Application codes / integrations must not store passwords in human readable format; rather it should be encrypted.
- The Company's IT team must prevent open file shares on company network. Such shares are first target of attackers to spread malicious codes. Such shares must be restricted or stopped to preventlateral movement of treat infection.
- All security agents / services must be tamper proof; services like antivirus, encryption, web access agent must not be allowed to be disabled/deactivated by users/local administrators.

2.6 Log Management

Almost all IT systems generate various types of logs during operational activities. These logs are very essentials as it contains useful information about events happened during operation of IT services and are very crucial for forensic analysis to trace root cause.

2.6.1 Objective

The goal of this policy is to define framework for effective log management of the Company's IT systems and provide guideline for the Company's IT team to capture, store and analyze logs generated by servers, applications, databases, network devices etc.

Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance. The Company will performa periodic risk assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilization – how much capacity is used by services

- Security Events – what activity occurred during an incident, and when
- User Activity – what people are doing with services

2.6.2 Policy details

2.6.2.1 Log Configuration

- All production systems should be configured to capture audit logs to track critical events like stop/start any service, system shutdown event, failed attempts and successful login events, access audit logs, application events etc. along with timestamp of event and source system/IP.
- All logs sources must be secured from unauthorized access/deletion. Any such action must be logged to indicate changes executed in log files.
- Anti-malware logs must be enabled on every system to capture events of protection enable/disabled, full scan performed, definition/software update, detected malware's, file and system disinfection attempts, files quarantined etc.
- Intrusion detection/prevention system events must be logged to collect information about suspicious behavior of processes, identified attacks, actions performed by intrusion prevention system to stop the malicious activities or source.
- Events of all the access through web firewall/gateways should be logged. These logs should include but not limited to all the URLs accessed through web gateway, outbound requests and incoming responses, source of traffic, general classification of web destination, user details and timestamp.
- All events of authentication servers including active directory servers and single sign-on servers should be logged. These logs must include information about but not limited to each authentication attempt, origin of authentication attempt, target service/port, username, success orfailure, timestamp.
- Events of all the access through network firewall should be logged. These logs must include complete details of outgoing requests, source/destination IP address, source/destination port/protocol, connection timestamp, policy/rule applied, and action taken.
- Application servers must log events about to the user authentications, requested URLs, server responses, records accessed by user, action performed and timestamp.
- Database servers must log events related to DB user authentication, connection source, client version/type, action performed/queries executed by users, session period etc.
- Wireless equipment must log events about connecting devices type, MAC ID, timestamp of connections, action performed on connection etc.
- Administrative actions/events also to be logged in systems log such as administrator login/logoff, action performed and timestamp.

2.6.2.2 Log management & analysis

- All production system logs mentioned under log configuration or other which are necessary, mustbe captured and stored in centralized log (syslog) management system.
- Syslog solution must collect, monitor and analyze logs in compliance to regulatory mandates.
- Data collected in syslog must be tamper proof; modification/deletion of logs should not be allowed.
- All collected log data must be retained for at least 90 days in log management system and older

data can be moved into archive before purging after 365 days.

- Care should be taken not to retain log records that are not needed. The cost of long- term retention can be significant and could expose the Company to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.
- At any given point of time, IT team must be able to extract and share evidence on IT log management to internal of external auditor.
- Information security officer/function shall monitor the log database actively to unearth possible threat attacks/data leak on the Company's IT system.
- IT Operations team along with Information security officer/function is responsible for effective management of IT logs and log management system.
- Statistical report on IT system logs must be shared with IT leadership team at regular interval.

2.7 Vulnerability Assessment and Penetration Testing

2.7.1 Overview

Vulnerability Assessment and Penetration Testing, at the Company is necessary to manage the increasing number of threats, risks, and responsibilities. Vulnerabilities are mainly related to security loopholes and bugs in software's/operating systems/applications, if not fixed on time, these vulnerabilities could cause big risk to IT systems and may result in loss of reputation and revenue.

2.7.2 Objective

The goal of this policy is to establish a standard framework for periodic vulnerability assessments and penetration testing of the Company's IT systems. This policy reflects the Company's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

2.7.3 Policy details

- This policy covers IT devices like web/application servers, database servers, network devices like firewall/wireless devices owned or operated by the Company.
- Vulnerability assessment and penetration testing is a mandatory process and shall be performed for all in-scope applications/servers/IT devices.
- VA must be performed biannually, and PT annually, on all critical information systems, particularly those with customer interfaces within the De-Militarized Zone (DMZ*). **[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (a)]***
- The Company shall conduct VAPT on these systems at various lifecycle stages, including pre-implementation, post-implementation, and subsequent to significant modifications*. **[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (a)]***
- Risk-based methodology be employed to determine the necessity and frequency of VAPT for non-critical information systems. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (b)]***
- VAPT shall be conducted by trained and independent Information Security expert. VA is conducted internally while PT is conducted by RBI empaneled auditor. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (c)]***
- New deployments/major code changes must undergo vulnerability assessment and penetration testing to confirm system is secure enough to run production workload.

- Vulnerability assessment and penetration testing of production systems must be performed from internally as well as externally to provide maximum coverage of risk exposure as VA tool able to scan all the services and ports from internal network.
- Vulnerability assessment and penetration testing must be run against all services/applications/ports open/available on IT devices.
- To ensure vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment and penetration testing.
- IT must define fixed matrix of vulnerability assessments and penetration testing according to application criticality; this schedule must be clearly defined in approved vulnerability assessment process and penetration testing note.
- VAPT results must be re validated to ensure applied mitigation have fixed the open risks. A system generated report must be published to confirm system health.
- Vulnerabilities must be categorized, and high severity observations should be fixed on priority.
- Following the implementation of an IT project or system upgrade, VAPT must be conducted within the production environment. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (d)]***
- In exceptional cases where PT is carried out in a test environment, Company is obligated to guarantee that the test environment's version and configuration resembles the production environment. Any discrepancies must be recorded and receive formal approval from the InfoSec Committee. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (d)]***
- While vulnerabilities mitigation is important, impact of the changes must be validated first in non-production environment before moving the changes into production.
- Mitigation related to application components major version upgrade and database service packsmust be carefully executed as it may destabilize whole application.
- All data collected and/or used as part of the VAPT process and related procedures to be formally documented and securely maintained.
- Running applications/workload with known vulnerabilities is big risk and violation of “InformationSecurity” policy.
- Information security officer/function assisted by IT operations team are responsible for maintainingvulnerability free system in the Company’s network.
- Any deviation under this policy must be documented and approved by IT Head / CTO with definedtime to revisit the risk acceptance.
- Statistical report on IT systems VAPT health status must be shared with IT leadership team at regular interval.
- Company to remediate identified vulnerabilities and associated risks promptly through appropriate corrective actions. They must maintain ongoing compliance to prevent the recurrence of known vulnerabilities, including those listed in the Common Vulnerabilities and Exposures (CVE) database. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (e)]***
- Company must have VAPT methodology/process to encompass the definition of scope, extent of coverage, and a standardized vulnerability scoring framework and this protocol shall extend to

information systems of the Company that are hosted within cloud-based environments. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 26 (f)]***

2.8 Patch Management

2.8.1 Overview

Patch management is key process of IT security operations. Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing the Company at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

2.8.2 Objective

This policy works as guideline for the Company's IT team to identify, list and patch known vulnerabilities on allIT systems including endpoints, servers, applications, databases and network devices.

2.8.3 Policy details

- Patch management cannot be selective; all components including operating systems, software's, 3rd party applications must be checked for missing security updates.
- The business impact of implementing patches (or not implementing a particular patch/ change request) are assessed. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 13 (a)]***
- IT Team shall ensure that all the patches are applied and implemented following a secure and structured change management process. This process must ensure that changes are reviewed and receive the necessary approvals in a timely manner. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 13 (b)]***
- All the patches to the application systems or data must be justified by genuine business requirements and must receive documented approval. These patches are to be governed by a comprehensive patch management process to ensure their validity and integrity. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 13 (c)]***
- IT Team should ensure that mechanism is established to recover from failed changes/ patch deployment or unexpected results. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 13 (d)]***
- Company shall ensure that the configurations of information systems and deployed security patches at the DC and DR are identical. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 29 (i)]***
- Tool use for patch management must be equipped with continuous scanning, detecting, reporting and mitigating know security/non-security updates on various endpoints & applications including Windows as well as Linux & MAC.
- Patches must be ranked and priorities for deployment according to severity, scope and relevance.
- Patch management must follow staged approach, all patches must be deployed in non-production systems before deploying it on production environment.
- Change management process must be followed to record changes done on production systems.

- Approved patch management process must clearly define acceptable level of patch levels to tagsystems as healthy, vulnerable or highly vulnerable.
- All patches must be deployed at earliest possible time; IT team must have defined schedule forpatch deployment cycle under approved process note.
- If any zero-day patch for critical vulnerability released, IT team must take steps to apply it onpriority basis.
- All newly configured endpoints/servers/network device must be running latest version of security/non-security patches before commissioning into the Company's network.
- Failure to properly update new system is a violation of this policy. Disabling, circumventing, ortampering with patch management protections and/or software constitutes a violation of policy.
- Unsupported / outdated software's must not be allowed to run on system; IT team must takeadequate measurements to handle such legacy software's.
- Post patch deployment, IT systems can be restarted/force to restart, provided prior notificationand communication send to respective device owner or stakeholders.
- Information security officer/function assisted by IT operations team is responsible maintaining adequate security level of the Company's IT systems.
- Any deviation under patch management process must be clearly documented and approved by IT Head/CTO with defined period of risk acceptance.
- System generated statistical report on IT systems patch health status must be shared with IT leadership team at regular interval not exceeding 1 month.

2.9 Mobile device management

2.9.1 Overview

Mobile devices have become major component of modern enterprise business functions as multiple apps are being designed/developed to work on mobile devices for ease of operation and improvise business functions. Organizations also promotes use of personal mobile devices for business operation purpose to take benefits of mobile technology, but this has open new angle of security risks and if not handled properly,could lead to severe risks like data leak, theft and revenue loss.

2.9.2 Objective

This policy has aim of standardizing framework to allow permissible use of mobile devices for operating, storing and accessing the company data, applications, emails on mobile devices.

2.9.3 Policy details

- Only use of personal mobile devices is permitted under BYOD process to access, operate and store company data.
- Personal devices like laptops, notebooks are not permitted and shall not be used to connect to the Company's network.
- All mobile devices including personal, and company provided, must enroll to the Company's mobile device management before gaining access to Company IT services.
- MDM solution must be centralized platform to control, govern and discard mobile devices from the Company. This solution will capture relevant information like IMEI number, device model, OS, storage, applications, location, battery information to effectively manage enrolled devices.
- Authorized user is permitted to enroll only one mobile device in company MDM solution; if

situation demands, additional device enrolment can be allowed followed by approval from IT Infra Head.

- MDM solution must be configured to authenticate user first, before allowing them to enroll their mobile devices.
- For BYOD devices, mobile device must support containerization to isolate company work files from personal profile. Company data / files must not be visible / shareable with other apps on personal profile.
- Company owned devices must be enrolled as device owner and fully managed by MDM policies, allowing user only functions/applications necessary to complete tasks to support job role.
- MDM enrolled devices must be restricted from transferring/copying company data/files using channels like WIFI, Bluetooth, share apps, OTG storage etc.
- Screenshot on work profile is prohibited and any such attempt is violation of this policy.
- Users enrolling to the Company’s MDM service must accept MDM policy and agree keep their usagein accordance with ‘Acceptable Usage’ policy defined under ‘Corporate IT Policy’.
- MDM enrolled corporate devices / work profiles must not be allowed to download, deploy application / software's from unknown sources. Only whitelisted application approved by the Company’s IT team should be permitted to run on MDM enrolled devices.
- Non-compliant, rooted, jail broken devices are not allowed in the Company. If detected, the Company’s IT team reserves rights to take appropriate action to delete corporate data on such devices without prior notice.
- Users are responsible and accountable for safekeeping company data on personal devices. Any incident led to data risk like device lost, theft/stolen must be immediately notified to IT Team.
- The Company’s IT team has responsibility of disabling access to and delete work profile for users leaving organization.
- The Company’s IT team reserves right to completely wipe enrolled devices to protect and maintain integrity of corporate data.

2.10 Data security & recovery

2.10.1 Overview

Data is at the heart of any organization and information systems are main source of company’s data store. IT system produce, process and store business critical and customer related information which must be protected and maintained in a manner to avoid loss of data which could risk organizations business function and lead to revenue loss.

2.10.2 Objective

The goal of this policy is to identify and report possible risk areas for data security in term of data storage and recovery prospective. This policy defines framework to manage ‘data at rest’, ‘data in transit’, ‘data sharing within the organization’, ‘data sharing outside the organization’, ‘data backup & restore’ etc.

2.10.3 Policy details

- All IT device’s storage location used for storing company data must be encrypted using strong disk level encryption.
- By default, access to removable storage devices must be prohibited on all endpoints. Exception canbe allowed post necessary approvals from authorities.

- Access & ownership of removable storage devices must be tracked and reviewed at periodic interval.
- Data in-transit between endpoints and applications must be secure by applying session encryption technology like transport level security (TLS) 1.2 and above.
- All weak ciphers and protocols must be disabled; application/endpoints should be configured to work on latest version of TLS security.
- Key management procedures should ensure that only authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.
- Key management should include but not limited to key generation, distribution, storage, archiving, destruction, revocation and recovery when lost or corrupted.
- Data in-transit between branch locations and data centre must be secure by applying tunnel encryption technology like site-to-site IP-Sec tunnel.
- Use of insecure file sharing tools like Bluetooth connectivity, Wi-Fi hotspot, 3rd party apps like Share-it is prohibited, and such services must be disabled/removed during commissioning of asset.
- User performing data sharing with internal company users must be cautious and must not be share data with irrelevant user / department. Marking unnecessary mails with large number of recipients is not appropriate and shall not be done.
- Internal share folders must not allow access to anyone/everyone. Only authorized users must be allowed to connect basis defined process.
- Share folder access containing highly critical and sensitive data must be logged under access audit mg-mt.
- Data sharing with user outside organization is not permitted and should be blocked. If necessary, ITteam can temporarily allow this access followed by specific approval from authorities.
- Deliberate attempt to share data is violation of the Company’s Corporate IT Policy, IS Policy and would attract to strict action against involved users.
- Company data must be always backed up inline to backup policy at regular interval and stored in separate encrypted storage or password protected repositories. Recovery of data from backup file must be authorized through secret passphrase.
- Access to backup data must be restricted and only authorized persons from IT team should be allowed to view and recover data from backup repositories.
- The Company’s IT team must take periodic review of backed up data and verify its recoverability time to time basis.
- Any deviation on data security policy must be documented and approved by IT Head/CTO with defined date to re-validate.

2.11 Access Security

2.11.1 Overview

“Access management” is critical process for the Company’s information security. Effective control on access management allows IT team to reduce risk by preventing unauthorized access to business-critical data, IT equipment and systems.

It is essential to develop and implement system and procedures in order to safeguard information and computing resources from threats like unauthorized access, modification, disclosure or destruction thereby,ensuring that information remains accurate, confidential and is available when required.

2.11.2 Objective

The purpose of the "Access Security Policy" is to establish the requirements necessary to ensure that access to and use of the Company's IT resources is managed in accordance with business requirements, information security requirements, and other Company policies and procedures.

2.11.3 Policy details

- The Company encourages role-based access control mechanisms, with unique user-ids attached to roles. In all cases, the employee/ contract staff user identification number must be associated with every access mechanism.
- Access to the Company's IT systems should be allowed according to approved process only. No service,system should allow default or unauthenticated access to anyone.
- Access to information assets shall be allowed only where a valid business need exists. Company shall have documented standards and procedures, which are approved by the ITSC and kept up to date for administering need-based access to an information system. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 19 (a)]***
- Company shall adopt multi-factor authentication for privileged users of critical information systems and for critical activities, basis the risk assessment. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 19 (c)]***
- Personnel with elevated system access entitlements shall be closely supervised with all their systems activities logged and periodically reviewed. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 19 (b)]***
- Access delegation must follow the rule on least privilege, only the level of access required to perform authorized tasks may be approved.
- Ownership of IT systems and service must be defined and documented. Access to critical and sensitive IT systems is based on 'need to know'.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.
- Information Resource owners are responsible for the approval of all access requests. Respective stakeholders must take conscious decisions while reviewing and approving any access request.
- User accounts and access rights for all the Company's IT Resources must be reviewed and reconciledat least annually, and actions must be documented.
- Use of shared accounts is prohibited. Where shared accounts are required, their use must be documented and approved by the respective function owner and information security officer.
- IT team must have defined process to disable/deactivate accounts that have not been accessedwithin a specific period of time.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege andmust only perform the tasks required to complete their job function.

- Wherever possible special access accounts must be enforced with MFA or Dual authentication.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed, abuse of access privilege is strictly prohibited.
- Privilege access to IT systems must be logged and monitored at all times. Audit log of privilegeaccess sessions must be preserved for at least 1 year.
- Remote access to the Company's IT systems must be made through approved remote access methodsemploying data encryption and multi-factor authentication.
- Remote access privilege must be terminated after a defined period of inactivity.
- Network access to production servers/services from untrusted public network must pass throughDemilitarized Zone.
- Separate firewall must be configured to define DMZ from production subnet.
- Access or visibility to the Company's internal network IP schema should not be allowed for externalnetwork.
- Access to all IT resources including servers, firewalls, databases, wireless devices must be configured and managed according to the Company's "IT Systems and Operations" policy.
- Information security officer/functions is responsible for periodic review of all access and documentweak configuration to production system and critical IT resources.
- Summary of access security must be shared with IT leadership team at least once in every sixmonths.

2.12 Cloud Security

2.12.1 Overview

Cloud computing is defined by NIST as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It is composed of five essential characteristics including on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured services. It can be provided at a low level as hosted infrastructure (IaaS), at a mid-tier level as a hosted platform (PaaS), or at a high level as a software service (SaaS). Cloud service providers (CSP) can use private, public, or hybrid models.

In all term, Cloud security is essential to ensure confidentiality, integrity and availability of the Company's Information Systems.

2.12.2 Objective

The goal of this policy is to define framework for identifying, integrating and practicing security measurements for the Comapany's information systems running on 3rd party cloud service providers (CSP).

2.12.3 Applicability

This policy is applicable to all individuals/unit of employee and/or vendor/contractor working with CSP/3rd party vendors for identifying, hosting or running the Company's IT Systems on 3rd party cloud platforms.

2.12.4 Policy details

- This policy addresses all the Company's technology, systems, data and networks implemented in private, hybrid and/or public cloud infrastructures, plus all other the Company's IT assets implemented in cloud services as identified by the Company's IT department.

- All other defined policies and processes of the Company are also applicable to Cloud workload and compliance must be ensured to maintain integrity and security of the Company's Information systems.
- Data security must be the center of focus and Identification/assessment of Cloud Service Providers (CSP) should be done accordingly.
- CSP must ensure that they are compliant with a widely adopted cloud security standard that is acceptable to industry standards and regulatory requirements.
    - ISO/IEC 27017, demonstrated via certification with accreditation.
    - NIST SP 800-53, demonstrated via certification with accreditation; or
    - Level 2 of Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Certification
- CSP must ensure it can demonstrate compliance with a cloud security standard by way of an annual SOC 2 Type II audit conducted by an independent third-party auditor. CSP must demonstrate compliance with security obligations if they are not covered anywhere else.
- CSP must enforce strong password policy. At minimum, it shall meet the Company's password policy guidelines and should also have ability to enable and use multi-factor authentication for secure login.
- CSP must retain logs that are sufficiently detailed to determine who did what when for a period of 90 days online. CSP must provide online GUI access to logs.
- CSP must ensure that all underline infrastructure and services are synchronized with Stratum 1 time server.
- CSP must offer logical and verifiable separation of the Company's IT systems and its network traffic from rest all other tenants and management traffic.
- CSP must facilitate or offer data backup and retention facilities to protect data and IT systems deployed in cloud.
- CSP must implement or offer encryption functionalities for 'data at rest' and 'data in transit'. Encryption algorithm and technology must meet latest industry standards.
- CSP shall have appropriate protection against threats and malware's. Or conduct threat & risk assessments to ensure data security of the Company.
- CSP shall have/offer all technical controls like WAF, firewall, IPS to prevent internet threats and protect cloud workloads.
- The Company's IT shall have approved processes and procedures to review, assess cloud security ofpublic/private cloud.
- All existing operational controls like incident management, change management, inventory etc.must be applied in Cloud operations.
- Report about major changes and incidents involving cloud security should be shared with the Company's IT leadership team.

2.12.5 Disclaimer

While above policy tries to address known risks by applying possible controls on cloud security, some component and underline infrastructure is completely out of control for tenant owner; ensuring cloud security and protecting tenant from all possible threats is responsibility of Cloud Service Providers.

2.13 Information security awareness

2.13.1 Overview

Information security awareness is important for any organization and the Company isn't exception to it. "Information Security Awareness" is a formal process for educating employees about the information systems and security risks involved under Cyber security. A good security awareness program should educate employees about institutional policies and procedures for working with Company's information technology (IT).

2.13.2 Objective

The purpose of this policy is to ensure that all the Company's employees with access to Company data, are taught Information Security Awareness in order to gain an understanding of the importance of securing the Company's data. The Company seeks to establish a culture that ensures that business sensitive data is secure. This policy and associated procedures establish the minimum requirements for the Security Awareness and Training controls.

2.13.3 Policy details

- Educating users and administrators at all levels on the safe and responsible use and handling of information is necessary.
- All employees of the company must be aware of their responsibilities in protecting the data, devices and network of the company.
- Employees must be made aware of Company policies; awareness campaign must cover and educate users about the Company's IT policies and processes.
- The Company's IT Security function is responsible for running security awareness program for internal employees.
- The Company's IT team shall leverage all possible methods like Desktop wallpapers, digital flyers, banners, email communications, Instant chat groups to circulate awareness contents to internal employees.
- The company shall also provide brief training to all employees after conducting gap analysis questioner that will gauge their current knowledge on security areas. Employees will then be trained by individualized programs that will address their weakest areas first.
- Awareness campaign shall be sent out regularly, once every 4 weeks, in form of digital contentsand online training courses.
- The Company's information security officer/function has privilege and may use it to conduct surprise tests on security topics to gauge employee's knowledge of IT security areas.
- Undergoing IT security awareness program is highly recommended, and all employees are expected to complete all training courses received by them within no more than 20 working days.
- If an employee has trouble accessing or completing their training, they must contact their IT support team with no undue delay.
- Failure to appear for IT security awareness training, without justifiable reasons or deliberate attempts of ignorance could lead to internal enquiry or actioned according to employee code of conduct.
- Statistic report of awareness campaigns and employee's knowledge on subject areas must be capture and published with IT leadership team.

- The security awareness training program is subject to yearly review and enhancement based on changes to the information security environment.

2.14 Straight Through Processing

2.14.1 Overview

Straight Through Processing (STP) in Information Technology refers to the automated processing of transactions or data from the initiation point to completion without the need for manual intervention.

2.14.2 Objective

- **T**o streamline operations, reduce processing times, and eliminate errors that can occur with manual handling.
- To increase efficiency, reduce the risk of errors, enhance speed, and lower operational costs.

2.14.3 Policy Details

- Company shall implement Straight Through Processing to ensure the integrity and security of data throughout the transaction lifecycle, minimizing the need for manual intervention and reducing the risk of human error.
- All STP workflows shall be subject to regular security assessments and audits to verify compliance with the Company's information security standards.
- Company shall implement measures that eliminate manual intervention or modification of data during its transfer between processes or applications, particularly in relation to critical systems. **[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 17 (a)]**
- Data transfer mechanism between processes or applications must be properly tested, securely automated with necessary checks and balances, and properly integrated through “Straight Through Processing” methodology with appropriate authentication mechanism and audit trails. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 17 (b)]***

2.15 Secure Remote Access (Controls on Teleworking)

2.15.1 Overview

Secure Remote Access refers to policies, procedures, and technologies that enable employees to access an organization's network, systems, and data from remote locations in a secure manner. This is critical for protecting the organization's assets from unauthorized access, data breaches, and other cyber threats that can arise when employees work outside the traditional office environment.

2.15.2 Objective

- Safeguarding sensitive and confidential information from unauthorized access, disclosure, alteration, or destruction when accessed remotely.
- Maintaining the integrity of IT systems and ensuring that remote connections do not introduce vulnerabilities or compromise system security.

2.15.3 Policy Details

Company is required to:

- Guarantee the security of systems utilized and the remote connections from alternative work locations to the environments containing the Company's information assets. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 20 (a)]***
- Enforce the use of multi-factor authentication for logical enterprise access to critical systems. **[*Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 20 (b)]***

- Establish a system to detect all devices that remotely access or connect to the Company's systems. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 20 (c)]***
- Ascertain that data and information shared/presented during teleworking are secured adequately. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 20 (d)]***

2.16 Audit Trails

2.16.1 Overview

Audit trails refer to a secure, chronological record that provides documentary evidence of the sequence of activities that have affected any operation, procedure, or event within an organization's information systems.

2.16.2 Objective

- Establish accountability by logging actions taken by users, administrators, and automated systems, thereby creating a traceable link between activities and individuals or processes.
- Ensure the integrity of data and systems by providing a means to detect unauthorized or unintended changes, as well as errors in data processing.

2.16.3 Policy Details

- Audit Trail system shall be designed to meet business requirements and audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 15 (b)]***
- Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability and should provide audit trails. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 15 (a)]***
- Company shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 15 (c)]***

2.17 Cryptographic Controls

2.17.1 Overview

Cryptographic controls refer to the use of cryptography to protect information and ensure secure communication. These controls are designed to safeguard data confidentiality, integrity, and authenticity by transforming readable data (plaintext) into an unreadable format (ciphertext) and vice versa.

2.17.2 Objective

- To provide a framework for the secure use of cryptography to protect the confidentiality, integrity, and authenticity of information.
- Implementing cryptographic mechanisms to enforce access controls, ensuring that only authorized users can access certain data or systems.

2.17.3 Policy Details

- Company shall employ strong cryptographic techniques for the protection of sensitive data in transit and at rest, ensuring the confidentiality and integrity of such data.
- Information security to ensure that only approved cryptographic algorithms and key lengths shall be

used.

- Key guidelines for cryptographic control implementation include
  - Compliance with pertinent contracts, agreements, laws, and regulations is mandatory when utilizing cryptographic controls.
  - Sensitive information must be stored exclusively in encrypted format to safeguard its integrity and confidentiality.
  - Measures should be implemented to safeguard cryptographic keys against unauthorized modification, substitution, unintended destruction, or loss. Especially, secret keys linked to symmetric cryptographic algorithms must be shielded from unauthorized disclosure.
- Access to cryptographic keys shall be restricted to authorized personnel only, with appropriate authentication mechanisms in place to enforce this policy.
- Information Security Team shall ensure that key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 16]***
- Company shall adopt internationally accepted and published standards that are not deprecated/demonstrated to be insecure/ vulnerable, and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 16]***

2.18 Physical Security

2.18.1 Secure Areas

- To establish robust physical security for information processing facilities, it is imperative to implement strict measures.
- Information Owners must meticulously control access to designated secure areas within these facilities, ensuring the protection of sensitive information and assets while prioritizing personnel safety.
- The perimeter surrounding the buildings or sites housing these facilities must undergo rigorous fortification to eliminate potential vulnerabilities, thereby thwarting unauthorized intrusions.
- This entails constructing solid external walls and equipping all external doors with sophisticated protection mechanisms such as bars, alarms, and locks to prevent unauthorized access.
- Additionally, it is essential to maintain constant vigilance by securely locking doors and windows when unattended, with particular emphasis on reinforcing ground-level windows.
- Adherence to these physical security protocols is crucial for preserving the integrity and confidentiality of information stored within the facilities.

2.18.2 Equipment

- Robust controls must be devised and implemented to ensure equipment security, aiming to avert potential loss, damage, theft, or compromise of information systems and to maintain uninterrupted business processes. It is imperative to safeguard all equipment against environmental hazards and unauthorized access.
- Employees issued with laptops are individually responsible for their safekeeping, emphasizing the imperative of never leaving laptop screens unlocked when unattended. In the event of a laptop theft, the respective employee must promptly notify their reporting manager and the IT team
- All Company's Equipments must be shielded from power outages and any other disturbances resulting from failures in supporting utilities.
  - Installation of UPS systems, generators, fire suppression systems, and humidity control systems is undertaken to facilitate controlled shutdown or continuous operation of equipment crucial for critical business functions.

- Uninterrupted electrical power supply (UPS) and support utilities services, including air conditioning, heating, ventilation, water supply, and sewage, are ensured throughout all business hours.
- Scheduled maintenance exercises for utility equipment are conducted at specified intervals to uphold operational efficiency and reliability.
- Authorized personnel from the admin team conduct reviews of preventive maintenance activities to ensure compliance and effectiveness.

3 Respond

3.1 Cyber Incident Response and Recovery Management

- The Company shall maintain the classification and assessment of incidents and implement a clear communication strategy and plan to effectively manage these incidents, mitigate exposures, and ensure timely recovery. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 27 (a)]***
- The Company shall evaluate cyber incidents, including conducting forensic analysis if needed, to determine their severity, impact, and root cause. It shall implement both corrective and preventive measures to reduce the negative effects of incidents on business operations. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 27 (b)]***
- The Company must maintain written procedures for incident response and recovery, which should include the identification of key roles for both internal and outsourced staff involved in managing such incidents. (Refer "Cyber Incident Response and Recovery Management procedure" document) ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 27 (c)]***
- The Company should have well-defined communication plans for escalating and reporting incidents to the Board, Senior Management, and, if necessary, to customers. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 27 (d)]***
- The Company should proactively notify CERT-In and RBI in accordance with regulatory requirements. Additionally, the Company is required to report incidents to the Indian Banks – Centre for Analysis of Risks and Threats (IB-CART), established by IDRBT. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 27 (d)]***
- The Company shall develop processes to enhance incident response and recovery capabilities by incorporating lessons learned from previous incidents and from conducting tests and drills. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 27 (e)]***
- The Company should also ensure the effectiveness of their crisis communication plan and process through regular drills and testing with stakeholders, including service providers. ***[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 27 (e)]***
- Effective and orderly response to detected cyber security incidents.
  - Minimization of information loss or theft and service disruption.
  - Learning and knowledge creation for better handling of future incidents.
  - Compliance with legal regulatory and contractual requirements.
  - Appropriate escalation and communication to stakeholders
- The Company will form an incident response team responsible for analyzing and responding to cyber security incidents, as well as coordinating activities related to incident containment and resolution.

- Roles and responsibilities of the incident response teams will be documented and communicated to the team members.
- Incident response procedures, including the roles of staff and outsourced staff handling such incidents, will be documented
- For Critical Cyber Security Incidents, the Cyber Crisis Management Plan shall be followed.

3.2 Cyber Crisis Management Plan

- A Cyber Crisis Management Plan (CCMP) shall be defined, documented, and approved by the Board.
- CCMP shall address the following four aspects:
    - Detection
    - Response
    - Containment
    - Recovery
- The composition of the Cyber Crisis Management Team shall include.
    - CIO
    - CISO
    - Information Security – Co-Ordinator
    - IT GRC
    - Chief Technology Officer (CTO)
    - Chief Compliance Officer (CCO)
    - Chief Financial Officer (CFO)
    - Chief Risk Officer (CRO)

[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 24 (a)]

4 UIDAI Specific Security Policy

4.1 Overview - AUA/KUA Operations

Security of personal identifier information or demographic details processed through information assets handled by the Company employees for providing services, like eKYC process is of paramount importance. The confidentiality, integrity, and availability of these shall be maintained at all times by deploying security controls in line with the Aadhaar Act 2016, Aadhaar Authentication Application Security Standards.

4.2 Objective

The goal of this policy is to outlines the Information Security Controls applicable to the Company (Capri Global Capital Limited) acting as Authentication User Agency (AUA)/KYC User Agency (KUA). In addition to the general Information Security and Cyber Security Policy, this specific section focusses on UIDAI issued security guidelines for the additional security controls and specific measures to protect Aadhaar data collected, stored, and processed by the Company.

Company shall ensure the security of eKYC information assets as listed below:

1) Providing AUAs/KUAs with an approach and directives for deploying security controls for all information assets used in process of for providing services like eKYC.
2) Establishing review mechanism to ensure that the AUAs/KUAs adhere to all provisions of the UIDAI Information Security Policy for AUAs/KUAs.

4.3 Policy Details

4.3.1 Definition -AUA-KUA

Authentication User Agencies (AUA): Authentication User Agency is an organization or an entity using UIDAI provided AADHAAR authentication function as part of its applications to enable business / social services to residents.

KYC User Agencies (KUA): KYC User Agency is an organization or an entity using UIDAI provided AADHAAR authentication and eKYC services as part of its applications to enable business / social services to residents.

An AUA connects to the Central Identities Data Repository (CIDR) through an ASA (either by becoming ASA on its own or contracting services of an existing ASA). AUA/KUA captures/processes demographic data, and/or biometric data in addition to the resident's UID. Since the AUAs handle such PII category sensitive information about residents, it becomes imperative to ensure its security.

4.3.2 Overview - Authentication & eKYC

Aadhaar Authentication is defined as the process wherein, Aadhaar number along with the Aadhaar holder's personal identity information is submitted to the Central Identities Data Repository (CIDR) for matching following which the CIDR verifies the correctness thereof based on the match with the Aadhaar holder's identity information available with it.

The purpose of Authentication is to enable Aadhaar-holders to prove own identity and for service providersto confirm the resident's identity claim to supply services and give access to benefits. To protect resident's privacy, Aadhaar Authentication service responds only with a "Yes/No" and no Personal Identity Information (PII) is returned as part of the response.

The e-KYC service enables a resident having an Aadhaar number to share their demographic information (i.e., Name, Address, Date of Birth, Gender) and Photograph with UIDAI partner organization (called a KYC User Agency – KUA) in an online, secure, audit-able manner with the residents consent. The consent by the resident can be given via a Biometric authentication or One Time Password (OTP) authentication.

The Company has entered into a formal agreement with UIDAI to access Aadhaar authentication services and e-KYC services. To protect the Aadhaar Beneficiary, the data privacy policy of the Company has been defined and formulated.

4.3.3 Data Privacy on Aadhaar and Biometric details

The submission of Aadhaar details by a customer to the Company is voluntary and the Company shall not assist on a customer to produce their Aadhaar details for availing any of the services. In cases where Aadhaar number is offered voluntarily by the customer to the Company, the Company shall seek a declaration by the customer towards the same.

For cases where e-KYC verification is required, the Company shall get an explicit consent from the resident for download of resident demographic details from UIDAI mentioning the purpose for which the details are sought.

The consent shall be in the form of electronically record in an eKYC software application.

The biometric details whenever captured by the Company shall be used only for data exchange with UIDAI which validates the captured biometric data against the biometric data maintained in CIDR (Central Identities Data Repository) against the specific Aadhaar number.

The Company shall use STQC certified devices for processing biometric details of resident as onetime transaction; the biometric details shall not be stored by the Company in any manner and form

A system log wherever required shall be maintained to extract the details in case of disputes. The logs should capture Aadhaar Number, timestamp etc., but will not capture/store the PID (Personal Identity Data)associated with the transaction.

4.3.4 Human Resource

The Company shall appoint a SPOC/team for all UIDAI related activities and communication with UIDAI.

An induction as well as periodic functional and information security training shall be conducted for all the Company's personnel for UIDAI related services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.

All employees accessing UIDAI information assets shall be made aware of UIDAI information security policy and controls.

4.3.5 Access Control

- Only authorized individuals shall be provided access to information assets (such as servers, network devicesetc.) processing UIDAI information.
- The application should have auto log out feature i.e., after a certain time of inactivity (15 mins or as specified in the Company policy document), the application should log out.
- For applications there should be an automatic account lockout policy in case of three consecutive login failures or as per the access control policy/password policy of the organization.
- The local security settings on all the systems shall be aligned and synced with the Active Directory or similarsolutions for policy enforcement.
- If the application is operator assisted, the operator shall first authenticate himself before authenticatingthe residents.

4.3.6 Cryptography

- The Personal Identity data (PID) block comprising of the resident's demographic / biometric data shall be encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication (for e.g., PoT terminal)
- The PID shall be encrypted during transit and flow within the AUA / KUA ecosystem and while sharing this information with ASAs.
- The encrypted PID block should not be stored unless in case of buffered authentication for not more than 24 hours after which it should be deleted from the local systems.
- The authentication request shall be digitally signed by either by the Company or ASA as per the mutual agreement between them.
- While establishing a secure channel to the AADHAAR Authentication Server (AAS) the Company shall verify the following:

a) The digital certificate presented by the AAS has been issued / signed by a trusted Certifying Authority

b) The digital certificate presented by the AAS has neither been revoked nor expired.

c) The Common Name (CN) on the certificate presented by the AAS matches with its fully qualifieddomain name (presently, auth.uidai.gov.in).

- Key management activities shall be performed by ASA to protect the keys throughout their life cycle. The activities shall address the following aspects of key management, including.
  a) key generation.
  b) key distribution.
  c) Secure key storage.
  d) key custodians and requirements for dual Control.
  e) prevention of unauthorized substitution of keys.
  f) Replacement of known or suspected compromised keys.
  g) Key revocation and logging and auditing of key management related activities.

- HSM shall be deployed in the Company's network to store UIDAI issued the signing / encryption keys and other Aadhaar related key management process. Access to HSM shall be restricted and periodic access reviews must be conducted for HSM. HSM shall be working in FIPS 140-2 operational mode for all encryption activities.

4.3.7 Physical and Environmental Security

- The Company servers involved in Aadhaar authentication mechanism should be placed in a secure lockable cage in the Data Centre.
- The premises or facility should be manned by security guards during and after office hours
- CCTV surveillance shall cover the data centers where Aadhaar data is collected, processed, stored, and disposed.

4.3.8 Operational Security

- The Company shall complete the Aadhaar AUA / KUA on-boarding process before the commencement of formal operations.
- Standard Operating Procedure (SOP) shall be developed for all information systems and services related to UIDAI operations. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure; The Operating System as well as the network services used for communication with the PoT terminals shall be updated with the latest security patches.
- Periodic Vulnerabilities assessment (VA) exercise should be conducted for maintaining the security of the eKYC applications. Reports shall be generated and shared upon request with UIDAI.
- AUA / KUA employees shall not intentionally write, generate, compile copy, or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any PID information.
- All hosts that connect to the Aadhaar Authentication Service or handle resident's identity information shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed on such hosts.
- Network intrusion and prevention systems should be in place – e.g., IPS, IDS, WAF, etc.
- AUAs / KUAs shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring.
- Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only.
- The authentication audit logs should contain, but not limited to, the following transactional details:

  a) Aadhaar Number against which authentication is sought.

b) Specified parameters of authentication request submitted.

c) Specified parameters received as authentication response.

d) The record of disclosure of information to the Aadhaar number holder at the time of authentication

e) Record of the consent of Aadhaar number holder for the resident

f) Details of the authentication transaction such as API Name, AUA / KUA Code, Sub- AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-id entity information.

- Logs shall not, in any event, retain the PID, biometric and OTP information.
- No data pertaining to the resident, or the transaction shall be stored within the terminal device.
- The logs of authentication transactions shall be maintained by the Company for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.
- At the end of the period of 2 years, the logs shall be archived for a period of 5 years, or the number of years as required by the laws or regulations governing the Company, whichever is later, and upon expiry of the archive period, the logs shall be deleted except those records which are required to be retained by court or other legal boards for any pending disputes.
- All computer clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation.
- The Authentication server host shall reside in a segregated network segment that is isolated from the rest of the network of the organization; The said server instance shall be dedicated for the Online Aadhaar authentication purposes and shall not be used for any other activities.

4.3.9 Communication Security

In case of a composite terminal device that comprises of a biometric reader without embedded software to affect the encryption of the personal identity data, communication between the biometric reader and the device performing the encryption shall be secured against all security threats / attacks

Terminal devices shall provide different logins for operators. These users shall be authenticated using someadditional authentication scheme such as passwords, Aadhaar authentication, etc.

Each terminal shall have a unique terminal ID. This number must be transmitted with each transaction along with UIDAI assigned institution code for the Company as specified by the latest UIDAI API documents.

A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminal which should be incremented for each transaction processed.

The network between Company and ASA shall be secured. Company shall connect with ASAs through secure private lines. If a public network is used, a secure channel such as SSL or VPN shall be used.

The Company eKYC authentication server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the Company's authentication server from all sources other than AUAs / KUAs PoT terminals.

Special consideration shall be given to Wireless networks due to poorly defined network perimeter. Appropriate authentication, encryption and user level network access control technologies shall be implemented to secure access to the network.

Use of public web-based e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy.

UIDAI should be informed about the ASA, The Company has entered into an agreement with

4.3.10 Information security - Incident reporting

The Company shall be responsible for reporting any security weaknesses, any incidents, possible misuse, or violation of any of the stipulated guidelines to UIDAI immediately.

Company's Incident Management Policy shall be adhered in the event of an incident.

4.3.11 Application Security

All of the applications developed by AUA/KUA, or authentication applications being used by AUA/KUA developed by third party vendor must adhere to Aadhaar Authentication Application Security Standard (AAASS), the standard applies to all entities that perform Aadhaar authentication and store, process or transmit Aadhaar number holder data.

Application shall be certified by STQC or CERT-In empaneled.

Source code review shall be conducted on the application and the report of the same shall be maintained.

Aadhaar Authentication Application Security Standard includes technical and operational requirements set by the Unique Identification Authority of India (UIDAI) to protect Aadhaar number holder data. The standard also provides developers with standard best practices and testing requirements to build a secure application by leveraging other standards and best practices such as PA-DSS, OWASP Top 10, OWASP MASC,SANS 25 etc.

The standard is applicable to web-based applications, mobile applications and thick client applicationsleveraging Aadhaar authentication.

Prior to deployment of the application in the production environment, a requesting entity shall ensure thatthe application meets all the requirements of the AAASS satisfactorily.

4.3.12 Audit Trails and Logging

- Implement logging controls on trusted systems, such as servers, to ensure the integrity and reliability of log data, enhancing the security of the logging process.
- Ensure that logs contain essential event data, capturing both successful and failed security events, to provide comprehensive visibility into system activities and potential threats.
- Logging controls should be meticulously implemented to support the recording of critical security events, helping to detect and respond to security incidents effectively.

4.4 UIDAI Compliance

- The Company shall comply with all terms and conditions outlined in the UIDAI AUA / KUA agreement and AUA / KUA compliance checklist.
- The Company shall ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis and on a need basis to ensure compliance with UIDAI standards and specifications. The audit report shall be shared with UIDAI upon request
- If any non-compliance is found as a result of the audit, management shall:
- Determine the causes of the non-compliance.

- Evaluate the need for actions to avoid recurrence of the same.
- Determine and enforce the implementation of corrective and preventive action.
- Review the corrective action taken.
- The Company shall use only licensed software for UIDAI related infrastructure environment. Record of all software licenses shall be kept and updated regularly.
- The Company and its partners shall ensure compliance to all the relevant laws, rules, and regulations, including, but not limited to, ISO27001:2013 Standard, Information Technology Act 2000 and 2008 amendments, Aadhaar Act, 2016 and Regulations.
- It is recommended that AUA / KUA shall deploy as part of its systems, a Fraud Analysis module that is capable of analyzing authentication related transactions to identify fraud.
- eKYC should be used as a facility using only biometric and OTP modalities by the AUAs Separate license keys must be generated by all AUAs for their SUB-AUAs from the UIDAI portal
- The Company must have the authentication servers routing to CIDR hosted in Data Centre within India. The Company shall adhere to all the notifications, guidelines and circulars published by UIDAI. Compliance team of the Company shall be responsible for the communication of the published information by UIDAI to all its personnel.

5 Mobile Application Security

5.1 Overview

Mobile apps are software applications tailored to operate on mobile devices or tablets. This portion of the Information Security policy oversees the overarching principles and procedures that aim to capitalize on the advantages of mobile technology while minimizing its associated risks. This is achieved by ensuring the organization’s compliance with pertinent industry standards.

5.2 Objective

The aim of this policy section is to create a standardized framework that guarantees the inherent security, resilience, and resistance to security threats, vulnerabilities, and attacks of mobile applications designed, developed, or built by or for the Company. It also ensures compliance with regulatory guidelines.

5.3 Policy Details

- The Company’s IT needs to create a framework that aligns Information Technology (IT) with evolving technology and security updates in the management of mobile applications.
- Roles and responsibilities of stakeholders need to be defined, along with the review and approval of changes in the Mobile Application life cycle.
- Integration of security controls and mechanisms for mobile applications is essential, including data encryption and prevention of common vulnerabilities such as SQL injection, cross-site scripting (XSS), command injection, improper certificate validation, incorrect default permissions, and insecure data storage.
- Secure authentication, session management, and access control should be integrated to protect data.
- A robust version/release management process must be maintained to ensure application security; any deviation in the version/release management process should be clearly documented and approved by the IT Head / CTO with a defined period of risk acceptance.
- A proper incident response plan should be developed in line with the “IT Incident Management” process to detect, report, and mitigate incidents.
- Detailed approved documentation defining architecture, flow diagram, user manual, etc., should be maintained.

- The application should not be installed on an older version of Android/IOS that has multiple unfixed vulnerabilities.
- The principle of least privilege should be employed, ensuring that only the minimum necessary privileges/permissions are assigned and promptly revoked once their intended purpose has been fulfilled.
- The distribution of devices through app stores, mobile device management (MDM) systems, or other methods should be defined.
- A process for user acceptance testing before the deployment of mobile apps should be defined, and feedback on app functionality should be collected.
- Due diligence should be ensured while evaluating third-party services or APIs by considering data security, privacy, scalability, and support.
- A Cryptographic set of procedures, techniques, and methods should be implemented to secure sensitive information from unauthorized access & data breaches.
- The change management process must be followed to record changes made on mobile applications.
- A security vulnerability assessment should be conducted, in line with the IT-VA & PT Management process, to record and mitigate risks whenever a new app is built, or a version is upgraded prior to production movement; running apps with known vulnerabilities is a significant risk and a violation of the “Information Security” policy.
- The app security score of a mobile app scan should be a minimum of 80%.

6 Security Operations Centre (SOC)

6.1 Overview

The Security Operations Centre is a centralized unit that oversees and controls an organization’s Information security stance. It involves the use of information technology systems, processes, and personnel to identify, respond to, and mitigate Cyber security threats. This center frequently employs tools such as SIEM (Security Information and Event Management) systems, threat intelligence, audit trails and cooperation among security experts to protect against a variety of Cyber security threats.

6.2 Objective

A **Security Operations Center (SOC)** is a crucial component in an organization’s cyber-security strategy. This portion of IS policy serves as a critical foundation & provides a framework / guideline for safeguarding an organization’s digital assets. It aims to quickly detect and respond to potential cyber threats, protect sensitive information, ensure regulatory compliance, and maintain resilient cyber security. This is achieved through continuous monitoring, proactive defense measures, and rapid incident response, all in line with the company’s objectives.

6.3 Policy details

- Comprehensive SOC Procedures: Develop procedures that integrate technology, processes, and people. This could involve defining roles and responsibilities, establishing communication protocols, and integrating security tools and technologies. The procedures should align with business objectives and enhance cyber security readiness.
- Confidentiality Protocols: To protect sensitive information, the Company’s IT should define protocols ensuring confidentiality. Access controls must be implemented for sensitive data handled by the SOC. Only authorized personnel should have access to sensitive data.
- Logs Handling and Retention: Establish measures for the proper handling, storage, and retention of IT security-related data and logs. This could involve secure storage solutions, encryption of data at rest

and in transit, and defined retention periods based on regulatory requirements and business needs.

- Incident Severity Levels: Define levels such as Low, Medium, High, and Critical based on factors like impact on business, data sensitivity, and user count. This helps prioritize incident response and escalation.
- Incident Analysis Procedures: Establish a systematic approach to investigate incidents, identify root causes, and implement corrective actions. This could involve steps like initial analysis, system log review, and impact assessment.
- Access Controls: Implement multi-factor authentication (MFA) for all SOC systems and tools. This adds an extra layer of security by requiring multiple forms of verification.
- Security Awareness Training: Regularly train SOC staff on recognizing and responding to threats like phishing and social engineering. This could involve simulated attacks to test their awareness.
- Continuous Monitoring: Deploy monitoring tools for real-time surveillance of networks, systems, and applications. This helps in early detection of anomalies and potential security threats.
- Periodic SOC Assessments: Regularly evaluate the SOC’s effectiveness in analyzing and responding to security events. This could involve metrics like incident response time and resolution rate.
- Regular Reporting: SOC teams should provide regular updates on security incidents, vulnerabilities, and trends to senior management and stakeholders. This helps keep everyone informed about the security posture.
- 24/7 Monitoring: Ensure that the SOC has the capability to detect and respond to security incidents round the clock. This is crucial as threats can occur at any time.
- Threat Intelligence: Provide SOC teams with access to up-to-date threat intelligence. This helps them identify and respond to security incidents more quickly.

7 Data Loss Protection Policy

7.1 Overview

Data is modern treasure and its incredibly important. Data Loss Prevention (DLP) is a security strategy that focuses on preventing the loss, leakage, or misuse of sensitive data. It involves a combination of people, processes, and technology. DLP is about protecting sensitive information from loss, corruption, misuse, or unauthorized access. It identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data.

With the rise of cyberattacks, data leaks, ransomware attacks, and insider threats, DLP efforts have become indispensable. It helps organizations monitor and protect sensitive information across on-premises systems, cloud-based locations, and endpoint devices. DLP can improve data visibility, secure data in remote/BYOD environments, protect intellectual property, promote brand reputation, prove regulatory compliance, and prevent cyber-attacks and data breaches.

Implementing a robust DLP strategy is crucial for any organization to safeguard its sensitive data and comply with various data privacy laws and regulations.

7.2 Objective

Company’s ‘Data Loss Prevention Policy’ is a declaration of the management’s commitment to provide a structured approach using rules, technologies, and procedures. This approach ensures that end-users do not transmit sensitive or confidential data outside the organization without appropriate authorization. It also aims to safeguard sensitive data in case of a data breach, facilitating effective management and helping the company achieve its objectives.

7.3 Policy details

- Develop a robust DLP framework: The Company's IT must create a strong DLP framework that includes technology and processes to meet business objectives and regulatory requirements.
- Implement a risk identification system: There should be a system that identifies and addresses high-risk areas for unauthorized release of protected information and misuse of data, applications, networks, and endpoints.
- Educate end-users: The IT Team must educate end-users about potential Cyber threats and data privacy to prevent data-related incidents and unauthorized document sharing.
- Technology control for sensitive data: The company with help of IT assistance needs to build technology controls to discover and maintain an inventory of sensitive data across the organization's systems and networks for information security compliance.
- Data classification: The company must ensure data is classified based on its confidentiality and criticality.
- Encryption methodology: The company needs to build a robust encryption methodology for sensitive data, both in transit and at rest, to protect against unauthorized access or interception.
- Endpoint security measures: The company must enforce endpoint security measures, such as USB port restrictions and device encryption, to prevent unauthorized transfer or storage of sensitive data.
- Secure data transfer methodology: The company must ensure a secure methodology for transferring sensitive data within and outside the organization by implementing encryption and secure file transfer protocols.
- Incident response plan: The company needs to develop a comprehensive incident response plan for data loss incidents, including steps to be taken in the event of a data breach, communication protocols, and legal obligations.
- Periodic assessments of DLP controls: There must be periodic assessments of DLP controls to address any vulnerabilities or gaps. DLP controls should be aligned to changing dynamics of business functions and Cyber threats.

8 New system induction System Go-Live

8.1 Overview

As business dynamics shift, IT systems undergo constant evolution to meet business demands and align with changing strategic goals. In today's digital landscape, this evolution is ongoing. However, any new addition of IT software or system represents a significant change to the existing IT configuration and its security posture. While these changes often bring enhanced functionalities or process improvements to the business environment, they also introduce new security risks or vulnerabilities to IT systems. Failing to address these promptly can result in serious problems down the line.

8.2 Objective

The goal of this policy section is to create a consistent framework that ensures secure, robust, and resilient applications developed by or for the Company. These applications must withstand security threats, vulnerabilities, and attacks while adhering to regulatory compliance guidelines.

8.3 Policy Details

- The Company's IT should create a framework where Information Technology (IT) aligns seamlessly with evolving technology. This alignment aims to maximize the value that technology brings to the business while minimizing associated risks and implementation costs.

- Ensure robust security controls and mechanisms for applications, like Integrate secure authentication, session management, and access control to safeguard sensitive data. Implement encryption practices to protect data from unauthorized access.
- Guard against common vulnerabilities such as SQL injection, cross-site scripting (XSS), command injection, improper certificate validation, incorrect default permissions, and insecure data storage.
- Establish a robust version/release management process to uphold application security.
- Any deviations within this process must be thoroughly documented and approved by the IT Head or Chief Technology Officer (CTO), with a defined period of risk acceptance.
- Develop an incident response plan in alignment with the "IT Incident Management" process. This plan should enable timely detection, reporting, and mitigation of incidents.
- Maintain comprehensive Standard Operating Procedures (SOPs) and documentation for application:
    a) Define the architecture.
    b) Create flow diagrams.
    c) Provide a user manual.
    d) Detail ID management procedures.
    e) Conduct business impact analysis.
- Establish a clear process for:
    a) User acceptance testing.
    b) Performance testing.
    c) Data migration readiness.
    d) Validation before deploying any new application.
- Ensure proper assessment while evaluating third party services or API's by considering data security, privacy, scalability and support.
- Change management process must be followed to record changes done as and when required on applications in line with IT-Change Management process.
- Conduct an application security vulnerability assessment in line with the IT VAPT Management process. This assessment is crucial whenever a new application is under development or when a major release is being moved into production. The goal is to identify and mitigate risks effectively.
- Obtain an "IT-Governance" sign-off by fulfilling the requirements in the IT Governance Checklist before going live.

9 Roles and responsibilities

Sr. No.	Roles	Responsibilities
1.	Information Security Committee (ISC)	• Periodic security updates on threat landscape and any major incidents across BFSI are discussed in these committees. These committees oversee the implementation of the Cyber Security Policy and provide guidance on cyber security initiatives. • Further details of this Committee are mentioned in Information Security Committee charter
2	Head of ISC **[Ref: Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 24 (b)]**	• Development of information/ cyber security policies, implementation of policies, standards and procedures to ensure that all identified risks are managed within the Company's risk appetite. • Approving and monitoring information security projects and security awareness initiatives. • Reviewing cyber incidents, information systems audit observations, monitoring and mitigation activities; and • Updating ITSC and CEO periodically on the activities of ISC.
3	Chief Information Security Officer (CISO)	• The Chief Information Security Officer (CISO) lead the implementation of cyber security controls. Teams under CISO to ensure all cyber security related controls are implemented at their levels and risks are identified, reported and corrective actions are taken.
4	Line Management	• Ensuring all direct reporters have completed the security training
5	Security Operations Centre (SOC)	• Monitor, analyze and escalate security incidents. • Conduct incident management and forensic analysis. • Coordination with stakeholder within the Company
6	Crisis Management Team (CMT)	• Oversee the response to cyber incidents. • Provide critical decisions during the response cycle. • Manage external communication.

10 Policy Compliance

The Information Security Officer in conjunction with the IT Operations Team will verify compliance to this policy through various methods, including but not limited to application tools reports, internal and externalaudits, and feedback to the Info-Sec group.

Information security of the Company's IT assets and resources is obligation of every employee, board members, external vendor resources, affiliated contractor, consultants or IT service providers. Any action by user having access to Company IT resources, which jeopardizes the Company's IT security is forbidden and shall attract appropriate action including legal proceedings.

In case where non-compliance is identified, ISC should review the reason for such non-compliance, disciplinary action should be consistent with the severity of the incident as determined by an investigation.

11 Policy Review and Approval

- This policy document should be reviewed at least annually by the Information Security Committee and approved by the Board annually or in the event of any significant changes (i.e., changes in operations, technology, regulations, or major security incidents) affecting the existing Cyber Security environment and its related procedures.
- Information and Cyber Security Policy should be updated in-line with any major changes within the Company’s operating environment or on recommendations provided by internal / external auditors and legal counsel.

12 References

- Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices - RBI/2023-24/107 DoS.CO.CSITEG/SEC.7/31.01.015/2023-24
- Information Technology Policy
- Cyber Crisis Management Plan
- Information Risk Management Policy
- Information Risk Management Procedure
- Information Risk Register