Information and Cyber Security Policy

Version 7.1 (Abridged)

May-2025

2. Objective

The goal of Information Security and Cyber Security Policy is to:

- provide management direction and support for information security in accordance with business strategies, and related legal, regulatory and contractual requirements. Also set the guiding principles for establishing Information Security strategies to achieve Confidentiality, Integrity, Availability of the Information and Information systems.
- contribute to continual improvement of the organization's Cyber Security & Cyber Resilience compliance posture
- understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers.

Information and cyber security are defined as the preservation of the following key security attributes:

- **Confidentiality**: Ensuring access to sensitive data to authorized users only.
- **Integrity**: Ensuring accuracy, completeness, and reliability of information by ensuring that there is no modification without authorization.

3. Information and Cyber Security Framework

3.1. Scope

- It is applicable to all employees (permanent/temporary/trainee), consultants, contractors, vendors and third parties termed as "Associates" and all relevant stakeholders.
- Applies to all information assets, and IT infrastructure including cloud environment used for the purpose of attaining business objectives. The IT infrastructure includes applications, databases, computer systems, communications networks and associated devices/technologies, etc.
- All processes and practices related to information & cyber security.
- Interfaces and activities (services) performed by vendors/third parties on behalf of or for the organization.

3.3 Policy Violation

- Breach of policy shall be immediately reported to CISO.
- Violations of any Information and cyber security policy, either by negligence or intentional, shall be subject to disciplinary actions as deemed fit by the management.

5. Organizational controls

5.19. Information Security in Supplier/Vendor Relationships

Third Party assessment and control requirements

- Formal Third-Party risk assessment process shall be in place and adhere to all the vendors before finalization of contract.
- Third party or vendor / partner dependencies to run the day-to-day operations should be assessed on a yearly basis and monitored via periodic reports on a quarterly basis.

5.22 Monitoring and Review of Supplier Services

- Organizations shall regularly monitor, review and audit supplier service delivery.
- Critical Vendors / Suppliers must be audited at-least once a year or in case of any major process change.

5.25. Assessment and decision on information security events

- Information security events/alerts should be detected through various security monitoring mechanisms.
- End users shall report any observed security events or weaknesses in information systems and services.
- Organization shall decide if incidents are to be classified as information and cyber security incident as per Information and Cyber Security Incident management procedure.

5.26. Response to Information Security Incidents

- Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information and cyber security incidents.
- Information and cyber security incidents shall be responded to in accordance with the documented procedures.
- Cyber Insurance shall be provisioned for liability associated with any cyber-attacks and fraudulent transactions that occurred due to security breach.

5.30. ICT readiness for business continuity

- The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g., during a crisis or disaster.
- The organization shall perform a business impact analysis to determine critical processes and assets to ensure business continuity during a crisis or disaster.

6. People Controls

6.2. Terms and Conditions of Employment

- Employee contracts or vendor agreements should state terms and conditions stating users and organization's responsibilities including confidentiality and non-disclosure regarding information and cyber security.
- Employee contracts and vendor/partner agreements shall be vetted by Legal team for any update in the approved format.

During Employment

- To ensure that employees and contractors are aware of and fulfill their information and cyber security responsibilities.

Management and User's Responsibilities

- User's reporting manager shall ensure that employees, contractors and third-party users under their management conform to security in accordance with the established policies and procedures.
- All users hold primary responsibility to comply with the security policy. When in doubt, users shall seek guidance and clarifications from their line manager or CISO for policy interpretations.

6.3. Security Awareness and Training

Security Awareness for Employees

- All associates shall receive appropriate initial and ongoing security awareness training by various means such as awareness mailers, security posters, phishing simulations, classroom and online trainings for relevant organizational policies, procedures, security best practices, emerging security threats.
- All associates shall undergo Information Security Training through online curriculum defined by the organization at least once a year.
- Security awareness training records shall be maintained and made available at the time of requirement.
- Disciplinary action shall be taken by HR for users who failed to complete security awareness related assignments.
- Effectiveness of training shall be measured through assessments.
- Detailed procedure for email phishing simulation activity shall be established.

Security Awareness for Top Management and Board

- Appropriate security awareness shall be conducted for top management and board to have a fair degree of awareness of the fine nuisance of the threats.

Security Awareness for Customers

- Organization shall promote security awareness among their customers.
- Organization shall send periodic security awareness emailers for their customers

6.4. Disciplinary Process

- A formal disciplinary process should be defined for employees, contractors and third-party users who have committed a security breach and violations of any Information and cyber security policy.
- Disciplinary action shall be taken by HR as per their defined process.

8. Technological controls

8.8. Management of Technical Vulnerabilities

- Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, The organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk as per technical vulnerability management procedure.
- Vulnerability assessment (VAPT) shall be carried out periodically for Information systems in use and prior to any new or major change put into production to identify vulnerabilities. Identified vulnerabilities shall be mitigated and revalidated before production goes live.

8.30. Outsourced Process

- Criteria for selecting an outsourcing vendor shall be considering the:

  v) Security management standards currently followed by the company (e.g., certified with ISO/IEC 27001, SOC-I and SOC-II, STQC).

******End of the Document******