KALPATARU PROJECTS INTERNATIONAL LIMITED
(Formerly Kalpataru Power Transmission Limited)

Cybersecurity Policy

Document reference	**KPIL/Cybersecurity/Policy/01**
Document Version	**01**
Proposed by	**Chief Digital & Information Officer**
Approver	**Managing Director and CEO**
Date approved	**1st December 2024**

Contents

1. INTRODUCTION

As a leading company at the forefront of innovation, Kalpataru Projects International Limited (hereinafter referred to as “KPIL” / “Organization” or “we” or “our”) recognize the critical importance of cybersecurity in safeguarding our operations, intellectual property, and most importantly, the trust of our clients and partners. Our commitment to cybersecurity extends beyond mere compliance; it is ingrained in our corporate culture and embraced at every level of the organization. We understand that cybersecurity is not just an IT issue but a fundamental aspect of our business strategy and ethos. As we navigate the complexities of the digital age, we are committed towards cybersecurity excellence, safeguarding not only our company's future but also the collective interests of our clients, partners, and stakeholders.

2. OBJECTIVE

The objective of this Policy is to establish and standardize IT security policies and practices across the KPIL’s business units (BUs) and locations to ensure the protection of integrity, confidentiality and availability of all IT assets and the information generated across all facets of KPIL’s operations. This Cybersecurity Policy serves as a comprehensive framework designed to mitigate risks, protect sensitive data, and ensure the resilience of our digital infrastructure. It underscores our unwavering commitment to upholding the highest standards of security across all facets of our operations.

3. DEFINITIONS

i. **Cybersecurity**: The practice of protecting systems, networks, and data from digital attacks and unauthorized access.

ii. **IT Assets**: Any hardware, software, or digital resources owned or managed by KPIL, including computers, servers, applications, and databases.

iii. **Information Assets**: Data and information generated, stored, processed, or transmitted by KPIL, including proprietary information, client data, and sensitive business data.

iv. **Sensitive Information**: Any information that, if disclosed, altered, or accessed without authorization, could result in harm to KPIL's reputation, financial loss, or legal liabilities. This includes personally identifiable information (PII), financial data, and trade secrets.

v. **Access Control**: Policies and procedures governing the granting, modification, and revocation of access to IT systems, applications, and data, ensuring that only authorized users can access sensitive information.

vi. **Asset Management**: The process of inventorying, tracking, and managing IT assets throughout their lifecycle, including procurement, deployment, maintenance, and disposal.

vii. **Change Management**: A structured process for evaluating, approving, and implementing changes to IT systems, applications, and configurations, minimizing disruptions and vulnerabilities.

viii. **Network Security**: Measures and protocols designed to protect the integrity, confidentiality, and availability of network infrastructure and communication channels, including firewalls, intrusion detection systems, and encryption.

ix. **Data Protection**: Policies, procedures, and technologies implemented to safeguard the confidentiality, integrity, and availability of data, including encryption, access controls, and data backup and recovery.

x. **Third-Party Security**: Requirements and controls governing the security of third-party vendors, partners, and service providers who have access to KPIL's IT assets or sensitive information.

4. SCOPE

This Policy applies to KPIL and extends to:

- All employees who have access to KPIL's information assets
- Other parties including but not limited to joint ventures, contractors, consultants, partners and third-party users (in-house or external) who directly or indirectly access information assets of KPIL.
- All business operations and processes of KPIL.
- All information assets and communication resources accessible irrespective of sites and locations.
- It is mandatory for all roles listed above, and any other person to whom this Policy applies, to adhere to this Policy while supporting the organizations' business from any other location in any country.

5. POLICY PROVISIONS

This Cybersecurity Policy outlines specific measures and guidelines established to safeguard KPIL's digital assets and infrastructure. These provisions serve as a comprehensive framework to mitigate cyber threats, protect sensitive information, and ensure the integrity, confidentiality, and availability of our data and systems. By adhering to these provisions, we demonstrate our commitment to proactive risk management, regulatory compliance, and the continuous enhancement of our cybersecurity posture:

i. **Operational Security**: KPIL recognizes the critical importance of operational security in safeguarding sensitive information, infrastructure, and operations against cyber threats. To ensure the highest level of operational security, the company shall implement the following measures:

- **Access Control**: KPIL has implemented robust access control mechanisms to restrict unauthorized access to sensitive systems, data, and facilities. This includes the use of strong authentication methods, regular access reviews, and least privilege principles.
- **Asset Management Security Policy**: KPIL has a Policy in place listing down protocols regarding inventory of IT assets, ownership of assets and acceptable use of assets. This Policy also covers handling, return, theft/loss, damage and disposal of IT assets.
- **Change Management**: KPIL has established a structured Change Management process to systematically assess, authorize, and implement changes to the company's information systems, infrastructure, and configurations. This process ensures that changes are thoroughly evaluated for potential security implications, approved by appropriate stakeholders, and implemented in a controlled manner to minimize disruptions and vulnerabilities.
- **Network and Communication Security**: KPIL prioritizes the implementation of robust security measures across various facets of network and communication infrastructure. We have key strategies and protocols in place aimed at fortifying our network against cyber threats and vulnerabilities, encompassing areas such as network management, perimeter security, email security, video conferencing security, and wireless network security.

ii. **Data Protection and Privacy**: KPIL has a Data Privacy and Protection Policy in place to protect and promote data protection and privacy right of individuals and of the business, by informing working for the organization, of their data protection obligations and of the procedures that must be followed in order to ensure compliance. This Policy lays down measures to ensure confidentiality, availability and integrity of data. This Policy also lays down necessary controls for protection of data in all stages of data lifecycle.

iii. **Legal and Regulatory Compliance**: KPIL shall identify and document all applicable legal, statutory, regulatory and contractual requirements

pertaining to information security. The organization shall ensure adherence to third party licensing agreements, intellectual property rights, and identify requirements (legal, regulatory and contractual) with respect to protection of Personally Identifiable Information (PII). KPIL shall define an internal audit plan for performing information security audits on its information systems to review the compliance status of policies, procedures, applicable standards and regulations.

iv. **Third party security**: KPIL shall assess all its third parties with respect to information security based on associated criticality and risk profiling. The third-party contract shall define the information security requirements to be adhered by the service provider. Information sharing and retention arrangements with third parties shall be done as per KPIL's Lifecycle Management and Protection Policy.

v. **IT procurement and vendor management**: KPIL has an IT procurement and vendor management system and Policy in place to standardize procurement of IT products and services across all BUs and the KPIL IT. This provision minimizes potential business risk by allowing procurement of only standard IT products and ensures reliability and transparency of the overall IT procurement by establishing objective vendor selection practices. The Information Security Risk (ISG) shall be consulted for all information and cybersecurity risks by the procurement team.

6. INFORMATION SECURITY RISK MANAGEMENT

Cybersecurity practices at KPIL are being implemented under the guidance of the Risk Management Committee. These practices are KPIL are categorized into people, process and technology control areas under the company-wide Cyber Security Assurance Framework. Under this framework, KPIL performs risk assessment annually for all BU IT assets, IT infrastructure, Business IT applications, IT systems networks that supports business processes, and third-party vendors and partners.

The Company also actively monitors security logs to detect any malicious attempts and takes the necessary measures to mitigate the risk. Adequate data safety is ensured during its creation, storage, transit and retrieval. The results from the Cybersecurity risk assessment conducted across the organization, as well as the risk mitigation plans prepared thereafter are communicated to the business and executive management. KPIL also has a robust Business Continuity and Disaster Recovery Management Plan (IT DR plan) in place to ensure continuity of critical business processes, enable efficient recovery and minimize data loss during disruptions. IT DR plan considers:

- IT services supporting critical businesses to be recovered.
- Time span in which they are recovered.
- Expediencies requiring triggering of IT DR plan.
- Recovery levels for each critical IT service.

7. POLICY IMPLEMENTATION AND CYBERSECURITY GOVERNANCE:

In the realm of cybersecurity, accountability is paramount. At KPIL, we understand that safeguarding our digital assets requires more than just policies and protocols; it demands clear roles, responsibilities, and accountability mechanisms. To this end, we have adopted a robust framework for implementation: the RASCI matrix. The RASCI matrix serves as a cornerstone of our cybersecurity strategy, providing clarity and structure to the complex task of Policy implementation. The RASCI matrix highlights the roles and responsibilities of IT Security Head at KPIL, IT Security Manager, IT Head, IT Services Manager, IT Network Manager, Business owner/End user at every stage of the cybersecurity lifecycle across BUs for ensuring smooth implementation of this Cybersecurity Policy.

This Cybersecurity Policy and the various internal policies mentioned in this document are established in accordance with ISO 27001:2013.

8. TRAINING

KPIL has developed a strong culture of Cybersecurity awareness and training within the company. All stakeholders having access to information assets of the organization are made aware of Cybersecurity Policies (This Policy as well as internally available other Cybersecurity Policies) and procedures relevant to their business function through various channels like awareness programs, trainings, and other initiatives. Employee awareness on cybersecurity is enhanced through initiatives such as online cyber security awareness campaign on phishing and e-mail securities. All employees undergo cybersecurity trainings annually, and new joiners are required to complete their cybersecurity trainings within 45 days of their induction. Cybersecurity training compliance is ensured by IT Security Manager across BUs.

9. INFORMATION SECURITY INCIDENT MANAGEMENT

KPIL has incorporated a formal process of Information security incident management which lays down relevant roles and responsibilities associated with incident management. The process lays down the protocols for Incident identification and reporting, Incident response and resolution, Incident escalation and closure. Furthermore, there is a dedicated Information Security Incident Response Team (ISIRT) at KPIL to address Information Security incidents in an appropriate and timely manner.

10. NON-COMPLIANCE

Any Employee found to have violated this Policy will be subjected to disciplinary action. The consequences of non-compliance may result in revocation of access to KPIL's IT assets, denial of future employment references, termination of employment and appropriate legal actions.

Other parties (including but not limited to joint ventures, contractors, consultants and third parties (in-house and external) who directly or indirectly provide operations

management to KPIL, if found to have violated this Policy, then the organization reserves the right to terminate the contract with party, blacklist the party for any future business.

The nature of violation shall be assessed to determine the impact to organization, and adequate level of action shall be taken, as deemed appropriate by IT security head in consultation with the HR.

11. POLICY REVIEW AND UPDATE

This Policy shall be reviewed on an annual basis and / or if required by IT Security Head (BU)/IT Security Manager (BU) and approved by the IT Head (KPIL).

This Policy has been reviewed and approved by the Managing Director & CEO of Kalpataru Projects International Limited.

Mahish Mohnot

Managing Director and CEO