Information Protection & Cybersecurity Policy

Introduction:

Today's digital environment presents a continuously evolving threat to Information Protection & Cybersecurity. Techno Electric & Engineering Co. Ltd. (TEECL) recognizes that data is a critical business asset. At TEECL, we take a "defense-in-depth" approach to protect our data, our customer data, our infrastructure, our information assets and our employees. Information security means protecting our data, applications, networks, and computer systems from unauthorized access, alteration, or destruction. The security of TEECL's information, and that is trusted by our customers, partners, suppliers and contractors who may hold information on our behalf, is fundamental to protecting, maintaining and operating our business. The loss, corruption, or theft of information and supporting systems could have a serious impact on the Group's business activities and reputation. Our people, information and processing systems are critical to our business and need to be protected appropriately. We embed data protection throughout our business operations and information technology programs, relying on multiple and various controls to prevent and detect threats, with the goal of providing a disciplined approach to safeguarding our information assets, customer data and employees. As a foundation to this approach, TEECL maintains a comprehensive set of Information Protection & Cybersecurity policies and standards. These policies and standards are developed in collaboration with a wide range of disciplines, such as information technology, cybersecurity, legal, compliance and business. This policy incorporates practices that are compliant with regulatory and other external requirements relevant to IT.

1. **Commitment:**

TEECL is committed to protecting confidentiality, integrity, and availability of its information through various security measures. These measures include policies, intrusion prevention systems, employee training, and periodic IT audits. We are committed to combating the threat of cyber-attacks and to securing our business through our information security programs by developing a deep understanding of cybersecurity risks, vulnerabilities, mitigations, and threats.

TEECL follows a robust Information Security framework to safeguard its IT infrastructure, data, and business applications from potential threats. We implemented industry-standard security policies and protocols to ensure a secure IT environment while maintaining business continuity.

TEECL implemented a comprehensive Cybersecurity strategy that integrates strong password policies, access management, network security, IT audits, and an effective IT Service Management (ITSM) system. Continuous improvements, regular upgrades, and adherence to industry best practices ensure a secure and resilient IT environment.

2. Scope:

This policy is applicable to all TEECL individuals (employees, directors, management, contractors, consultants and third parties) that are granted access to any technological information using the information systems deployed by TEECL. This security policy applies to all IT assets, information systems, and business processes supported by IT across TEECL. The policies are applicable for all offices & locations along with all business lines and affiliates of TEECL.

3. Purpose:

TEECL's Information Protection & Cybersecurity Policy establishes the rules and expectations regarding user's privacy. This policy must be followed to ensure the IT environment is operating in a manner that satisfies applicable privacy compliance requirements. The purpose of the policy is to:

- Inform employees about the importance of securing company information and resources.
- Establish a company-wide approach to information security.
- Prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of company data, applications, networks, and computer systems.
- Define mechanisms that protect Company's reputation and allow the Company to satisfy its legal and regulatory responsibilities.

4. Governance and Oversight:

Our Information Protection & Cybersecurity strategy and policies are continually reassessed to ensure to identify and proactively address the constant changes in the global threatscape. Decision makers are regularly kept up to date on Information Security trends, and ongoing collaboration with stakeholders throughout the business help ensure continued awareness and visibility of future needs. These processes are managed diligently by our IT team headed by TEECL's Vice President of Digital Infrastructure and Innovation with support from our business continuity teams. Our processes are regularly evaluated by IT security experts, with the results of those reviews reported to senior management and, where appropriate, reported to the Board.

5. Awareness & Training:

Employees play a critical role and are typically our first defense against Information Protection & Cybersecurity concerns. For this reason, we provide online cybersecurity awareness sessions and INFOSEC training to employees to enhance their data security knowledge. These measures include regular awareness campaigns on phishing, email security, cybersecurity awareness training and data protection training. Employees are informed of the importance of Information Security and potential threats through policies, procedures, and periodic communications.

6. Certification & Compliance:

We are actively pursuing ISO 27001 certification for Information Security Management Systems (ISMS) to further strengthen our internal Information Security framework. TEECL is committed to complying with best practices in data governance and privacy.

7. Audits:

We conduct regular internal and external INFOSEC audits and risk assessments to identify and mitigate gaps in our IT infrastructure. Audit findings are reviewed and addressed in a timely manner and used to refine security policies and controls, technology implementations, staff training, and escalation procedures.

8. Technology:

TEECL utilizes sophisticated technologies and tools to protect its IT environment from global threats, including:

- Strong password management and multifactor authentication (MFA)
- Single sign-on (SSO)
- VPN access for external connectivity, firewalls and network security, antivirus & endpoint protection
- ITSM portal, automated ticketing, and escalation
- Secure cloud storage, including data protection & back-up
- Email security, centralized authentication, internal applications on the intranet
- Access controls for server rooms and office premises and logical access management
- Strong encryption policies on its data, utilizing both encryption in transit and at rest
- Adequate data safety measures are ensured during data creation, storage, transit, and retrieval.

Our network devices, server operating systems, and hardware are regularly upgraded. TEECL has a robust and aggressive patch management process designed to reduce software-based vulnerabilities quickly and effectively.

Avaneesh Kumar Vats
(Chief Information Officer)

Policy	Version	Adopted	Revised
Information Protection & Cybersecurity Policy	v 1.0	05 April 2025	NA