Keppel Cyber Security Policy

Keppel is dedicated to adopting a comprehensive approach to managing cybersecurity risks and building robust cyber resilience.

We are committed to maintaining trust, ensuring regulatory compliance, and safeguarding against cyber threats to prevent data breaches and other cyber incidents, thereby securing the integrity and continuity of Keppel's operations.

Governance

The Head of Cyber Security oversees the Cyber Security Centre and Cyber Governance, driving the enterprise vision, strategy, and program to ensure Keppel's technology assets are adequately protected from cyber threats.

Business Information Security Officers are appointed as cybersecurity business partners to work closely with respective platforms and divisions, strengthening cyber risk management and building cyber resiliency.

Keppel maintains a range of detailed cyber policies internally that are aligned with industry standards and local regulatory requirements for effective cybersecurity risk management and executes assurance and compliance programs to ensure processes and controls are effective and adhered to. Our cyber practices are reviewed regularly to keep abreast with evolving threats and to incorporate advancements in cybersecurity technology to protect and safeguard Keppel’s data from unauthorised access, disclosure, alteration and misuse, as well as loss and destruction.

The Keppel Supplier Code of Conduct and Third-party Technology Vendor Management policies are also in place to manage risks and ensure that these relationships do not compromise Keppel's security, compliance, or operational integrity.

Cyber Threat Management and Response

Keppel is committed to staying ahead of cyber threats and continuously strengthening our cybersecurity defenses through:

- Continual improvement in cybersecurity systems;
- Maintaining information security controls to ensure the integrity and protection of data;
- Monitoring and responding promptly to any cybersecurity threats;
- Ensuring employee responsibilities in safeguarding cybersecurity, including training and awareness initiatives to empower employees to understand and adhere to security protocols and practices; and
- Establishing cybersecurity requirements for third parties to ensure their compliance with Keppel’s cybersecurity policies and practices.

Cyber Safety Culture

Keppel is also committed to continuously nurturing a cyber safety culture.

Regular advisories and training sessions on the latest cybersecurity threats, policies, and best practices are held to inculcate a cyber-safe mindset.

Our Cyber Incident Response plan provides guidance on the escalation process for employees to report incidents, vulnerabilities or suspicious activities, as well as dealing with potential crisis events or major incidents that impact important business processes.