SECURITY POLICY

Kinetic IT's reputation and social licence to operate is founded on the trust and respect we build with our stakeholders. Fundamental to maintaining this position is our ability to protect the technologies, physical environment and information assets of our company, and those which have been granted to us by our employees and contractors (crew), customers and other stakeholders.

We are committed to employing contemporary, integrated security practices which ensure the confidentiality, integrity and availability of information entrusted to us, and as applicable to our business and services, addressing challenges of evolving technology and physical landscapes. We will continue to foster a security aware culture, ensuring our crew and partners possess the essential competencies to maintain a secure business environment.

ROLES AND RESPONSIBILITIES

The Company, its Managers and Leaders will support our crew to achieve this by:

- Prioritising information and physical security considerations in the delivery of our services, management of our staff and partners, and fulfilment of company responsibilities.
- Working with our customers to assess, adapt and apply their security controls.
- Identifying and implementing contractual, legal and regulatory-compliant security controls to protect Personal Information and other sensitive data.
- Defining expectations in relation to the acceptable use of company and customer assets and systems.
- Undertaking risk and threat assessments to manage and treat security-related risks.
- Providing clearly defined roles and responsibilities and documented procedural controls.
- Ensuring our staff entrusted to manage information assets possess the essential competencies to maintain a secure information and physical environment.
- Fostering a security-aware culture through effective communications and awareness training.
- Establishing relevant and measurable objectives to assess and continually improve our privacy and security capability and practices.

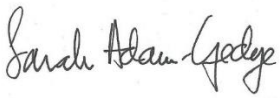
We expect our crew and partners to take a proactive approach to protecting information assets by:

- Understanding, respecting and complying with security guidelines and standards issued by the company and as required by our customers and other stakeholders.
- Appropriately protecting confidential and other sensitive data.
- Using Kinetic IT and customer assets and systems in a responsible way and in accordance with defined guidelines.
- Adhering to procedures and controls to protect private, sensitive and confidential information and information assets from unauthorised access or inadvertent distribution.
- Reporting any potential security-related risks, threats, vulnerabilities or incidents including suspected or actual breaches.
- Strengthening Kinetic IT's security-aware culture by actively participating in security practice improvements, knowledge-sharing, training and other supporting activities.

OBJECTIVES:

Our Security Policy is the foundation of our Management system and underpins Kinetic IT's commitment to ensuring the confidentiality, integrity and availability of information entrusted to us.

- Identify & effectively manage security risks.
- Provide appropriate resources to manage information assets entrusted to us.
- Continually improve our security posture through proactive evaluation of our practices & performance.



Michael North
Chief Executive Officer

Sarah Adam-Gedge
Chairperson