Information Security Policy

Information security is the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, information integrity and protection of information in all formats.

TIMG, entrusted by clients with their information and records management, identifies the importance and implements appropriate measures. Information security is achieved by implementing a suitable set of controls (based on risk profile), including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that specific security objectives are met.

This policy applies to all information that is physically or electronically generated, received, stored, printed, filmed, or keyed; and to the IT applications and systems that create, use, manage and store information and data. The policy covers the following areas:

- Access Control
- Telecommunication and Operations Security Management
- Human Resource Security
- Communication and Operation Management
- Physical and Environmental Security
- System Acquisition, Development and Maintenance
- Supplier Relation
- Information Security Incident Management
- Information Security aspects of Business Continuity Management
- Compliance Management
- Information Security Risk Management
- Asset Security Management and Control

TIMG is committed to continuous improvement of information security systems.

- All users (employees, contractors and 3rd party suppliers) are responsible for following the security controls to contribute towards managing TIMG securely.
- All users should adopt a risk-based, and risk averse approach to Information Security.
- All users are to protect sensitive and confidential data and information in order to prevent unauthorised disclosure.
- All users must comply with relevant legal and regulatory requirements.

Information Security Policy

The policy is directly aligned with the Information Security Industry standard AS/NZS ISO/IEC 27001:2022 (E) and PCI-DSS Physical Storage v.4.0.

PCI DSS is a comprehensive set of requirements created by the Payment Card Industry Security Standards Council to enhance cardholder data security and to ensure the safe handling and storage of sensitive customer credit card information and data. Maintaining security of cardholder data is very important and at TIMG all physical information are treated as such. TIMG PCI DSS responsibilities as a Secure Physical Storage Provider are outlined in the Attestation of Compliance (AOC) as independently audited by Qualified Security Assessor (QSA) each year.

All aspects of the PCI DSS physical storage security are managed by ISMS Steering Committee at TIMG.

Jason Carr
General Manager
Reviewed 01 June 2024
Issued 25 July, 2019