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 and University 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
- Digital Messaging
- 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

TIMG is committed to continuous improvement of information security systems.

The policy is directly aligned with the Information Security Industry standard AS/NZS ISO/IEC 27001:2013(E) and PCI-DSS Physical Storage v.3.2 April 2016.

Chris Cotterrell
General Manager
11th of August, 2017

Version 2.0