GEYER

Information Security Policy

Geyer is an award-winning, strategic design practice specialising in the development of workplace, retail, hospitality, and education interior environments across the Asia Pacific. With a portfolio of global and regional clients and an impressive track record, Geyer has a reputation for strategy-led design solutions which enrich our clients' performance, brand, and culture.

Information security is the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximise return on investments and operational opportunities.

Data, information and the underlying technology systems are essential assets to Geyer and provide vital resources to staff and stakeholders and consequently need to be suitably protected.

Geyer is committed to providing a secure, yet open information environment that protects the integrity and confidentiality of information without compromising access and availability. This policy applies to all information that is electronically generated, received, stored, printed, filmed, or keyed; and to the IT applications and systems that create, use, manage and store information and data.

Our information security policy aims to:

- Limit access to information and information processing facilities in support of business requirements.
- Establish and maintain the protocol for using information in all its forms, including the security aspects of information transfer within Geyer and with any external entities.
- Ensure the protection of information and the secure operations of networks and supporting processing facilities.
- Prevent unauthorised physical access, damage and interference to Geyer's information and information processing facilities.
- Ensure that information security is an integral part of information systems across the entire lifecycle. This includes information systems that provide services over external networks.
- Ensure protection of Geyer's information assets that are accessible by Service Providers.
- Ensure a consistent and effective approach to the management of information security incidents, including security events and vulnerabilities.
- Ensure information security continuity is embedded in business continuity plans and management processes.
- Avoid breaches of legal, statutory, regulatory or contractual obligations related to information security.

The provisions of this policy apply to all Geyer staff (including temporary agents and staff engaged under contract) and Service Providers. This policy includes, but is not limited to:

- Geyer information in any form, including print, electronic, audio, video, and backup and archived data. This includes, computer systems, peripheral devices, software applications, databases, middleware and operating systems;
- Physical premises occupied by the personnel and equipment;
- Operational environments including power supply and related equipment;
- Processes and Procedures; and
- Transmission of Communications and related pathways.

This Information Security Policy defines the principles for establishing effective security measures to ensure the Confidentiality Integrity, Availability and Privacy of Geyer information. The Policy also covers the continued availability of information and the information environment to support Geyer business activities, including the implementation of appropriate controls to protect information from intentional or accidental disclosure, manipulation, modification, removal or copying. This is achieved by:

GEYER

Information Security Policy

- Defining roles and responsibilities and establishing clear lines of accountability;
- Protecting Geyer's information assets against internal and external threats (e.g. security breach, loss of data);
- Ensuring that Geyer complies with applicable laws, regulations, and standards;
- Identifying and treating security risks to Geyer's information environment through appropriate physical, technical and administrative channels; and
- Developing best practices for effective Information Security across Geyer.

User Responsibilities

- Users must abide by all relevant laws and all Geyer policies.
- Users are expected to take responsibility for developing an adequate level of information security awareness, education, and training to ensure appropriate use of the information environment.
- Users may only access information needed to perform their authorised duties.
- Users are expected to determine and understand the sensitivity of the information to which access has been granted through training, other resources or by consultation with the relevant supervisor.
- Users must protect the confidentiality, integrity and availability of Geyer's information as appropriate for the information sensitivity level.
- Users may not in any way divulge, copy, release, sell, loan, alter or destroy any information, except as authorised by the Director.
- Users must safeguard any physical key, ID card or computer/network account that enables access Geyer information. This includes maintaining appropriate password creation and protection measures as set by the organisation from time to time.
- Any activities considered likely to compromise sensitive information must be reported to the Director.
- Users are obliged to protect sensitive information even after separation from Geyer.

Managers and Supervisors Responsibilities

In addition to complying with the requirements listed above for all staff and contractors, managers and supervisors must:

- Ensure that departmental procedures support the objectives of confidentiality, integrity and availability and that those procedures are followed.
- Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
- Ensure that each staff member understands his or her information security related responsibilities.
- Ensuring adequate security for computing and network environments that capture, store, process and/or transmit Geyer information.

This policy is communicated to all personnel working for and on behalf of Geyer and is available to the interested parties as required.

Marcel Zalloua, Director