Information Cybersecurity Policy

10000-ITX-POL-002

Revision B

Policy Statement

The Principals OGP Group (OGP) has adopted and is committed to reasonably ensuring the confidentiality, integrity and availability of the data generated by us and entrusted to us, including personnel data, and customer data, based on good risk management practices, legal regulatory and contractual obligations, and business requirements, all of those underpinned by fostering a strong information security culture.

Roles and responsibilities

Information security is everyone's responsibility through the understanding and adherence to this policy and the requirements of our Information Security Management plan.

Data and Information

Accepting the basic differences between the terms 'data' and 'information' both terms are used interchangeably in this policy.

Network (server) security

OGP has chosen Microsoft (MS) SharePoint as its system platform, benefiting from its robust data management and cyber security functionality, including incident recovery.

We use Bit Defender, MS Defender and proven RMM products for cyber risk management with automatic device alert monitoring, full remote access to wipe out device data, automatic security patch management and ransomware scanning and detection.

Network access control

OGP shall not allow third parties to access its server and systems. We shall establish a new library within an independent server should we require to exchange large amounts of data with third parties and will scan and verify received documentation before it is accessed.

Employees cannot access the server from mobile devices or any other private device without being enrolled in the Company Portal Application and covered by its security measures. Multi-factor authentication shall be enabled for all OGP users.

Users have a unique OGP ID number, they shall be monitored for a limited number of password attempts and locked out if exceeded in addition to unusual behavior monitoring. All such events shall be logged and the log kept for 12 months.

Data access control

We shall grant access to data on the principle of least privilege, complying with contractual terms and regulatory requirements. Users are only provided access to the information they require to perform their role and tasks.

Data protection and retention

Based on its type and classification, data shall be stored in segregated areas of the corporate server or in independent servers requiring multi-factor authentication to access.

Data being this digital or supported in hardware media shall be retained and disposed safely in accordance with current privacy principles, laws and contractual obligations.

Office access is by secure door activation with personalized FOB. After-hours access is restricted, and we keep physical confidential information in a lockable room.

Risk Management

OGP shall apply sound risk management principles to protect information security, its data confidentiality, integrity and availability and shall implement appropriate mitigating measures throughout the organisation.

Monitoring

Compliance with this policy and associated procedures shall be monitored via periodic audits.

Training and awareness

This policy shall be made publicly available and supported by training with strong internal focus on the awareness of the criticality of information security.

Incident response and recovery

Devices shall be automatically locked out from the network should they be identified as non-compliant, including external storage devices should they include potential threats. Such an event shall trigger our security response procedure.

All network drives shall be backed up multiple times a day and stored for 12 months.

Security incident communication and disclosure

It is everyone's responsibility to communicate security events and near misses to their immediate supervisor. OGP shall immediately inform customers of any cyber safety incident.

OGP is committed to managing a coordinated response to minimize potential exposure and impact to us and customers.

The OGP incident communication procedure spans from the initial communication to customers to a post-incident review and lessons learnt effort.

Continuous improvement

OGP shall ensure that the information security management plan is regularly reviewed and improved as part of OGP's continual improvement process.

Janik Soysa.
Directors
OGP Group Pty Ltd
November 2024

Gary Dagres.

OGP Group is a provider of a wide range of services, technologies and products to the infrastructure and engineering industries. Our activities include design, supply, procurement, installation and commissioning.