Document Title: Information Security Policy Statement
Document Reference: ITG-ISE-006
Issue Date: 04/11/2022
Revision: 23.0
Document Classification: Unrestricted

INFORMATION SECURITY POLICY STATEMENT

The Company Information Security Management System (ISMS) is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

The Company is a telecommunications systems integrator specialising in multi-vendor networking service solutions. Due to the nature of the business the Company is required to handle sensitive information for our customers. We have a responsibility to both our employees and our customers to ensure that information supplied to us is treated with respect.

The Company is committed to operating an effective Information Security Management System which protects data from disclosure or corruption while allowing its appropriate use. To achieve this, the Company applies ISO 27001 in the operation of its Information Security Management System. The principles of the Information Security Management System are:

- To fully assess the risks associated with handling information
- To eliminate risks to the loss or corruption of information
- To implement pragmatic controls to minimise risks of information corruption or loss
- To handle information in ways which ensure legal compliance with appropriate legislation
- To operate an integrated Information Security Management System which functions within the company's current ISO 9001 management system
- To maintain and continuously improve the Information Security System

Definition of information security

Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Responsibilities

The Information Security Management System is co-ordinated by Nikke Walker who carries out the role of Group Security Officer.

Technical advice is provided by the IT and Systems Department. Advice on specific issues may be given by in house specialists if appropriate.

All employees have a responsibility to report information security incidents.

Monitoring, Review, and Auditing

ISO 27001 Committee meetings (ISMS) are held every month to review the Information Security Management System. Ad-hoc meetings are held as and when required to set objectives, principles for action and progress Information Security Management System issues as they arise. Updates on Information Security are also included as part of the Senior Management team monthly meetings and information is provided on the Monthly board report. Internal audits of the ISMS processes and procedures are completed biannually.

Risk Assessment

The information security risk assessment process establishes criteria against which risk will be evaluated and is recorded in the document "Information Security Management System Risk Assessment" (ITG-ISE-011), which is held on the Business Management System (BMS). This is a

ENGINEERING A DIGITAL FUTURE

semi-quantitative risk assessment based on a fault mode event analysis. The methodology is contained within the Risk Assessment document.

Legal Requirements

The Company has contractual and legislative responsibilities to ensure the security of information it possesses is maintained. The operation of the Information Security Management System is designed to ensure best practice is adhered to, ensuring both customer and legislative requirements are met.

Signed:

Ian. Dugg –

Ian Duggan
Group CEO