Information Security Policy Statement

Objective

The objective of information security is to ensure the business continuity of Interr and to minimise the risk of damage by preventing security incidents and reducing their potential impacts.

This Statement should be read in conjunction with the rest of the Company policies related to ISO27001 – International Standard for Information Security.

Policy

The policy's goal is to protect the Company's informational assets against all internal, external, deliberate or accidental threats. The company operates a system that regularly evaluates its processes and customer requirements and has set quantifiable objectives with plans in place to ensure that they are reviewed year on year for improvement.

Information can exist in various forms, and includes data stored on computers, transmitted over networks, printed or written on paper, sent by fax, stored hard drives, in cloud-based systems or discussed during telephone conversations.

The security policy ensures that:

- Information will be protected against and unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Availability of information for the business processes will be maintained
- Legislative and regulatory requirements will be met
- Business continuity plans will be developed, maintained and tested
- Information security training will be available for all employees
- All actual or suspected information security breaches will be reported to the HR and Compliance Director (Data Protection Officer), through line management and HR, and will be thoroughly investigated

Procedures exist to support the policy, including virus control measures, passwords and continuity plans.

Business requirements for availability of information and systems will be met. The information security manager is responsible for maintaining the policy and providing support and advice and ensuring compliance.

The management of the company is firmly committed to the systems, procedures and controls; compliance with the information security policy is mandatory.

It is the intention of the Directors that this policy along with all other policies will be reviewed on an annual basis at the management review meeting.

Statement Review and Assessment

This statement may be amended by Interr at any time to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024