INTEGRITY PRINT

INFORMATION SECURITY POLICY

This information Security Management System (ISMS) policy outlines the commitment of Integrity Print Ltd, Midsomer Norton towards protecting its information assets and ensuring the confidentiality, integrity, and availability of information in compliance with ISO 27001:2022 standards.

Scope

This policy applies to all employees, contractors, and third parties who have access to the organisation's information assets.

Information Security Objectives

- Ensure the protection of sensitive information from unauthorised access, disclosure, alteration or destruction.
- Comply with relevant laws, regulations, and contractual requirements related to information security.
- Continuously improve the effectiveness of the ISMS to address emerging threats and vulnerabilities.

Information Security Responsibilities

Senior management is dedicated to supporting and overseeing the Information Security Management System (ISMS) by providing essential resources and leadership, ensuring alignment with organizational objectives and ISO 27001:2022 requirements.
The Information Security Forum manages the implementation and continuous improvement of the ISMS. All employees are responsible for adhering to information security policies and procedures and reporting any security incidents promptly.

Software Development Security

We adhere to secure coding practices to prevent vulnerabilities and protect information confidentiality and integrity. Regular security assessments and code reviews help us identify and address risks. Access controls and segregation of duties restrict unauthorized access to development environments and sensitive information.

Risk Assessment and Treatment

Risk assessments are conducted to identify and evaluate information security risks. A Risk Treatment plan has been put in place to mitigate identified risk to an acceptable level.

Security Controls

Security Controls are regularly monitored, reviewed, and updated to address changing security requirements.

Incident Response and Management

All security incidents will be reported, investigated, and documented for analysis and improvement.

Compliance and Audit

Regular audits will be conducted to assess the effectiveness of the ISMS and ensure compliance with ISO 27001:2022 standards.

Training & Awareness

Our organization is committed to fostering a culture of information security awareness and competence amongst all employees. We recognize that regular effective training and awareness programs are crucial in mitigating risks and ensuring the successful implementation of our Information Security Management System (ISMS).

Continuous Improvement

We continuously monitor and evaluate the effectiveness of the ISMS to identify areas for improvement. Corrective and preventive actions are implemented to address deficiencies and enhance the overall security of the organization.

This policy will be communicated to all relevant parties and will be reviewed annually or when significant changes occur to ensure its continued relevance and effectiveness in adhering to information security risks and compliance requirements.

Mark Cornford

Mark Cornford
Chief Executive