KiNGS
SECURE TECHNOLOGIES

Information Security Management System Policy

Scope of the Business

This policy covers the scope of all Group Solutions Limited Companies (Kings) including:

- Kings Security Systems Ltd T/A Kings Secure Technologies
- Kings Guarding Solutions Ltd
- East Fire Extinguishers & Alarms UK Ltd T/A E-fire
- Silver UK Ltd T/A Silver Group
- Cougar Monitoring Ltd
- Quidvis Ltd

Introduction

The purpose of this Information Security Management Policy is to protect the confidentiality, integrity, and availability of information assets within Kings This policy aligns with the requirements of the ISO 27001 standard and establishes a framework for managing information security risks.

Scope

This policy applies to all employees, contractors, and third parties who have access the company's information assets. It encompasses all information assets, including but not limited to data, systems, networks, and physical assets.

Objectives

The objectives of this policy are to:

- Ensure the protection of information assets against unauthorized access, disclosure, alteration, or destruction.
- Maintain the confidentiality, integrity, and availability of information.
- Comply with relevant legal, regulatory, and contractual obligations.
- Establish a culture of information security within the organization.
- Provide a mechanism for the continuous improvement of information security.

Information Security Principles

- **To preserve Confidentiality - t**hat is to protect assets and information from unauthorised disclosure
- **To maintain Integrity** – that is to protect information from unauthorised or accidental modification ensuring accuracy and completeness of the organisations assets
- **To ensure Availability** – that is to ensure that information and assets are available as and when required adhering to the organisations business objectives

Roles and Responsibilities

Kings Management Team are responsible for the day to day operation of the SMS.

All staff have a duty to inform management of any incidents and shall do so via the Incident Management Procedure or the Whistleblowing Policy. This is outlined in individual job descriptions.

The Compliance Team are responsible for ensuring the Security Management System (SMS) conforms to the requirements of ISO 27001 and for reporting on performance and any issues to senior management, either through Management Review or Board reports.

Third parties with access to the companies or its customers information assets must comply with this policy and any applicable contractual requirements.

Leadership

The Chief Executive Officer assumes ultimate responsibility for the SMS demonstrating the commitment and leadership from top management.

The CEO shall ensure adequate resources are available to all managers to maintain the SMS.

Risk Management

To identify through appropriate risk assessment, the degree of protection of all assets, the preparedness against threats, to understand their vulnerabilities and the threats that may expose them to risk.

To manage and minimise risks, to an acceptable level through the design, implementation and maintenance of a formal Security Management System.

Information Security Management System Policy

To comply with legislation including:

- All legislative requirements
- To comply with contractual obligations that lay down the requirements for Asset and Information Security
- Commitment to comply with the requirements of ISO 27001
- Commitment to continual improvement adherence with the controls and where possible implement industry best practice

Risk Treatment

The company will;

- Develop and implement risk treatment plans to mitigate identified risks.
- Monitor and review the effectiveness of risk treatment measures.

Information Security Controls

Access Control

Implement access control measures to restrict access to information based on the principle of least privilege. Regularly review and update access permissions.

Physical Security

Protect physical assets and facilities against unauthorised access, damage, and interference. Implement measures such as access controls, surveillance, and environmental controls.

Incident Management

Establish and maintain an incident management process to detect, report, and respond to information security incidents. Conduct regular incident response exercises.

Business Continuity

Develop and maintain business continuity and disaster recovery plans. Ensure the availability of critical information and systems during and after a disruption.

Training and Awareness

Provide regular information security training and awareness programs for all employees. Ensure that employees understand their information security responsibilities and the importance of protecting information assets.

Monitoring and Review

Monitor information security performance through regular audits, reviews, and assessments. Review and update this policy and the ISMS at least annually or in response to significant changes in the organization or its environment.

Continuous Improvement

Establish a process for the continuous improvement of the SMS. Use feedback from audits, reviews, and incidents to enhance information security practices.

Policy Review

This policy will be reviewed annually by the Compliance Team and be approved by the Board of Directors. Any changes will be communicated to all relevant parties.

Bob Forsyth
Chief Executive Officer