ISMS Executive Support Statement

Reference: ISMS IS-209

Date: 31 January 2024

Classification: Public

Information Security within Davies

As a modern, forward-looking business, Davies recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Davies has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

The operation of this ISMS has many benefits for the business:

- To protect Davies business processes & information assets
- Minimise business disruption & damage
- Maximise return on investments
- Increase credibility, trust & confidence of partners, clients & customers

Our ISMS does this by:

- Working to defined policies, standards, procedures & guidelines
- Implementing processes to evaluate, maintain and manage these policies proportionately to each Business Division
- Building relationships between Information Security and the Business Divisions to develop efficient & effective security planning & compliance

An Information Security Policy is available and is communicated within the organisation and to all relevant stakeholders and interested third parties.

Commitment to the delivery of information security extends to senior levels of the organisation and is demonstrated through the information security policy and the provision of appropriate resources to establish and develop the ISMS.

Top management also ensures that a systematic review of performance of the programme is conducted on a regular basis to ensure that information security objectives are being met and relevant issues are identified through the audit programme and management processes.

A risk management approach and process is used which is line with the requirements and recommendations of ISO/IEC 27001. Risk management takes place at several levels within the ISMS, including:

- Assessment of risks to the achievement of our information security objectives
- Regular information security risk assessments within specific operational areas
- Assessment of risk as part of the business change management process
- At the project level as part of the management of significant change

We would actively encourage all employees and other stakeholders in our business to ensure that they play their part in delivering our information security objectives.

Yours Sincerely,

Dan Saulter, Chief Executive Officer

Validity and Document Management

Information Security is responsible for the maintenance of this document and for assuring that all divisions and business units adhere to the provisions contained within this document.

This document will be reviewed and updated, as appropriate or at least annually to ensure that it meets its legal obligations and business needs.

Contacts

Any queries regarding the policy should be discussed in the first instance with your Line Manager or a member of the Information Security Team as listed below. Please note that where the term "Line Manager" is used this refers to the person you directly report to.

Role	Contact Details
Chief Information Security Officer (CISO)	Sam Hart sam.hart@davies-group.com
Group Information Security & Risk Manager	Pat Stocker info.sec@davies-group.com
Davies Information Security Team	info.sec@davies-group.com

Document Control Table

Version	Author	Details of Change
1.0	P Stocker	New Infosec Policy Document set aligned to ISO 27001 - 2022

Approval

Published Date	31 January 2024
Policy Owner	Information Security
Approved By	Chief Information Security Officer
Next Review Date	1 January 2025