Confidentiality: Public

ISMS Executive Support Statement

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 all stakeholders.

To support this, Davies has implemented an Information Security Management System (ISMS) in alignment with the International Standard ISO/IEC 27001 for information security.

The ISMS offers numerous benefits to the business, including:

- Protecting business processes and information assets
- Minimise operational disruption and potential damage
- Maximise return on investments
- Enhancing credibility, trust & confidence of partners, clients & customers

Our ISMS achieves these objectives by:

- Adhering to defined policies, standards, procedures & guidelines
- Implementing processes to evaluate, maintain and manage these policies across each Business Division
- Fostering collaboration between Information Security and the Business Divisions to ensure effective security planning & compliance
- Committing to ongoing continual improvement

The Information Security Policy is communicated within the organisation and to all relevant stakeholders, including third parties.

Commitment to information security is embedded at all levels of the organisation, demonstrated through the policy and the allocation of resources necessary to establish and maintain the ISMS. Senior management regularly conducts systematic reviews of the program's performance to ensure that information security objectives are met and that relevant issues are identified through audits and management processes.

A risk management approach aligned with ISO/IEC 27001 underpins our ISMS. Risk management is implemented across several levels:

- Assessing risks related to achieving our information security objectives
- Conducting regular information security risk assessments in specific operational areas
- Evaluating risks as part of the business change management process
- Managing risks at the project level during significant change

We encourage all employees and stakeholders to actively participate in supporting and achieving our information security objectives.

Yours Sincerely,

Dan Saulter
Chief Executive Officer

Document Control

Version	2
Effective Date	01-Jan-2025
Policy Owner	Information Security team
Approved By	Chief Information Security Officer

This document is subject to annual periodic review and may also be subject to ad hoc review. The latest version of this document will be published on the Group Intranet and available from Information Security team on request.

The review process and audit history for this document is managed on the Group Policy Management Platform. Document review and approval audit history can be provided by Information Security team on request.