Information Security Policy Statement

The Causeway board of directors ("**Board**") recognises the significance of integrity and security of information. Causeway's Information Security Management Framework ("**ISMF**") has been developed to maintain the highest standard of confidentiality, integrity and availability of internal, customer and supplier information. This forms part of Causeway's Integrated Management System.

The purpose of the ISMF is to protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. The Board commits to providing the resources necessary for the effective operation and continual improvement of the ISMF,. Corporate information is a critical business asset. These assets are identified and managed in accordance with the risk assessment methodology that endorses the acceptable risk levels. Causeway leadership ensures that information security objectives are established and compatible with the strategic direction of the organisation.

The success of Causeway's business is dependent upon the company's ability to store information securely and retrieve and process it as and when required. Such information and the way it may be processed is subject to UK legislation, or regional as appropriate. Information security supports and enables Causeway's strategic objectives, digital transformation, and delivery commitments to customers

Causeway's ISMF is achieved by adherence to controls in Annex A, including policies, processes, procedures and software and hardware functions. These controls are continuously monitored, reviewed, improved and approved by the Board to ensure that specific security and business objectives are met. This is operated in conjunction with other business management processes, and incorporates the applicable statutory, regulatory and contractual requirements. Information security objectives will be measurable, reviewed annually, and monitored for performance.

Causeway's ISMF awareness program is incorporated in our induction process and training program. The ISMF is readily accessible internally and presented to existing and prospective customers.

The ISMF applies to all business units, information assets, systems and processes within the defined ISO 27001 scope whether direct employees of the organisation or Causeway suppliers. All employees are empowered to take responsibility for Information Security and a robust process for identifying and reporting security risks and incidents is in place and is regularly reviewed.

Through compliance to applicable statutory, regulatory and contractual requirements, and the standard for Information Security Management ISO/ IEC 27001, Causeway will demonstrate confidence, integrity and credibility both internally and externally.

Objectives

Causeway's Information Security objectives are set by the Information Security Team and are cascaded throughout the organisation. The objectives include:

(a) To raise awareness of security issues company-wide through proactively communicating the ISMF, incorporating the Information Security policies and supporting procedures;

(b) To raise awareness of the benefits of Causeway being ISO 27001 certified to enhance customer loyalty, reputation and strengthen the Causeway brand;

(c) To establish and monitor an effective Information Security Management System to reduce risk to both Causeway and its customers.

The Information Security Policy is made available to relevant interested parties upon request.

Signed by Phil Brown, Chief Executive Officer

27th January 2026