Group Information Security Policy

Introduction

Clemark, Assent and Lorators store, handle, and process a broad range of information across our group, and we take the responsibilities that come with that very seriously.

It's essential that we maintain the trust of our clients, employees, contractors and other third parties in the Confidentiality, Integrity and Availability of that information.

To meet this unwavering commitment, we have incorporated information security best practices into our everyday business processes through our group integrated management system.

Frameworks and Legislation

As a minimum we commit to be legally compliant with applicable legislation in the territories we operate in. We maintain a register of applicable legal requirements supported by monthly legal updates and an internal audit evaluation of compliance.

In addition, we are committed to complying with the requirements of ISO 27001:2022 as a minimum, with the requirements incorporated into our integrated management system (IMS).

Risk Management Programme

We take a risk-based approach across the group which informs everything we do.

Our risk management framework has been designed using best practices including the international principles of ISO 31000 and considers threats to information security.

We take actions to manage these risks, while balancing our risk appetite to enable us to take advantage of opportunities that are consistent with our core principles.

The risk management programme is reviewed by risk-owners, the compliance team and the board of directors on a regular basis.

Find Out More: https://www.clemarkgroup.com/together/

Information Security Objectives Programme

Through our group objectives programme we maintain **specific, measurable, actionable, results-based and time-bound** information security objectives, with the intention of managing risks to confidentiality, integrity and availability of information.

Information Security Awareness

To ensure that all relevant staff, customers and third parties are aware of our information security programme, and their particular responsibilities within it, this policy is communicated and supported by regular awareness and training activity.

Continual Improvement

We are committed to the continued review and improvement of our IMS in order to reduce the risk of security incidents and ensure continued compliance with contractual, legal and other requirements applicable to the organisation.

Fully Supported

This policy, and the entire IMS, is fully supported by the company's board, compliance team and team members.

Approved by Robert Clements, Founder, 28th November 2025

Find Out More: https://www.clemarkgroup.com/together/