Information Security Policy Statement

Hercules PLC is committed to maintaining and improving information security whilst minimising exposure to risk in line with the strategic direction of the company. The objective of information security is to ensure business continuity by preventing loss of information while preserving confidentiality, integrity and availability.

All organisations create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal. The purpose of our information security policy is to reduce the risk of data loss or theft from internal and external threats. The information security policy also ensures that all employees are aware of their responsibilities for protecting the data held by their organisations.

Our information security management system (ISMS) preserves the confidentiality, integrity and availability of information by applying a risk management process. This provides confidence to interested parties that risks are adequately managed.

The purpose of the policy is to protect the Company's information assets from all threats, whether internal or external, deliberate or accidental, and to ensure that information and vital services are available to users when they need them. It is the policy of the Company to use all reasonably practicable measures to ensure that:

Hercules shall:

- Implement and maintain our company standards to ISO 27001: 2022 requirements.
- Preserve the confidentiality, integrity and availability of information.
- Ensure information is protected from unauthorised access.
- Comply with all applicable legislation and regulations.
- Constantly monitor, review and develop our Information Security Management System (ISMS) and company procedures in order to achieve continual improvement, suitability and effectiveness.
- Set information security objectives, as laid out in our Information Security Management System, and monitor the progress and achievement of these objectives.
- Assign responsibilities for information security management to defined roles.
- Continually review and monitor current and projected information security risks and threats.
- Discuss and review information security issues regularly at the highest levels of the company.
- Ensure appropriate information security controls are in place and implemented as detailed within ISO 27001: 2022 Annex A and ISO 27002:2022. These controls are monitored, reviewed and improved within our Statement of Applicability as necessary.
- Ensure our employees understand and comply with all associated information security policies and procedures.
- Provide appropriate training and communication of information security requirements to employees.
- Ensure that top management understand their responsibilities in information security and are committed to ensuring all employees are aware of and fulfil their information security obligations.
- The Information Security Steering Committee (ISSC) shall continually review the implementation and the effectiveness of the ISMS.

This Information Security Policy is communicated and made available to all employees, learners, clients, contractors, suppliers, and other interested parties. This provides the framework for the review of objectives, documentation and maintenance of Information Security.

The Information Security Policy is supported by internal topic-specific policies to further mandate the implementation of security controls. These policies are aligned and complementary to this Information Security Policy.

This statement should be read in conjunction with the ISMS Manual and procedures, and all managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff. It is the responsibility of each employee to do everything reasonable within their power to ensure that this policy

is carried into effect. Controls are already in place which include the requirements of legislation such as the Companies Act, Data Protection Act and General Data Protection Regulations (GDPR).

Information Security Training:

- 100% of Office and Operations Staff who deal with Personal Data and protection of data in any form undergo full training courses on GDPR.
- 100% of all employees have been trained through induction/briefing/toolbox talk/e-learning on Information Security and GDPR policy and procedure, to a level appropriate to their role.
- Information is sent out by email to all employees detailing any changes to Data Protection Laws, along with our Privacy Statement, policy, procedure and data processing information.

Breaches of Internet Security:

Any breach of information security, actual or suspected, should be reported to, and investigated by, the ISMS Digital Manager, who will report to the appropriate Senior Leadership personnel.

The CEO shall review this policy annually or following significant changes.

Brusk Korkmaz
Chief Executive Officer
Hercules PLC

Approved on: 01/12/2025