

Information Security Policy

|  |
| --- |
| Version History |
| Version No | Version Date | Author | Summary of Changes |
| 1.0 | 24-07-12 | MH | First Issue |
| 2.0 | 31-01-17 | MH | Second Issue |
| 3.0 | 11-04-18 | MH | Third Issue, GDPR Compliance |
| 3.01 | 28-01-19 | MH | GDPR policy adjustment |
| 3.1 | 09-09-19 | MH | 12.4 Multi Factor Authentication2.3 Cloud-based service |
| 4.0 | 27-01-20 | MH | Reformat for ISO27001 |
| 4.1  | 12-06-20 | IMcG | Added section 16  |

|  |
| --- |
| Approvals  |
| Name | Title | Date of Approval |
| Barry Menzies | Technical Director | 26-07-12 – Version 1.0 |
| Matt Harper | ICT Director | 31-01-17 – Version 2.0 |
| Matt Harper | ICT Director | 11-04-18 – Version 3.0 |
| Matt Harper | ICT Director | 28-01-19 – Version 3.01 |
| Matt Harper | ICT Director | 09-09-19 – Version 3.1 |
| Steve Darsey | Chairman | 27-01-20 – Version 4.0 |
| Steve Darsey | Chairman | 12-06-20 – Version 4.1 |

|  |
| --- |
| Distribution |
| Audience | Date of Issue | Version Number |
| Public | 30-7-12 | 1.0 |
| Public | 31-1-17 | 2.0 |
| Public | 11-4-18 | 3.0 |
| Public | 28-01-19 | 3.01 |
| Public | 09-09-19 | 3.1 |
| Public | 27-1-20 | 4.0 |
| Public | 12-06-20 | 4.10 |

**Table of Contents**

1. Purpose
2. Scope
3. Definitions
4. Structure
5. Risks
6. Statement of Applicability
7. Responsibilities
8. Asset Management
9. Physical and Environmental Security
10. Communications and Operations Management
11. Access Control
12. Information Systems Acquisition, Development, Maintenance
13. Information Security Incident Management
14. Business Continuity Management
15. Compliance
16. Independent Review of Information Security
17. Breaches of Policy
18. Disciplinary Policy
19. Deviations from Policy

#### **1.0 Purpose**

Information is an asset that Erith Holdings and all of its subsidiaries, known collectively as The Erith Group, has a duty and a responsibility to protect. The availability of complete and accurate information is essential to enable The Erith group of companies to function in an efficient manner and to provide products and services to customers.

The Erith group holds and processes confidential and personal information on private individuals, employees, partners and suppliers and information relating to its own operations. In processing information, The Erith group of companies has a responsibility to safeguard information and prevent its misuse.

The purpose and objective of this Information Security Policy is to set out a framework for the protection of The Erith Group’s information assets

* To protect The Erith Group’s information from all threats, whether internal, external, accidental or deliberate.
* To enable secure information sharing
* To encourage consistent and professional use of information
* To ensure that everyone is clear about their roles in using and protecting information
* To ensure business continuity and minimise business damage
* To protect the group from legal liability and the inappropriate use of information
* To protect individuals from the risks associated with the loss or misuse of their personal information.

The information security policy is a high-level document and adopts several controls to protect information. The controls are delivered by policies, standards, procedures, supported by training and tools.



#### **Scope**

The Information Security Policy outlines the framework for management of Information Security within The Erith group of companies

The Information Security Policy, standards, processes and procedures apply to all staff and employees of the organisation, contractual third parties and agents of The Erith group of companies who have access to the company’s information systems or information.

The Information Security Policy applies to all forms of information including, but not limited to:

* + - speech, spoken face to face, or communicated by phone or radio,
		- hard copy data printed or written on paper,
		- information stored in manual filing systems,
		- communications sent by post / courier, fax, electronic mail,
		- stored and processed via servers, Storage Area Networks, PCs, laptops, mobile phones, tablets, PDAs,
		- stored on any type of removable media, CDs, DVDs, tape, USB memory sticks, digital cameras, USB Storage Drives
		- stored within any cloud-based service

The Erith Group’s Compliance Team commits to review the changes in Information Security reflecting the risks that the business faces. The Compliance Team will filter the required changes to the Ops Board via the ICT Director. This policy statement ensures the commitment to continual improvement whilst all areas of the business continue to adopt best practices.

# 3.0 Definitions

For the purposes of this document, the following terms and definitions apply:

**Asset**: Anything that has value to the organization

**Control**: Means of managing risk, including policies, procedures, guidelines, practices

**Guideline**: A description that clarifies what should be done and how

**Information Security**: Preservation of confidentiality, integrity, and availability of information

**Policy**: Overall intention and direction as formally expressed by management

**Risk**: Combination of the probability of an event and its consequence

**Third Party**: Person or body that is recognised as being independent

**Threat**: Potential cause of an unwanted incident, which may result in harm to a system

**Vulnerability**: Weakness of an asset that can be exploited by one or more threats

**GDPR**: General Data Protection Regulation

**ISMS**: Defined as the Erith Group’s Information Security Management System

**IASME:** [Information Assurance](https://en.wikipedia.org/wiki/Information_assurance) standard that is designed to be simple and affordable to help improve the cyber security of [Small and medium-sized enterprises](https://en.wikipedia.org/wiki/Small_and_medium-sized_enterprises) (SMEs).

# 4.0 Structure

This policy is based upon ISO 27001 and is structured to include the 11 main security category areas within the standard.

This policy is a high-level policy which is supplemented by additional security policy documents which provide detailed policies and guidelines relating to specific security controls.

The information security policy document sets out the organisation’s approach to managing information security. The Policy is approved by the Board and is communicated to all staff and employees of The Erith group of companies, contractual third parties and agents of The Erith Group. The security requirements for the organisation will be reviewed at least annually by the ICT Director and approved by the Operations Board. Formal requests for changes will be raised for incorporation into the Information Security Policy, processes, and procedures.

# 5.0 Risks

* Data and Information which is collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss and corruption.
* Data and information may be put at risk by poor education and training, misuse, and the breach of security controls.
* Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against The Erith group of companies.
* The Erith group of companies will undertake risk assessments to identify, quantify, and prioritise risks. Controls will be selected and implemented to mitigate the risks identified.
* Risk assessments will be undertaken using a systematic approach to identify and estimate the magnitude of the risks.

Please refer to **5.1.1.6 ICT Risk Register** for further information.

6.0 Statement of Applicability

It is the policy of The Erith group to ensure that information and personal data will be protected from a loss of:

Confidentiality: so that information is accessible only to authorised individuals.

Integrity: safeguarding the accuracy and completeness of information and processing methods.

Availability: that authorised users have access to relevant information when required.

The IT Director will review and make recommendations on the security policy, policy standards, directives, procedures, Incident management and security awareness education.

Regulatory, legislative, and contractual requirements will be incorporated into the Information Security Policy, processes and procedures.

The requirements of the Information Security Policy, processes, and procedures will be incorporated into The Erith group of companies’ operational procedures and contractual arrangements.

The Erith Group’s Board of Directors will ensure that the six principles of the General Data Protection Regulations (GDPR), specifically **5.1.1.06 Data Protection Policy**.

Specialist external advice will be drawn upon where necessary to maintain the Information Security Policy, processes, and procedures to address new and emerging threats and standards. See **6.1.3 Contact with Authorities** and **6.1.4 Contact with Special Interest Groups** for further guidance.

This policy will be updated as necessary to reflect best practices in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and the EU General Data Protection Regulation (GDPR) 2018.

7.0 Responsibilities

The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the organisation and in its dealings with third parties. See **6.1.1 Information Security Roles and Responsibilities**.

Department Heads are responsible for ensuring that all staff and employees, contractual third parties and agents of The Erith group of companies are made aware of and comply with the Information Security Policy, processes and procedures.

The Erith Group’s auditors will review the adequacy of the controls that are implemented to protect The Erith group of companies’ information and recommend improvements where deficiencies are found.

8.0 Asset Management

Please refer to **8.1.1 ICT – Asset Management Policy** for details about how the Erith Group manages tangible and non-tangible assets.

# 9.0 Physical and Environmental Security

# Please refer to **5.1.1.02 ICT Policy** with regards to Security arrangements, **11.1 ICT – Erith Group Secure Areas** and **5.1.1.6 ICT Risk Register** for the corresponding Risk Assessments

# 10.0 Communications and Operations Management

The Erith Group will operate its information processing facilities securely.

Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.

Appropriate operating procedures will be put in place. See **5.1.1.02 ICT Policy**

Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse. See **16.1.1 ICT – ICT Department Responsibilities**, **6.1.1 – ICT Information Security Roles and Responsibilities** and **5.1.1.06 ICT Data Protection Policy**

Please see **18.1.5 ICT – Regulation of Cryptographic Controls** for information on how the Erith Group complies and assists with regulators and authorities in relation to cryptography.

Please see **13.1.1 ICT – Erith Network Security** VPN Locations for schematics of the WAN underpinning Erith Group operations.

11.0 Access Control

Please refer to **9.1.1 ICT – Access Control Policy** for details about how the Erith Group manages access to restricted information.

# 12.0 Information Systems Acquisition, Development, Maintenance

Please refer to **14.2.1 ICT - Secure Development Policy**

# 13.0 Information Security Incident Management

Please refer to **5.1.1.02 ICT Policy** for security incident reporting information

# 14.0 Business Continuity Management

Please refer to **5.1.1.05 ICT Policy** for Business Continuity Policy information and **17.1.2 ICT – DR Plan** for Disaster Recovery information

# 15.0 Compliance

Please refer to section 5.0 of **5.1.1.02 ICT Policy** for details about how the Erith Group remains up to date with legislative changes which affect the Group’s Information Processing activities.

# 16.0 Independent Review of Information SecurityThe Erith Group have signed up to the Cyber Essentials Plus security program which is a government backed scheme. The program is designed to audit the Erith Group security controls to the high standard set by the accrediting body, IASME.

# The Cyber Essentials Plus scheme covers external and on-site assessments of Erith Group ICT assets. The Erith Group use the Cyber Essentials Plus audits as part of the overall security program to review the in-house processes and ensure they are functioning to a high standard.

# In addition to the yearly Cyber Essential Plus audits the Erith Group will seek independent Security advice and reviews from specialised cyber security contractors in order to look into key projects as and when required.

# 17.0 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to the Erith Group’s assets, or an event which is in breach of the Erith Group’s security procedures and policies. All Erith Group employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of the Information Security Policy as quickly as possible through the Erith Group’s Incident Reporting Procedure see 5.1.1.02 ICT Policy. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Erith Group.

The Erith Group will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. Where it becomes apparent that there may have been a breach of this policy by an employee then the matter may be dealt with under the disciplinary process.

**18.0 Disciplinary Process**

The Erith Group reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the Erith Groups Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

**19.0 Deviations from Policy**

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall need to be reported to and approved by the ICT Director.

Signed for and on behalf of

The Erith Group



Steven Darsey

Chairman