**

ICT Procurement & Third-Party Security Policy

|  |
| --- |
| Version History |
| Version No | Version Date | Author | Summary of Changes |
| 1.0 | 20/05/2020 | MH | First Issue |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| Approvals  |
| Name | Title | Date of Approval |
| Matt Harper  | ICT Director | 20/05/2020 |
|  |  |  |
|  |  |  |

|  |
| --- |
| Distribution |
| Audience | Date of Issue | Version Number |
| Public | 20/05/2020 | 1.0 |
|  |  |  |
|  |  |  |

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Policy Statements
5. Responsibilities
6. Policy

6.01 Risk Review

6.02 ICT Supplier Review / Data Exchange Agreement

6.03 Compliance and Certification

6.04 Information Security within Contracts (Appointment of a Service Provider / Collaborator)

6.05 Service Provider / Collaborator Relationship Management

6.06 ICT Supplier Review Process

6.07 ICT Supplier Review Process (Roles and Responsibilities)

6.08 Technical Security Review (Testing and Assessment)

6.09 Transfer / Security of Erith Group Assets

6.10 Security Incident Response

6.11 Freedom of Information Request (FOI)

6.12 Legal Obligations and Policies

6.13 Compliance and Monitoring

1. Breaches of Policy
2. Disciplinary
3. Deviations from Policy

#### **1.0 Purpose**

The need to secure information is now a legal and moral requirement, rather than an option. Information is a vital asset to any organisation and virtually all the Erith Group’s activities create information in one form or another.

This policy sets out the conditions that are required to maintain the security of the Erith Group’s assets via an ICT procured and contracted service. ICT services may be required to use, create, access and store Group assets (either information or equipment)

 **2.0 Scope**

The scope of this policy includes any Preferred Suppliers or Specialist ICT Contractors who may be required to deliver goods or perform services. An example of which may include:

* Financial Control Systems
* Network Equipment and Software
* Database / Server / Storage solutions
* Programming / Code Writing / Software adaptation (see 5.1.1.07 ICT Secure Development Policy)
* Printing / Copying / Scanning services

This is not an exhaustive list and is provided as an indication as to the scope of this policy. ICT Services that are provided and managed by the ICT Department include provision of support for that service or asset. Examples include:

* Resource and day-to-day management of the procured service / ICT asset
* Training and skills to be able to manage the procured service / ICT Asset
* Incident and Problem Response Management

The ICT Department, specifically the ICT Servicedesk, will be the central point of contact for all Erith Group managed services and centrally managed assets.

#### **3.0 Definitions**

‘*Erith Group*’ is a collection of companies that lie under the Erith umbrella. All these companies are referred to as the Erith Group. For the purposes of this document the companies within the Erith Group are known as, Erith Contractors Ltd, Erith Haulage Company Ltd, Erith Business Solutions Ltd, Erith Training Services Ltd, Swanton Consulting Ltd and Erith Plant Services Ltd.

‘Supplier’ is defined as any third-party company or individual who may provide goods or services to the Erith Group

‘Contractor’ is defined as any third-party company which undertakes a contract to provide materials or labour to perform a service or to do a job.

‘ICT Service Desk’ or ‘ICT Helpdesk’ is defined as the software portal through which first contact is made regarding any request for service / software / hardware.

‘ISR’ is an acronym for ‘ICT Supplier Review’

‘ISMS’ is defined as Information Security Management System.

**4.0 Policy Statements**

Procedures are in place to ensure the effective use of the ICT Procurement & Third-Party Security Policy and the following statements underpin these procedures:

* All Erith Group staff and operatives that have access to information assets have a responsibility to handle them appropriately and in accordance with their classification.
* Information asset owners are responsible for ensuring that the Erith Group’s classification scheme (8.2.1 ICT – Classification of Information), is used appropriately.
* Erith Group’s information assets should be made available to all who have a legitimate need for them.
* The integrity of information must be maintained and must also be accurate, complete, timely and consistent with other related information and events.
* The ICT Department operates to provide ICT services to all Erith Group staff and will provide support to staff when selecting third-party suppliers. The ICT Service Desk should be contacted in the first instance before making any approaches for ICT services to a third-party.

#### **Responsibilities**

Directors are responsible for ensuring that staff and managers are aware of the Erith Group’s ICT Information Security Policies and that they are complied with.

* Any supplier / contractor / service provider which has access to the Company’s assets (either information or equipment) must always agree to follow the Erith Group’s Information Security Management System (ISMS).
* Erith Group staff must assess the risk that assets may be exposed to by employing external ICT Service Providers.
* All ICT contracts with service providers must be monitored and reviewed to ensure that current Erith Group Information security requirements are being satisfied.
* All Suppliers / Contractors / Service providers must be approved using form P10(ICT)

**6.0 Policy**

**6.01 Risk Review**

All ICT services must have a risk assessment undertaken and the risks mitigated prior to the services being adopted.

The ICT Department will assess risks and will make decisions as part of the following activities

* Awarding ICT Service Contracts / Collaboration
* Reviewing arrangements with new or existing ICT Service Providers / Collaborators (for examples), to ensure that their promises are evidenced.
* Understanding how Erith Group assets will be managed and secured on a day to day basis
* Release of Erith Group Information Assets (see table 1 below)

|  |  |
| --- | --- |
| **Data Sharing – Identifiers that could be communicated following review** | **Data Sharing – Identifiers which should NEVER be communicated** |
| The Identifiers below are subject to formal review prior to sending to a third party or collaborator. It is dependent on the nature of use, whether there are other means of collecting the data and whether it is required for critical Erith Group systems and operations | These identifiers must NEVER be communicated publicly and / or transferred to a third parties as part of external collaborations due to legislation and general security of Erith Group systems and data |
| * User ID / Username
 | * Gender
 |
| * First Name
 | * Marital Status
 |
| * Surname
 | * Ethnicity
 |
| * Mobile / Landline / Teams ID
 | * Religion
 |
| * Email Address
 | * Sexual Orientation
 |
| **These identifiers are not an exhaustive list and are subject to change dependent on Erith Group Systems and Controls** | * Country of Nationality
 |
| * Health or Disability Records
 |
| * Address
 |
| * Date of Birth
 |
| * PIN / Password
 |
| * Payroll Number
 |
| * National Insurance Number
 |
| **Data / Identifiers must NOT be disclosed unless disclosure has been agreed by the ICT Director and consent from Staff or Operatives has been given and can be evidenced.** |

**Table 1 – Erith Group collected / owned data and identifiers**

**6.02 ICT Supplier Review / Data Exchange Agreement**

All Erith Group assets, to which a service provider / collaborator has access to or requires access to, must be handled in accordance with procedures which satisfy legislative, regulatory and Group risk and security management activities. The details of these procedures will depend on the nature of the data and identifiers required for that service.

The table below shows the types of reviews, services and documents that will assist the ICT Team in appointing a collaborator and / or service provider.

|  |  |
| --- | --- |
| **Pre-Contract / Collaboration** | **Completion of Risk Review / Mitigation and Appointment** |
| Pre-Release of Data / Risk Review |  |  |
| **ISR** | **Data Exchange Agreement** | **Formal Contract** |
| Erith Group staff who are authorised and responsible for appointing service providers / collaborators or release of Group assets must complete an ICT Supplier Review (ISR) prior to awarding / appointing a contract or agreement of work or releasing data. | Where all risks identified within the initial ISR assessment have been mitigated appropriately. | Where formal contracts are required or for advice, restrictions and boundaries of a formal contract please refer to the Procurement Team in the first instance. |
| The ISR should be completed and reviewed by the ICT Director as soon as possible to ensure the risk assessment can be undertaken appropriately | Where a formal contract is not required, the staff member must ensure that a non-disclosure / Data Exchange agreement has been signed and accepted by the Collaborator / Service Provider. |
| Failure to send the completed ISR within a reasonable timescale may delay or defer the Information Security compliance audit and delay the risk assessment or project entirely. | Advice and guidance from commercial / finance, Compliance Team and/or the Group’s registered Data Protection Officer should be sought in the first instance. |
| Email the ICT Service Desk for further information at **helpdesk@erith.com** | For further information, please refer to the **Data Protection Officer** or **ICT Director** | For further information, refer to the Procurement Team at **procurement@erith.com** |

**Table 2 – Professional Services Review (ISR / Data Exchange Agreement (NDA) and formal contract**

**6.03 Compliance and Certification**

Evidential requirements for IT Service providers can include, but are not limited to:

* ISO27001 Compliance / Certification
* PCI-DSS Compliance / Certification
* Data Protection Registration Number / Association
* ADISA Registration (Asset Disposal and Information Security Alliance)
* Evidence of Information Security Framework and Documentation
* Evidence of workings with specific standards / associations / controls of security industry bodies e.g. ITIL

**Where evidence of compliance and certification cannot be established, the Erith Group, as part of its review and continuous improvement activities, must undertake an assessment of the third-party controls prior to allowing access to Group assets (information or otherwise).**

**If compliance and certification cannot be evidenced, other mitigating controls should be evidenced from the service provider, for example:**

* **Personnel background checks e.g. DBS and CCJs**
* **Protection of Data Methods (both physical and technical)**
* **Incident / Business Continuity / Disaster Response Plans**
* **Terms and Conditions of Support Services**
* **Special Interest Group (SIG) recommendations (see 6.1.4 ICT – Special Interest Groups)**

**6.04 Information Security within Contracts (Appointment of a Service Provider / Collaborator)**

**Staff responsible for agreeing ICT Service contracts must ensure that the terms and conditions do not contravene the Erith Group’s ISMS, standard procurement policy, procedures, and supplier codes of conduct. All documentation must be forwarded to the ICT Director for vetting prior to signature by an authorised officer of the business.**

**All Erith Group contracts must ensure boundaries of undertakings and protection of Group assets for the full duration of the contracted services. Contracts and services must:**

* **Be monitored and reviewed annually to ensure that information security requirements are being satisfied.**
* **Include appropriate provisions to ensure the continued security of information and systems if a contract is terminated of transferred to another supplier.**
* **Be able to demonstrate compliance with the Erith Group’s ISMS.**
* **Include specific acceptance of the Group’s ISMS**
* **Include an undertaking that Group assets will be retained or transferred to the Group upon completion of contracted works and that any sensitive data will be removed from the provider’s data sources.**
* **Ensure that the contract / agreement states that Erith Group data being transferred will only be used for the purposes of collaboration and no data will be transferred to any third parties for any other purpose.**
* **Include a right to audit. The Erith Group must ensure that the right to audit is agreed with the contracted service prior to acceptance of the contract.**

**6.05 Service Provider / Collaborator Relationship Management**

**It is imperative that the Erith Group and its appointed service provider or collaborator understand the Group’s position of continuous improvement.**

**Regular compliance and monitoring must be undertaken by the Erith Group about its assets. For more information, please review 5.1.1.08 ICT – Information Security Review Policy.**

**6.06 ICT Supplier Review Process**

****

**Figure 1 – ISR Review Process**

**6.07 ICT Supplier Review Process (Roles and Responsibilities)**

**The ISR form must be completed and reviewed before any contracts or orders are placed. Failure to supply all relevant information may delay the process. The ICT Department will request further input from other teams in the Group as required.**

**The ICT Director or the Systems Manager will undertake a security review of the information provided within the ISR. Either will consult and advise on the potential risks and threats to the Erith Group and / or its assets, with mitigation and follow up actions required, if necessary.**

**6.08 Technical Security Review (Testing and Assessment)**

**If sensitive Group assets (Confidential) are involved, this may require technical security assessments to be undertaken prior to introducing new services to the production ICT environment**

**To ensure that procured ICT Services are ‘fit for purpose’ and do not pose a risk to the Erith Group and its Core Network Infrastructure, person outside of the ICT Department are not permitted to place orders for services. Appropriate technical reviews and guidance must be sought in advance of any work.**

**6.09 Transfer / Security of Erith Group Assets**

**Any assets created, used, accessed, processed, managed and stored by the service provider / collaborator (including any third-party contractors, subcontractors or other entities hired by the awarding service provider, as part of an Erith Group ICT development or service), which are considered to be the property of the Group, must be:**

* **Securely transferred to the Erith Group**
* **Securely removed from non-Erith Group data sources**

**6.10 Security Incident Response**

**Should the service provider or contractor encounter any security risks or threats which may impact the Confidentiality, Integrity or Availability of Erith Group assets, they must inform the Erith Group within a reasonable timeframe to allow the Group to undertake the necessary remedial action. Please review the Information Security Incident Response sections of 5.1.1.02 Information Technology Policy and 5.1.1.01 – ICT Information Security Policy for further guidance**

**6.11 Freedom of Information Request (FOI)**

**Any information requested by an approved authority, third party, or member of the public under the Freedom of Information Act is to be referred to the Erith Group’s Data Protection Officer in the first instance. This role will ensure that all requests are responded to within the agreed timeframe, and within the structured process set by the Information Commissioner’s Office (ICO).**

**6.12 Legal Obligations and Policies**

**This policy is aimed at all Directors, Staff and Operatives of the Erith Group of Companies who have a responsibility for the use, management, and ownership of information assets. It is a part of the Group’s Information Security Management System (ISMS) and should be read in conjunction with 5.1.1.01 ICT - Information Security Policy, its sub policies, and relevant UK Legislation. Further relevant policies and legislation are listed in 5.1.1.02 ICT – Information Technology Policy.**

**6.13 Compliance and Monitoring**

**All Directors, Staff and Operatives of the Erith Group are directly responsible and liable for the information that they handle. All are bound to abide by the Group’s ICT policies and procedures by the terms and conditions of their employment.**

**Authorised ICT Department staff may monitor the use and management of information assets to ensure effective, and authorised use.**

**7.0 Breaches of Policy**

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.

**8.0 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.

**9.0 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.