*f*

ICT Policy

(Information Communications Technology)

|  |  |  |  |
| --- | --- | --- | --- |
| Version History | | | |
| Version No | Version Date | Author | Summary of Changes |
| 1.0 | 31.1.17 | MH | First Issue |
| 2.0 | 11.04.18 | MH | Compliance  13.7 Social Networks |
| 2.10 | 04.12.19 | IMcG | 6.13 Removable Media |
| 2.11 | 05.12.19 | IMcG | New Definitions |
| 2.12 | 09.12.19 | IMcG | 6.14 Standard Operating Procedures |
| 2.13 | 13.01.20 | IMcG | 6.15 Electronic Messaging |
| 3.0 | 27.01.20 | MH | SD Signature |
| 3.01 | 18.02.20 | MH IMcG | Change of Senior Management Intent. Section 1.0 paragraph 2. Reference 1876566-202001-N2 |
| 3.02 | 19.02.20 | IMcG | CCTV Section added 6.16 |
| 3.03 | 12.03.20 | IMcG | Supporting utilities / ATP / Clear Desk |
| 3.04 | 27/03/20 | IMcG | Added Section 16 Privileged Utilities |
| 3.05 | 04/06/20 | MH | Added section 6.19 concerning “Unattended User Equipment” |
| 3.06 | 05/06/20 | MH | Add section 6.20 Removal of information or software  Added section 6.21 Access to Program Source Code |
| 3.07 | 05/05/20 | IMcG | Added section 6.22 Clock Synchronisation |
| 3.08 | 26/01/21 | IMcG | Added PAT to section 6.02 Hardware |
| 3.09 | 23/12/2021 | IMcG | BYOD section added |
| 3.10 | 13/07/2022 | IMcG | Updated the SOP section |
| 3.11 | 7/12/2022 | MH | Changes to 6.23 BYOD surrounding third party owned devices and SIMs removed from company devices, administrative privileges |

|  |  |  |
| --- | --- | --- |
| Approvals | | |
| Name | Title | Date of Approval |
| Matt Harper | ICT Director | 31.01.17 v1.0 |
| Matt Harper | ICT Director | 9.9.19 v2.0 |
| Steven Darsey | Chairman | 27-01-20 v3.0 |
| Steven Darsey | Chairman | 18-02-20 v3.01 |
| Steven Darsey | Chairman | 19-02-20 v3.02 |
| Steven Darsey | Chairman | 12/03/20 v3.03 |
| Steven Darsey | Chairman | 27/03/20 v3.04 |
| Steven Darsey | Chairman | 05/06/2020 v3.07 |
| Steven Darsey | Chairman | 21/01/2021 v3.08 |
| Steven Darsey | Chairman | 23/12/2021 v3.09 |
| Matt Harper | ICT Director | 13/07/2022 v3.10 |
| Matt Harper | ICT Director | 7/12/22 v 3.11 |

|  |  |  |
| --- | --- | --- |
| Distribution | | |
| Audience | Date of Issue | Version Number |
| Public | 31.01.17 | 1.0 |
| Public | 9.9.19 2019 | 2.0 |
| Public | 27-01-20 | 3.0 |
| Public | UNISSUED | 3.01 |
| Public | UNISSUED | 3.02 |
| Public | UNISSUED | 3.03 |
| Public | 27/03/20 | 3.04 |
| Public | 05/06/2020 | 3.07 |
| Public | 21/01/2021 | 3.08 |
| Public | 23/12/2021 | 3.09 |
| Public | 13/07/2022 | 3.10 |
| Public | UNISSUED | 3.11 |

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Structure
5. Policy Statements
6. Responsibilities
7. Disciplinary Process
8. Safe Use of ICT Equipment
9. Arrangements
10. Enterprise Voice (Mobile and Fixed Line)
11. Inductions and New Starter Packs
12. Auditing and Monitoring
13. Business Continuity Planning
14. Controls Against Malware
15. Use of Privileged Utility Programs

#### **Purpose**

The Erith Group recognizes the need to keep up-to-date with technology and supply chain advancement and to provide its customers and staff with an ICT infrastructure that supports its Core Values, acknowledges Best Practice, and is capable of ‘exceeding customer expectations’.

The Executive and Operations Boards recognises that continual improvement and investment into Information, Communications Technology Services and the ISO27001:2013 Information Security Management System is essential to the Business, to support the development of its processes and its staff.

The Chairman will appoint a Director to be responsible for the management of ICT and to oversee strategic development.

The main objective of ICT is to ensure Information Security, deliver strategy, to support the Group and ensure that employees have controlled access to corporate knowledge. With increasing use of electronic communication, it is essential that the Erith Group protects its systems from illegal, defamatory, fraudulent, or other misuse.

Improvement Plans will be recommended and approved at Operations Board Meetings prior to implementation, to ensure that they continue to focus and deliver against business needs.

The IT Director, in conjunction with the Main and Operations Boards, will prepare an annual budget to ensure that what is planned can be provided for. It is the responsibility of the Board of Directors to ensure that once approved, the appropriate budget is made available.

The Erith Group recognises that the ICT infrastructure alone is insufficient to guarantee success. The Board is therefore committed to providing training in the ICT network, system maintenance/development and licensed software, as required.

As ICT is such an integral part of The Erith group’s operations and essential to the delivery of information not only internally but also to the customer and supply chain, The Erith Group will ensure that a robust ICT continuity plan will be put in place.

This does not form part of the contract of any employee and the Erith Group reserves the right to change this policy at any time without notice.

#### **2.0 Scope**

This policy is to be read in conjunction with 5.1.1.1 ICT Information Security Policy, and contains guidance on the measures that must be taken by Erith Group employees, workers, third party contractors, and any other users to ensure that Erith Group ICT systems and the information contained thereon, are adequately secured and appropriate standards are met. It also outlines when the Erith Group will monitor the use of ICT systems.

#### **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 Erith Group Ltd, Erith Business Solutions Ltd, Erith Training Services Ltd, Swanton Consulting Ltd and Erith Plant Services Ltd.

To avoid confusion, the ICT systems constitute the following:

* Network servers,
* Cabling, Communications equipment and Wireless WANS and Mobile Data Routers / Personal MiFi devices
* Desktop, Laptop computers, PDAs and Tablets
* Printers, scanners, photocopiers
* Licensed software, CRM and ERP portals
* Landline and Mobile Telephones
* Other software or hardware connected to such equipment

‘Third Party Provider’ is a term used to designate a company other than an Erith Group member who is contracted to provide support or Installation services on any Erith Group System.

Removable media is defined as any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and [Blu-Ray](https://whatis.techtarget.com/definition/Blu-ray) disks, as well as diskettes and [USB drive](https://searchstorage.techtarget.com/definition/USB-drive)s.

AV Realtime Shield is defined as virus protection featuring automatic protection which checks computer systems for suspicious activity in real-time. It detects malicious objects, once they are accessed or started. The Erith Group has enabled Predictive Offline Protection from the application vendor’s central database.

Malware is defined as software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Ezone is branding assigned to the browser-based, on-premise hosted Customer Relationship Management (“CRM”) and Document Management System (“DMS”) that the Erith Group maintains in respect of project and business related information. The system is developed and maintained by Deltek Inc.

COINS is the browser-based, on-premise hosted Enterprise Resource Planning (“ERP”) system provided by Construction Industry Solutions Ltd covering core financials, payroll, plant control, procurement and supplier relationship management.

‘O365’ is Microsoft Office 365. A Software as a Service (SaaS) solution that includes Microsoft Office and other services, such as email and collaboration, from Microsoft's cloud server. Microsoft Office 365 also provides desktop functionalities and MFA.

‘OneDrive’ is Microsoft's storage service for hosting files in the "cloud.". OneDrive offers users a simple way to store, sync and share various types of files, with other people and devices on the Internet.

A ‘network domain’ is an administrative grouping of multiple private computer networks or hosts within the same infrastructure. Domains can be identified using a domain name.

‘Group Policy’ is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

‘Mobile device management’ (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network.

‘UPS’ - Uninterruptible Power Supply, refers to a device that provides battery backup when the electrical power fails or drops to an unacceptable voltage level. Small UPS systems provide power for a few minutes; enough to power down the computer in an orderly manner, while larger systems have enough battery for several hours.

‘ATP’ Advanced threat protection refers to a category of security solutions that defend against sophisticated malware or hacking-based attacks targeting sensitive data.

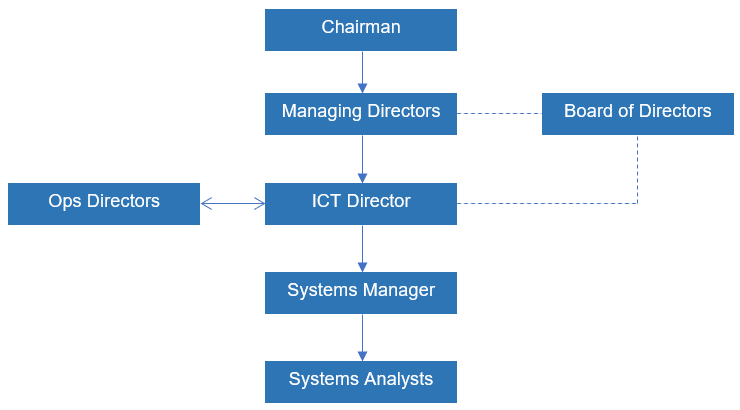
‘Active Directory’ is the mechanism by which user and group access is leveraged to provide targeted and restricted access to software and information.

‘ACL’ is defined as an Access Control List which is a list of users stored as a group within Windows Server Active Directory.

‘ICT Helpdesk/Service Desk’ is a portal, within the ICT Department designed specifically for systems administrators and IT professionals to manage requests and task within the department.

‘BYOD’ - Bring your own device (BYOD) refers to an employee using a personal devices to connect to Erith Group networks and data.

#### **4.0 Structure**



The Erith Group’s ICT systems are managed by the ICT Director and administered, delivered and supported by the ICT Team. The ICT Service Desk is the first point of contact in respect of system difficulties and development ideas.

#### **5.0 Policy Statements**

The general ICT Policy for the Erith Group is described below:

The entire Erith Group information system will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality.

To satisfy this, Erith Group will undertake to carry out the following.

* Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
* Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
* Implement ICT Policy and all information Security Policies in a consistent, timely and cost-effective manner.

Where relevant, the Erith Group will comply with:

* UK Data Protection Act 2018 (inclusive of GDPR)
* Communications Act 2003
* Freedom Of Information Act 2000
* The Telecommunications (lawful Business Practice and Interception of Communications) Regulations 2000
* Computer Misuse Act 1990
* The Electronics Signatures Regulations 2002
* The Telecommunications (Data Protection & Privacy, Direct Marketing) Regulations 1999
* Regulation of Investigatory Powers Act 2000 (RIPA)
* Business Continuity Practice Guide: 2006 (UK Tripartite Authorities: Financial Services Authority (FSA), HM Treasury, Bank of England)
* Copyright, Designs and Patents Act 1988 (CDPA)
* The Human Rights Act 1998 (HRA)

The Erith Group will comply with other laws and legislation as appropriate. The policy forms part of the ICT Security policy and reflects the objectives of the Information Security Management System (ISMS).

The Erith Group will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network infrastructure that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

#### **6.0 Responsibilities**

6.01 Use and Possession of ICT Equipment

ICT equipment supplied by the Erith Group is to be used only for Erith Group purposes, and any information held thereon is considered to belong to the Erith Group. See section below on downloads 3.3.15 – 3.3.18.

Employees will be expected to treat any ICT equipment in their possession with care - bearing in mind the value of the equipment and, more importantly, the value of any information thereon.

Employees are to be mindful of the security of any ICT equipment whilst in their possession. The Erith Group is not insured for ICT thefts from vehicles, therefore, if any ICT equipment is taken away for use outside the office it shall be kept in secured place (i.e. glove box, car boot) ICT equipment should be placed out of sight of opportunist thieves. All ICT equipment is to be removed from vehicles overnight.

Where equipment is lost or stolen and the Erith Group requirements are not complied with, there may be a charge to the individual concerned for a replacement.

Mobile Telephones, Computing Devices, Tablets, and other devices are to be kept secure at all times. Where email data is stored thereon, this is a particular security risk. Care should be taken to ensure that the handset is kept out of view when not in use.

Mobile telephones and other devices are supplied to staff for business use only and maybe used for personal reasons with the express permission of an Operations Director.

ICT equipment is supplied for the exclusive use of employees of the Erith Group and is not to be used by family, or any other third party.

Whilst there is an acceptance by the Erith Group that devices from time to time may be required to be used for personal transactions this must be limited to “reasonable” use only. The Erith Group hold the right to a) charge b) disciplinary action for extreme usage.

Should any employee leave the Erith Group, it is expected that all ICT equipment be returned in the condition in which it was given excepting acceptable wear and tear as decided by the IT Director. Equipment will be logged and signed for using 8.1.4 COR (Confirmation of Receipt). If equipment is not returned when an employee leaves, the Erith Group reserves the right to either recover the value from the employee or delay the release of monies due pending the return of the equipment.

6.02 Hardware

Computer hardware and associated peripherals will be made available to its workforce by the Erith Group to suit its business activities.

The Erith Group expects employees to use the computing equipment provided in their day to day activities. However, the use of personal equipment is acceptable, with prior agreement of the ICT Department, and ensuring that all systems are patched to the highest level and will include the Erith Group’s current Anti-Virus application and ZScaler. The Erith Group will accept no responsibility for personal equipment used in conjunction with Erith Group owned equipment; damage to Erith Group equipment arising from such use will be the employee’s sole responsibility.

All hardware devices acquired by the Erith Group or developed by it (through its own employees or through those hired by the Erith Group to develop the hardware devices) is and always shall remain Erith Group property. All such hardware devices must be used in compliance with applicable licences, notices, contracts and agreements paying attention to legislation stated at Section 5.0.

All requests for ANY ICT equipment (other than site set-up) must be made through the ICT Department via a Service Desk request. The ICT Department will provide budget costs on formal requests prior to the equipment being procured. The relevant Operations Director will provisionally authorise the need and identify the capital investment expenditure authorisation code/requirement.

Employees will be expected to report any faults with ICT equipment in their possession as soon as possible. Maintenance or repair must only be carried out via the ICT Team. Priority will be given according to severity and business criticality.

Employees will be given access to appropriate network printers. In some limited cases, employees may be given local printers if deemed necessary by the employee’s manager, in consultation with the ICT Department.

Where required Hardware will be protected behind a UPS Uninterruptible Power Supply - A device that provides battery backup when the electrical power fails. UPS’s are installed within all the Erith Groups Core Comms rooms.

Equipment users will ensure that equipment is maintained to a suitable standard and protected from damage, from being dropped, from coming into contact with any liquid and will be carried in a bag appropriate for its size and weight. The ICT Team will always provide an appropriate carry case where required for any equipment supplied. The end user is entitled to purchase their own bag at their own cost should they so wish, however it must be appropriate and provide adequate protection. The aim of this policy statement is to ensure the continued availability and integrity of the equipment.

All ICT portable hardware will be safety checked as part of the Erith Group portable appliance testing (PAT) schedule. PAT is an examination of electrical appliances and equipment to ensure they are safe to use. Where equipment is reported to have failed the PAT then is will be taken out of action and disposed of via the Erith Group 8.3.2.1 ICT WEEE Waste Policy.

6.03 Software

The Erith Group will provide a suitable network infrastructure using the best of the locally available network infrastructure. Erith Group equipment and software will be configured to be suitable for use on this infrastructure.

The Erith Group will provide suitable software for use with ICT equipment, ensuring control of software licenses. Standardisation of applications will be exercised wherever possible. Requests for additional software should be made through Line Managers, who will evaluate the need and confirm procurement requirements with the ICT Department. The ICT Department will seek authorisation from the relevant Operations Director to maintain cost control.

The Erith Group is mindful of the legal penalties for the use of unlicensed software. Consequently, all software must be installed by, or under the direction of, the Erith Group’s ICT Department. Installation of personally acquired applications is strictly forbidden since ownership of the application may infringe copyright laws and contravene other legislation shown in Section 5.0

6.04 Permission to Install Software, Third Party Vendors and External Users

Software is only to be installed by an authorised employee or Member of the ICT Department. This applies equally to application upgrades, as well as new applications. There are systems in place to restrict the installation of any new software, and only authorised ICT department members or employees can install software on Erith Group assets, all other Erith Group employees do not have the rights to install software as per the local security settings on all Erith Group computers. Software installation requests should be sent to the helpdesk where they will be reviewed and acted upon if approved. If a purchase is required, the cost will require authorisation from the Operations Director responsible for the area of the business within which the requester works. Audits and network scans will be performed on the network at regular intervals these are all logged within the ICT department, ICT Management channel.

Any damage or problems caused to the Erith Group by installation of personal, third party software/unauthorised upgrades and use of personal unauthorised software, may result in the individual being subject to disciplinary action.

Employees will use only appropriately licenced web-based or cloud-based applications and any such use will be monitored by the ICT Department to ensure legislative compliance.

Third Party providers must liaise with the ICT Department prior to installing or upgrading any information/operational system. Only approved vendors will be granted access to make changes and form 14.2.1.1 Privacy Impact Assessment must be completed following the Third-Party Provider’s acceptance of the Erith Group’s mutual Non-Disclosure Agreement. All internal changes/installations to information/operational system will have to be approved by the ICT Director via a helpdesk change request. The change request will have a plan of action with a rollback procedure added to the request before the changes can be made. The change/installation can then be performed by an authorised member of the ICT team, once the change request has been authorised.

No Third-Party equipment maybe plugged into the Erith Group’s network or computer systems without prior written permission from the ICT Department.

6.05 Protection against Viruses, Trojans, Phishing Emails, Network Security incidents and any other Malware

Any suspected viruses on ICT equipment must be reported to the Erith Group’s ICT Department as soon as suspicion is aroused. Continued use of the equipment must cease immediately until the ICT Department has authorised continued use. The equipment in question MUST be disconnected from any network, wireless or wired, until instructed by the ICT Department.

If you fall victim to a Phishing email or any other security incident, then this must be reported immediately to the ICT Department.

Under no circumstances are any third-party files (e.g. via USB, Flash drives) to be copied either from or to Erith Group ICT equipment, unless an approved anti-virus checking mechanism is installed.

The Erith Group has deployed ATP and all emails will have to pass through a comprehensive scan before they are delivered to the employee.

6.06 Security of Stored Information

The Erith Group will ensure that work files stored within Ezone, Regional File shares, Teams and Exchange are regularly backed up for security purposes and/or in case of equipment failure.

At main office locations sufficient resources will be allocated to facilitate backing-up of files to the network daily. Back up data will be kept for a minimum of ten days.

All files and data created by employees shall be stored on a server or database whenever possible. Note that the business does not provide backup for individuals’ laptops unless the Desktop, Documents and Photos locations are synchronised with Microsoft OneDrive. All processing hardware that leaves the ICT Department will have this feature enable, along with version rollback.

6.07 Passwords

Employees must refer to Policy 9.3.1 ICT Password Policy for guidance on password selection, together with complexity and timeframe requirements.

6.08 File Sharing, Downloads, Media Streaming and Connectivity and Network Performance

The use of file sharing applications such as Kazaa, Limewire, Azureus and any other BitTorrent application is not permitted on any corporate equipment. Similarly the Erith Group does not condone the illegal download or streaming of Copyrighted material such as Movies and Applications. The Erith Group does not allow the use of Netflix on corporate devices inclusive of Desktops, Laptops, Tablets and Smartphones. This is to prevent additional cost arising from the waste of bandwidth on metered connections.

The use of downloaded and unlicenced software is illegal, and will be dealt with in accordance with the Erith Group’s disciplinary procedure. Relevant law enforcement authorities may also be involved, dependent upon the severity of the situation.

The use of illegally downloaded MP3 files is not permitted at any time or at ANY location. The Erith Group is not licensed to execute music files on corporate equipment. Breaches will be dealt with under the Erith Group’s disciplinary procedure. This is to prevent additional cost arising from the waste of bandwidth on metered connections.

The Erith Group monitors the performance of its Wide Area Network and Employees are not authorised to log on to internet radio sites, or to stream events from the internet. The Erith Group does not hold a Performing Rights Licence to broadcast such events. In addition, the use of such websites creates performance issues on the network which prevents legitimate traffic from being sent and received.

It is forbidden to use an Internet connection without the permission of the owner of the connection, this covers Wi-Fi connections that are not password protected, always seek permission before connecting.

It is not acceptable to download photographs or other files from the internet without appropriate permission, even if they are intended for Erith Group use. In the case of photographs these should be purchased through a licensed website, such as (but not limited to) iStock Photo.

6.09 Acceptable Use

Employees and potential users of any Erith Group communications system should make themselves aware of 5.1.1.03 Acceptable Use Policy before its use to ensure that awareness is brought about of the types of uses which are deemed to be acceptable.

6.10 Social Media

The inclusion of any Erith Group brand within a post on any Digital Social Media platform is strictly prohibited. The Erith Group’s view on the use of Digital Social Media is binary. The use of Social Networks for posting comments to deliberately cause distress or threaten, as well as any information, stories, conjecture, or opinion (personal or otherwise) regarding any Erith group business or business activity is strictly forbidden and monitored. The Board takes this extremely seriously and appropriate disciplinary action will be taken if this clause is not complied with.

6.11 Use of Corporate Email

Email is available for internal and external business communications only. Personal use is permitted in so far as this is subject to compliance with 5.1.1.03 Acceptable Use Policy.

Employees must be mindful of 18.1.3 Information Classification Policy and apply the relevant Cryptography Protocols (see 10.1.1 ICT - Cryptography Policy for details on how to apply the correct encryption and retention periods to protectively marked information. Sending offensive or indecent images of others is forbidden on the corporate email system.

6.12 Legislation

Employees are always reminded of their obligation to act within the law and Erith Group Policy.

Particular attention is drawn to the criminal law requirements in respect of:

* Publishing obscene material (downloading and/or sharing pornography);
* Civil law issues of libel and copyright.
* Employment law, such as publishing documents that could be viewed as discriminatory and contrary to the Erith Group’s Equal Opportunities Policy.
* Other obligations under the Human Rights Act, the Data Protection Act and Contracts (Rights of Third Parties), etc.
* Using only licensed hardware and software
* Broadcasting without a Performance Rights Licence
* unauthorised access to computer material
* unauthorised access with intent to commit or facilitate commission of further offences
* unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

6.13 Removable Media

Removable Media within the Erith Group is only allowed where there is a genuine business need and no other alternative system in place.

The Erith Group has adopted a Real time Anti-Virus Shield on all Erith Group Devices, removable media will be scanned for Malware in real time as data is accessed on the media to ensure that viruses are not transferred onto the Erith Group Network Infrastructure.

If data classified as Internal or Restricted is transferred to removable media an Encrypted Removable Media Device is required this will need to be approved and then assigned by the ICT Department, Please review 8.2.1 Classification of information policy and 10.1.2 ICT - Cryptography Control Policy for More information.

Removable Media that has been used to store Internal or Restricted Information will be disposed of securely in the same way as all electrical waste please review 8.3.2.1 ICT WEEE Waste Policy, all Hard Drive Destruction Certificates are to be stored on Ezone.

All Devices and Media that have become end of life due to age or damage must be returned to the ICT Department so that all data can be wiped or backed up where there is a genuine business need for the information.

The Erith Group has adopted a cloud storage backup system, whereby all core servers are backed up over 256-bit encrypted connections off site, giving the Erith Group a full off site backup in the event of an onsite disaster.

Where the Transfer of removable media is not avoidable then a trusted courier will be used and the media will be signed for, ensuring the media reaches its intended recipient. If the information is classified as restricted or internal, then encryption will be used as per the 8.2.1 Classification of information policy and 10.1.2 ICT - Cryptography Control Policy.

6.14 Standard Operating Procedures

The Erith Group has created a catalogue of documented operating procedure called SOPs, (Standard Operating Procedures) that will be stored within Sharepoint. The SOPs will be the first port of call for certain day to day operations within the Erith Group as a whole and specifically the ICT Department where required. The SOPs will be developed, maintained, secured, and made available to all employees that might need them to perform a task. SOP’s that are classified as Internal for the users will be stored within [Information Security - ISO27001:2013 - SOPs (user) - All Documents (sharepoint.com)](https://erithcontractorslimited.sharepoint.com/sites/InformationSecurity-ISO270012013/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2FInformationSecurity%2DISO270012013%2FShared%20Documents%2FSOPs%20%28user%29&FolderCTID=0x012000F4FB1D4356F80A4B93C8A311A3BEE700).

SOPs will be reviewed and maintained regularly ensuring they are kept up to date and current.

The ICT Department will maintain a Live SOP register within SharePoint.

All ICT SOP’s that are classified as restricted will be stored within the secure ICT Management channel in Teams.

6.15 Electronic Messaging

The Erith Group Monitor and audit all incoming and outgoing email messages, to ensure their security and compliance with the Erith Groups company policies.

Where required confidential information that is sent out will be done so in accordance with the Erith Group’s 8.2.1 Classification of Information Policy,

The Erith Group uses DLP controls to limit the opportunity of confidential data leaving the business, these controls are built into the fabric of the mail system.

The Erith Group has deployed an active real time shield on all its endpoints that actively scans for malware.

The Erith Group blocks Phishing and SPAM Emails at source with Advanced Threat Protection, in the event of any emails getting past the ATP, then the Erith Group has a comprehensive security awareness program, to teach employees, how to identify and deal with SPAM and Phishing.

The Erith Group has deployed MFA to access the Company Email System.

6.16 CCTV

The Erith Group has deployed CCTV throughout the Group’s buildings and sites, some of these locations may have face recognition technology as an extra security control, whereby your likeness maybe recorded and stored within the system. Where face recognition technology is in operation signage will be visible.

6.17 Clear Desk

Erith Group employees are required to ensure that all restricted and confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

Computer workstations must be locked when workspace is unoccupied.

Any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

File cabinets containing restricted or sensitive information must be kept closed and secured when not in use or when not attended.

Keys used for access to restricted information must not be left at an unattended desk.

Laptops must be locked away or taken home by an authorised employee at the end of the workday. Passwords may not be left on sticky notes posted on or under a computer.

6.18 Unattended Equipment

Any device capable of processing or displaying information shall remain locked when unattended.

6.19 Security of Cabling

The cabling to any device, either on a desk, under a desk, in a communications room rack system or attached to a photocopier should be managed to remain efficient and not present any risks to Health and Safety. Wiring must not be loose, must be tagged, make uses of cable runs and ways between desks, use the channels inside a server cabinet, laid along a wall and accessible carrying minimum risks. Communications rooms must be kept clear, tidy, and associated cabling should use the cable canals inbuilt. Communications cabinets should be locked unless they are not accessible without biometric solutions. Electricity Panels, Fire Panels, Burglar Alarms, CCTV Control Systems and Biometric Controls will remain locked and segregated from ordinary access.

6.20 Removal of Information or Software

In the same way that it is forbidden for Physical Assets to be removed from premises operated by the Erith Group, any Information or Software is not permitted to be removed from any system without the approval of the ICT Helpdesk and possibly, where relevant, the approval of the Data Protection Officer. It is imperative that labeled and classified Information remains protected for the lifespan specified in 8.2.1 ICT – Classification of Information.

Information may not be shared with a Third-Party without the necessary data exchange agreements in place, See 15.1 ICT – ICT Procurement and Third-Party Security Policy.

6.21 Access to Program Source Code

No standard Domain User will be permitted access to any source code to reverse engineer, decompile or make alterations to the original specification of any software product purchased or designed for use within the Erith Group. This will be governed by use of an electronic Windows Active Directory ACL.

No standard Domain User will be permitted to make changes to the running source code that constitutes Ezone or COINS. This will be governed by use of an electronic Windows Active Directory ACL.

No Standard Domain User will be permitted to access the raw database information running any software application with the Erith Group. This applies specifically to Ezone and COINS. Any database changes made will be logged by the system automatically.

If changes are required to a running application, then they must be submitted to the ICT Helpdesk and follow the processes laid out within 5.1.1.07 ICT – Secure Development Policy

Access to Source Code will be granted within the guidelines of 6.1.1 ICT – Roles and Responsibilities.

6.22 Clock Synchronisation

The **Erith Group uses the Windows Time Service and NTP - Network Time Protocol to ensure all servers and computer on the Erith Group Network are synchronised to the same time. The Erith Group operates solely out of the GMT time zone this ensures that all audit logs and event logs are easily readable.**

**Where assets are not connected to the Erith Group domain but the time keeping for logs and audits is crucial then the use of cn.pool.ntp.org and pool.ntp.org for time management is permitted.**

6.23 BYOD

**The Erith Group allows employees or External parties to be able to use their own devices if approved by the ICT Department.**

**To get approval the device must meet the following requirements;**

* **Have an industry recognised Antivirus solution installed and up to date.**
* **Have an operating system that is set to update automatically and has the latest security patches installed.**
* **The IT Department needs to be given the IP address of the devices and a local admin username and password to perform a vulnerability scan to ensure its compliancy. The certification will last for one year from date of issue.**
* **If the BOYD asset owner is external to the Erith Group they must sign an NDA.**
* **The External Party must Supply the Erith Group IT Department with a copy of their; IT Policy, Information Security Policy, Acceptable Use Policy, Data Protection Policy, if they are not ISO27001 certified.**
* **The device MUST be connected to Erith’s Active Directory and manageable in the same way as a company-owned device. The owner will lose administrative access and control over their device, and it will be treated as though it is a company-owned device.**
* **Company-owned voice and data SIMs should never be removed from the device that they are issued with and on no account should be used in a personally owned device unless any such device is managed within our SOTI Mobile Device Management (MDM) platform.**

**The personal device must also be used in accordance with all current Erith Group policies and procedures****.**

6.23 Administrative Privileges

Only authorised employees will be given access to administrative privileges, any user requiring administrator-level rights must be approved at board level.

**7.0 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.

**8.0 Safe Use of ICT Equipment**

8.01 Display Screen Equipment (“DSE”)

All employees who are habitual users of Display Screen Equipment are required to complete a DSE Assessment. Any necessary workstation adjustment will be discussed with an appropriately trained person.

8.02 Mobile Devices

Employees must ensure that they have read and understood the Erith Group *6.2.1 ICT - Mobile Device Policy*, which sets out both security and safe operating guidance.

No employee or anybody working on behalf of the Erith Group is permitted to use a mobile device whilst in control of a vehicle or item of plant.

8.03 Teleworking

All employees that have a need for Teleworking, where a particular employee works at an offsite location, on a regular or long term basis, must ensure they have read and adhere to the Erith Group *6.2.2 ICT - Teleworking Policy.*

**9.0 Arrangements**

The Erith Group is committed to providing employees with the requisite information on how to comply with the details contained within this Policy, if further information is required then contact the ICT Servicedesk.

**10.0 Enterprise Voice (Mobile, Fixed Line)**

Any users of telephony services on behalf of the business should refer to 5.1.1.03 Acceptable Use Policy to ensure that the guidelines are implemented whilst representing the Erith Group.

**11.0 Inductions and New Starter Packs**

Guidance is available to employees within the standard induction packs issued to new starters and thereafter via the ICT Department. All new employees must complete the Induction and Sign off on reading the Core Erith Group Policies and Procedures.

**12.0 Monitoring and Audits**

12.01 Audits

The Erith Group will carry out regular audits of software on Erith Group ICT equipment. Any software found that has not been installed by the Erith Group will be immediately removed, whether this has an impact on saved information or not. The relevant employee’s Operations Director will be informed at the earliest opportunity and it will be their responsibility, to consider the disciplinary situation arising from such occurrences.

Information system audit controls are in place and all audits that could have an adverse effect on operations or system performance are performed out of working hours. All audits are logged on the Erith Group Helpdesk as well as the corresponding audit schedule log. Daily and weekly automated audits are emailed to the ICT Director and ICT Systems Manager for review and any follow up actions are logged within the Erith Group Helpdesk.

12.02 Monitoring

The Erith Group operates software to monitor all communications and Internet access (particularly suspect emails which may contain viruses) and reserves the right to retrieve any messages or contents of e-mail messages.

The purpose of such actions is to monitor whether the use of the system is legitimate, to find lost messages or to comply with any legal obligations.

Due to business need, it may be necessary for a Line Manager to gain access to employee mailboxes, files and folders, privileged database permission areas, to respond to or deal with issues that may arise during absence. However, this can also be achieved via a request to ICT and approval given by a Director / Operations Director of the business.

“For Purpose Monitoring”/”Searching of Employees files” - this will only be carried out with the prior knowledge of the employee, normally as a result of or part of an investigation/disciplinary process.

**13.0 Business Continuity Planning**

Please refer to Policy 5.1.1.05 Business Continuity Planning for further information.

**14.0 Controls Against Malware**

Antivirus protection is used within the Erith Group on all computers, servers, mobile phones and tablets.

The Erith Group has group policies that install antivirus software on all computers and servers as they join the Erith network domain. The Erith Group also deploys an MDM on all our tablets and android mobile phones that incorporates antivirus protection.

All internet traffic is passed through a Firewall, which is used to block unwanted access and malware getting on to the internal Erith Group network.

The Erith Group used a mobile application-based firewall, which is installed on laptops this allows the Erith Group to keep mobile devices secure if they leave the safely of the Erith Group network. This application-based firewall is also used for web filtering and rules have been setup to block sites and traffic that is deemed unsafe for the Erith Group.

Erith Group Employees are not granted access to install software on their computers and laptops and approval from the ICT Department, via a request on the ICT Service desk is required to install any software. These request for software must be approved by the ICT Department and if required a director will need to approve the purchasing of any licences.

Technical controls are in place to protect against SPAM and Phishing Email, although there is a constant risk that some email may circumvent the controls and be delivered to the recipient. The Erith Group has a comprehensive education program that helps to educate the users in identifying this type of malware, please review 7.2.2 Information Security Awareness Education and Training, for more detail.

The Erith Group has been accredited with the Cyber Essentials Plus scheme since 2017 and this involves a yearly audit performed by a Third-Party scanning Erith Group Assets for vulnerabilities that could be exploited by Malware. Within the Erith Group we also do internal scanning to ensure we are up to date with the latest patching, and Malware definitions.

All Erith Group Servers and Computers are enrolled on a remote management system where software patches and updates can be rolled out automatically, helping to keep the underlying Operation system up to date.

The Erith Group uses O365 and has deployed OneDrive within the business. OneDrive acts like a secondary backup of all the files and storage held on the computer, in the event of the loss of functionality of a device due to malware the files will be accessible via the OneDrive account on another machine, this backup is held offsite so it won’t be effected by the malware.

**16.0 Use of Privileged Utility Programs**

The Erith Group installs privileged utility programs on all its mobile devices, inclusive of laptops, desktops, and servers. These programs are special purpose utilities that can perform specific tasks. The utility programs that the Erith Group deploy have the ability to; delete data, update software, defragment disks, format data drives, run scripts, perform virus scans, remotely control the host system, view audit logs, monitor device resources, lactation services via GPS, and monitoring of web traffic.

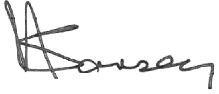
For this reason, unsupervised, and unauthorised use of these programs is a high risk. therefore, the programs are locked down and only privileged users, will be able to use these specialist tools.

The installation of non Erith group approved privileged utility programs is strictly forbidden and the installation without authorisation will be blocked by the enforced ICT installation group policies that are rolled out to the Mobile Devices, inclusive of Laptops, Desktops and Servers.

If an Employee requires access to a privileged utility program they can do so via a request to the helpdesk, if the request is approved the user will be given access to the privileged program for the required time to perform the task, once access is no longer required then access will be removed.

Signed for and on behalf of

The Erith Group



Steven Darsey

Chairman