Policy Document

Information Security

01/06/2026

Policy Title:	**ERH Information Security Policy**

Issue Date:	01/06/2026	**Date policy is to be reviewed:**	01/06/2027

Version:	1.1	**Issued by:**	Chris Petrucco
Scope	Whole Organisation		

Review and consultation process:	Annually from the review date above. IT Manager / Circle IT to oversee process
Responsibility for Implementation & Training:	Chris Petrucco/Mike Duffy

Distribution:	Via email attachment, publishing on the company Intranet, by email to suppliers where applicable.

Revisions:		
Date:	**Author:**	**Description:**

Table of Contents

Introduction

This Information security policy is a key component of ERH Ltd management framework. It sets the requirements and responsibilities for maintaining the security of information and assets within ERH Ltd. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

ERH Ltd recognises that individuals and organisations with which we conduct business value their privacy. However, in order to provide timely and secure services the collection of client information is often necessary and desirable. ERH Ltd is committed to protecting the privacy and security of individuals and individual business clients encountered whilst conducting its business, specifically related to ERH Ltd data management products.

Aim and Scope of this policy

The Managing Director is ultimately responsible for defining information security policy and standards. Other Directors, Managers and Staff are responsible for implementing the information security policies and standards. All employees and service providers of ERH Ltd are responsible for meeting the requirements of the policies and standards.

It is our intent to prevent and minimise the impact of information security incidents and deliver assurances to clients and other stakeholders that its information assets are protected from all types of threat, whether internal or external, deliberate or accidental.

The aims of this policy are to set out the rules governing the secure management of our information and physical assets by:

- preserving the confidentiality, integrity and availability of our business information
- ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies
- ensuring an approach to security in which all members of staff fully understand their own responsibilities
- creating and maintaining within the organisation a level of awareness of the need for information
- detailing how to protect the information and physical assets under our control
- Specifying company access control and physical security requirements

This policy applies to all information/data, information systems, networks, applications, locations and staff of ERH Ltd or supplied under contract to it.

Responsibilities

- Ultimate responsibility for security rests with the Managing Director of ERH Ltd, but on a day-to-day basis the IT Manager shall be responsible for managing and implementing the policy and related procedures.
- Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by The IT Manager. Both the Policy and the Risk Register shall be reviewed annually.
- Line Managers are responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:-
    - The security policies applicable in their work areas

    - Their personal responsibilities for physical and information security
    - How to access advice on physical and information security matters

- All staff shall comply with the security policy and must understand their responsibilities to protect the company's data and assets. Failure to do so may result in disciplinary action.
- Line managers shall be individually responsible for the security of information within their business area.
- Each member of staff shall be responsible for the operational security of the information systems and company assets they use or operate within.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contract shall require that the staff or subcontractors of the external organisation comply with all appropriate security policies and hold the required certifications.

Acceptable Use

- All staff, contractors, consultants and other workers of ERH Ltd must act in appropriately regarding the use of information, electronic devices and networks resources in accordance with ERH Ltd.'s policies and procedures as well as laws and regulations.
- All staff and contractors should ensure that if the device is left unattended, it is locked at all times.
- All employees and contractors must ensure that no sensitive information (including physical documents) is not left unattended and should be securely stored when not in use.
- Under no circumstance should any staff member attempt to purposefully misuse any of ERH Ltd.'s devices, systems and networks, email communications, social media, or accounts.
- Under no circumstances is an employee of ERH Ltd authorised to engage in any activity that is illegal under local or international law while utilising ERH Ltd-owned resources.
- This also includes the unacceptable use of the internet by visiting sites that contain obscene, hateful, or otherwise offensive or illegal material.
- The above is not an exhaustive list but attempts to provide a framework for activities that could fall into the category of unacceptable use.
- Those found misusing any of ERH Ltd resources will be subject to disciplinary action.

Legislation

- ERH Ltd is required to abide by certain UK, European Union and international legislation. It also may be required to comply with certain industry rules and regulations.
- The requirement to comply with legislation shall be devolved to employees and agents of ERH Ltd, who may be held personally accountable for any breaches of information security for which they are responsible.
- In particular, ERH Ltd is required to comply with:

    - The Data Protection Act (2018)
    - The Computer Misuse Act (1990)
    - The Health and Safety at Work Act (1974)
    - Human Rights Act (1998)
    - Regulation of Investigatory Powers Act 2000
    - Freedom of Information Act 2000

Personnel Security

Information security training will be available to all staff and forms part of the induction training for new starters. Supporting procedures are in place defining security policy with regard to availability of information and information systems, virus controls, password controls and software encryption. All breaches of information security, actual or suspected, are reported to the IT Manager, who is responsible for maintaining the security policy and providing advice and guidance on its implementation. It is the responsibility of each employee to adhere to this policy, to implement its principles through good practice outlined by senior staff. It is our objective to ensure that all staff are fully aware of their responsibilities within the ISMS.

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff shall be verified and a passport, driving licence or other document shall be provided to confirm identity.
- For specific roles ERH Ltd may require new staff to pass DBS checks.
- Information security expectations of staff shall be included within appropriate job definitions.
- Whenever a staff member leaves the company, their accounts will be disabled the same day they leave.

Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
- Security awareness training shall be included in the staff induction process and shall be carried out annually for all staff
- An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information and generic security is maintained and updated as necessary.

Email & Communication Activities

When using ERH Ltd resources to access and use the Internet, users must realise they represent the company. Questions may be addressed to the IT Manager.

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via social media, email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Intellectual Property Rights

- The organisation shall ensure that all third-party software is properly licensed and approved by the IT Manager.
- ERH Ltd Intellectual Property Rights (IPR) shall be protected at all times.
- ERH Ltd IPR information shall be classified and identified as Confidential.

- ERH Ltd IPR information shall be recorded and tracked within the company information asset register and stored in accordance with its classification.
- Users breaching this requirement may be subject to disciplinary action.

Access Management

Physical Access

- Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.
- Access to ERH Ltd offices and facilities shall be controlled by physical barriers and an auditable process and procedure.
- All personnel are required to wear a clearly visible identification (ID) badge or card when within ERH Ltd offices or facilities. This shall include visitors who will be signed in/out and provided with temporary ID.

Password Policy

ERH Ltd employees must ensure the following for all devices (where applicable):

- Passwords must offer an adequate level of security to protect systems and data
- All passwords shall be 8 characters or longer and contain at least two of the following: uppercase letters, lowercase letters and numbers
- All mobile devices must have a PIN of at least 4 characters.
- Two-factor authentication shall be used to provide additional security
- For those devices that are ERH Ltd owned, a lockout policy will be in place after 3 unsuccessful attempts.

Guidance for Passwords:

- Avoid using common or discoverable passwords (i.e. pet's name, street name etc)
- Use long passwords
- Consider using password management software i.e. LastPass, Keeper.

User Access

- Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a business need to access the information
- All users shall use uniquely named user accounts
- Generic user accounts that are used by more than one person or service shall not be used.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by the IT Manager.
- A list of individuals with administrator-level access shall be held by the IT Manager and shall be reviewed every 6 months
- Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.
- Administrator-level accounts must not be used for web browsing or accessing email.
- Administrator-level accounts must not be shared by multiple personnel.

Application Access

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only.
- ERH Ltd development network shall be appropriately segregated from the ERH Ltd business and operational networks and facilities.

System Perimeter access (firewalls)

- The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
- All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly.
- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.
- There shall be a documented business case in place for all open ports. The business case shall be authorised by the IT Manager

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- The business reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

Asset Management

ERH Ltd information and equipment assets records are maintained by the IT Manager and stored within the organisation's data management system.

Asset Ownership

- Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.
- Each information or physical asset ownership shall be recorded within the ERH Ltd asset register.

Asset Records and Management

- An accurate record of business information and physical assets, including source, ownership, modification, classification, location and disposal shall be maintained.
- All data shall be securely wiped from all hardware before authorised disposal.

Asset Handling

- ERH Ltd shall identify particularly valuable or sensitive information assets through the use of data classification.
- All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.

- All company information shall be categorised into one of the three categories in the table below based on the description and examples provided:

Category	Description	Example
Unclassified	Information which is not classified and can be made available through any channels.	• Details of products and services on the website • Published company information • Social media updates • Press releases
Commercial or Commercial Personal	Information which, if lost or made available to unauthorised persons could impact the company's effectiveness, benefit competitors or cause embarrassment to the organisation and/or its partners	• Company operating procedures and policy • Client contact details • Company plans and financial information • Basic employee information including personal data
Confidential	Information which, if lost or made available to unauthorised persons, could cause severe impact on the company's ability to operate or cause significant reputational damage and distress to the organisation and/or its partners. This information requires the highest levels of protection of confidentiality, integrity and availability.	• Client intellectual property • Data in e-commerce systems • Employee salary details • Any information defined as "sensitive personal data" under the Data Protection Act

Removable media

- Only company provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store business data and its use shall be recorded (e.g. serial number, date, issued to, returned).
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the IT Manager before they may be used on business systems. Such media must be scanned by anti-virus before being used.
- Where indicated by the risk assessment, systems shall be prevented from using removable media.
- Users breaching these requirements may be subject to disciplinary action.

Mobile working

- Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements.
- Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the IT Manager.
- Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for

the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.
- Users must inform the Technical Director immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

- Where identified, staff may use personal mobile phones to access business email. This usage must be authorised by the IT Manager. The device must be registered in the asset records and must be configured to comply with this policy
- Personal devices must be supported by a manufacturer and be updated to the latest revision of Operating System (OS) software within 14 days of release
- Any software that is no longer used or needed is to be removed from the device. This includes any free/ trial software that comes included on the device
- All default passwords should be changed and comply with ERH Ltd password policy, detailed in this policy. This should take place every time a new device is being set up or has been compromised
- BYOD equipment shall be protected by antimalware software which conforms to ERH Ltd specifications as detailed within this policy
- ERH Ltd have the right to access and/or remove ERH Ltd data from personal devices used for business purposes
- Staff who use personal devices for ERH Ltd business must register and sign to confirm that they will comply with the BYOD aspects of this policy
- Ensure that they aren't using the local administrator account for day-to-day use and only use the administrator account for administrative purposes.
- Ensure that auto-run / auto-play has been disabled. For Mac users, the default setting is that auto-run is disabled. For Windows users, this can be found by searching "autoplay settings" and toggling "use AutoPlay for all media and devices" to off.
- No other personal devices are to be used to access business information.

Business Use of Social Media

- Social media may only be used for business purposes by using official business social media accounts with authorisation from the IT Manager. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.
- Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.
- Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the IT Manager.
- Users breaching this requirement may be subject to disciplinary action.

Personal Use of Social Media

- ERH Ltd allows employees to access their personal accounts at work. Employees are expected to act responsibly and ensure their productivity is not affected. Using personal social media excessively while at work can reduce efficiency and concentration and must therefore be restricted to break periods.
- Additionally, where an employee's personal social media profiles identify their association with ERH Ltd, care must be taken when posting content whilst on Company business, travelling out of hours or socialising on a business-related event or trip.
- Examples of non-acceptable use include but are not limited to:

- Disregarding job responsibilities and deadlines to use social media.
- Disclosing confidential or proprietary information through personal or business accounts.
- Directing offensive comments towards other members of the online community.

Physical and Environmental Management

- In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.
- Systems shall be protected from power loss by UPS if indicated by the risk assessment.
- Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

Computer and Network Management

Operations Management

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the IT Manager.

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the IT Manager.

Accreditation

- The organisation shall ensure that all new and modified information systems, applications and networks include security provisions.
- They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the IT Manager before they commence operation.

Software Management

- All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.
- All software security updates/patches shall be installed within 14 days of their release.
- Only software which has a valid business reason for its use shall be installed on devices used for business purposes
- Users shall not install software or other active code on the devices containing business information without permission from the IT Manager.
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

Local Data Storage

- Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).
- A backup copy shall be held in a different physical location to the business premises
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

External Cloud Services

- Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

- The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
- All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system.
- All anti-malware software shall be set to:
    - scan files and data on the device on a daily basis
    - scan files on-access
    - automatically check for, and install, virus definitions and updates to the software itself on a daily basis
    - block access to malicious websites

Vulnerability scanning

- The business shall have a yearly vulnerability scan of all internal networks and external IP addresses carried out by a suitable external company.
- The business shall act on the recommendations of the external company following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities.
- The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

Response

Information Security Incidents

- All breaches of this policy and all other information security incidents shall be reported to the Managing Director
- If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Managing Director.
- Information security incidents shall be recorded in the Security Incident Log and investigated by the IT Manager to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident reoccurring.

Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Reporting

- The Managing Director shall keep the business informed of the security status of the organisation by means of regular reports to senior management.

Further Information

- Further information and guidance on this policy can be obtained from the IT Manager. Comments and suggestions to improve security are always welcome.