HRP40 Kirby Information Security Policy

Adopted:	25th May 2025
Contact Officer:	Fergus Barry
Last Amended/Reviewed:	25.05.2025
Version/Reviewed by:	V0 – 25.05.2025 by Fergus Barry
Next Formal Policy Review:	2 Yearly Next Review due – 24.05.2027
Formal Review of Policy by:	Fergus Barry
Policy Links:	This policy links to all policies, procedures and strategy documents adopted by Kirby Group Engineering. Specific reference is made to the following documents: • Disciplinary and Grievance Procedures • Dignity at Work Policy
Policy signed into effect by:	

HRP40 KIRBY INFORMATION SECURITY POLICY

1. Purpose and Scope

This policy encompasses all aspects of information technology ("**IT**") security at the Company and should be read by all staff in its entirety. The document will be reviewed, updated and recirculated periodically.

The purpose of the Information Security Policy is to:

(a) protect the integrity of the company's data and system resources from outside interference and cyber security threats; and

(b) secure the confidentiality of all electronically stored data owned or stored by the firm.

The Company's IT Department is responsible for the administration of this policy. The Board is responsible for the enforcement of the policy. Third parties who may have access to the Company's electronic communication systems and equipment are also required to comply with this policy.

Breach of this policy will result in disciplinary action up to and including dismissal for employees, or removal from the premises for agency workers / contractors / 3rd parties. Any employee of the Company suspected of committing a breach of this policy will be required to co-operate with the Company's investigation. Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

2. Information Security Principles

Computer information systems and networks are an integral part of the Company's business. The Company has made substantial investments in human and financial resources to create these systems.

This policy has been established to:

(a) protect the Company's investment in computer systems;

(b) safeguard the information contained within computer systems;

(c) reduce business and legal risk; and

(d) protect the good name of the Company.

The contents of the Company's IT resources and communications systems, hardware and software, are the property of the Company.

Employees should therefore have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on electronic information and communications systems provided by the Company.

Employees are advised that any attempts to remove personal data, client details or company information, whether in hard copy, soft copy, by email or otherwise from Company systems may be regarded as a data breach and/or theft. For the avoidance of doubt, this includes the distribution of such information outside Company systems, e.g. to personal email addresses of employees. Acts of theft constitute gross misconduct and may, in certain cases, constitute a criminal offence. The Company's property is a critical asset and the Company will take appropriate steps to protect it, up to and including reporting the matter to the appropriate authorities. The Company is also obliged under the General Data Protection Regulation to take appropriate steps to respond to and prevent data breaches occurring.

The Company reserves the right to monitor, intercept and review, without notice, employee activities using our IT resources and communications systems, including but not limited to social media postings and activities, to the extent reasonably required to ensure that our rules are being complied with. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of messages, communications, postings, log-ins, recordings and other uses of IT systems as well as keystroke capturing and other network monitoring technologies.

While the Company does not ordinarily use such systems to monitor individual employees, it reserves the right to use such information, and to retrieve the contents of email messages, voicemail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the legitimate interests of the business for the following purposes:

(a) for security purposes;

(b) to monitor compliance with Company policies including in relation to email and internet usage, intellectual property and confidential information; or

(c) to assist in the investigation of any potential breach of law, employment contract or workplace policies.

Employees must:

(a) handle Company information in a manner consistent with its sensitivity;

(b) use Company information and telecommunication systems for personal means in moderation and in a manner which avoids interference with job performance;

(c) not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;

(d) not disclose company, employee, customer or supplier data unless authorised;

(e) keep passwords and accounts secure;

(f) request approval from the IT Manager prior to establishing any new software or hardware, or third party connections;

(g) not install unauthorised software or hardware, including modems and wireless access unless without the express approval of the IT Manager;

(h) always leave desks clear of sensitive data and lock computer screens when unattended; and

(i) report information security incidents without delay to senior management.

All employees share responsibility for ensuring Company systems and data are protected from unauthorised access and improper use.

3. Employees' Own Personal Data

Employees are not permitted to use the Company's computer systems for matters that they wish to keep private or confidential from the Company. Storage of personal information on the Company's systems is not permitted. If an employee leaves the Company, all stored personal information is deleted without the possibility of a call-back.

Employees are not permitted to register for, or in any way use their company provided email addresses on publicly accessible websites, forums, boards, or other media for personal use.

4. Acceptable Use

The Company has an established culture of openness, trust and integrity. The guidelines on acceptable use are designed to protect the Company and its employees from illegal or damaging actions by individuals, either knowingly or unknowingly.

Web access is only permitted via secure proxy servers. Exceptions must be approved by the IT Manager. Strict policy enforcement limits web access to business related and low-risk site categories.

(a) Employees must exercise good judgment regarding the reasonableness of personal use of Company computer systems, services and devices;

(b) Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies;

(c) Employees should take all necessary steps to prevent unauthorised access to confidential data;

(d) Employees should ensure that technologies are set up and used only in acceptable secure network locations;

(e) Employees should keep passwords secure and not share individual account details;

(f) Authorised users are responsible for the security of their passwords and accounts;

(g) All PCs, laptops, tablets and workstations are secured with a password-protected screensaver with the automatic activation feature. If the computer screen saver does not automatically activate, the Company should be advised;

(h) Because information contained on portable computers, tablets and mobile telephones is harder to secure, special care and attention of these devices should be exercised by all staff members.

(i) Employees must use extreme caution when releasing email messages from the spam filtering system and when opening e-mail attachments received from unknown senders, which may contain malware, crypto lockers, viruses, e-mail bombs, Trojan horse code or other cyber security threats to the company.

5. Social Media

Social media should never be used in a way which may breach any of the Company’s policies. Employees are personally responsible for what they communicate on social media. Remember that what you publish might be available to be read by the public (including the Company itself, clients, customers, suppliers, future employers and social acquaintances) indefinitely. Please keep this in mind before you post content.

Employees should not:

(a) breach any obligations relating to confidentiality;

(b) defame or disparage the company or its partners, clients, customers, suppliers, competitors, other employees, or other stakeholders;

(c) harass or bully anyone or any other individual in any way;

(d) breach data protection, GDPR, or privacy obligations; and

(e) breach any other laws or ethical standards. Employees should never comment on other employees of the Company on social media or professional networking sites, since any such references, positive and negative are a breach of privacy and security and could be attributed to the organisation and create a legal liability for both the author and the Company.

Posts by employees from a Company E-mail address to newsgroups, blogs, wikis, websites, and social media sites such as Facebook, Twitter, LinkedIn, Tik Tok and Instagram should contain a disclaimer stating that the opinions expressed are strictly their own and not those of the Company, unless posting is in the course of business duties.

Employees may be required to remove internet postings which are deemed to be inappropriate or constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

The Company reserves the right to monitor, intercept and review, without further notice, employee activities using our IT resources and communications systems, including but not limited to social media postings and activities, to the extent reasonably required to ensure that our rules are being complied with and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of messages, communications, postings, log-ins, recordings and other uses of IT systems as well as keystroke capturing and other network monitoring technologies.

If you see content in social media that denigrates or poorly reflects the company, you should contact the Marketing Manager or HR Director/Manager. All employees are responsible for protecting the company's reputation.

If you are contacted for comments about the company to be published anywhere, including in social media, please direct your request to the Marketing Manager or HR Director/Manager..

If you see content on social media that disparages or reflects poorly on the Company, you should contact the Marketing Manager or HR Director/Manager. All employees are responsible for protecting the Company’s reputation.

If you are contacted for comments about the Company for publication anywhere, including in any social media outlet, direct the enquiry to Marketing Manager or HR Director/Manager.

6. Roles and Responsibilities

The IT Manager is responsible for overseeing all aspects of information security, including:

(a) monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.

The HR Director is responsible for

(a) creating and distributing security policies and procedures; and

Members of the I.T. team will:

(a) monitor and analyse security alerts and information and distribute to appropriate employees;

(b) administer user accounts and manage authentication;

(c) monitor and control all access to data; and

(d) ensure there is a process for engaging service providers including proper due diligence prior to engagement.

Violation of the standards, policies and procedures set out in this document by an employee will result in disciplinary action, up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will generally not be accepted as excuses for non-compliance.

7. Protection of Stored Data (Encryption)

Company data is confidential in nature. In some cases (e.g. Payroll, HR, Talent Acquisition & Development and Travel staff) employees may also handle sensitive personal data. For these reasons it is important that storage and handling of Company data meets a high level of security and encryption.

(a) Employees should store all Company data on the designated network drives rather than storing on local hard disks. In this way, the data is protected in the network backup system and these backup files are encrypted;

(b) Employees should not store personal data on company provided equipment.

(c) Electronic documents containing sensitive data will be stored as password protected files; and

(d) Hard copy documents containing sensitive data will be stored in locked cabinets.

(e) Employees shall only access confidential information if necessary to perform their function. Employees shall not under any circumstances download, copy or remove (or allow any other person to access, view, download, copy or remove) confidential information unless explicitly authorized to do so by Group Finance Director or HR Director.

8. Physical Security

Access to sensitive information should be physically restricted to prevent unauthorised individuals from obtaining sensitive data. In addition:

(a) Visitors to the office must always be accompanied by a staff member;

(b) All computers must have a password protected screensaver to prevent unauthorised use; and

(c) All network servers are secured in a dedicated computer room with access limited to the required staff necessary for operational requirements.

9. Protection of Data in transit

All personal data must be protected securely if it is to be transported physically or electronically.

All sensitive data or similar personal data must never be sent over the internet via unencrypted email, instant chat or any other end user technologies.

If there is a business justification to send personal data, it should be transferred via secure file transfer as an encrypted message.

10. Disposal of Stored Data

All data must be disposed of securely. Confidential shredding bins are provided throughout the offices and should be used for any documents containing personal data or information that is commercially, company, or personally sensitive.

11. Copyrights and Licence Agreements

Violations of copyright law expose the Company and the responsible individual(s) to civil penalties:

(a) liability for damages suffered by the copyright owner; and

(b) profits attributable to the copying, with potential fines for each illegal copy.

The Company will:

(a) maintain records of software licences owned by the Company; and

(b) on demand, scan company computers to verify that only authorised software is installed.

Employees must not:

(a) install, copy, or download software unless authorised by the Company to do so. Only software that is licensed to or owned by the Company is to be installed on the Company's computers; or

(b) download, upload or exchange (e.g. torrent) copyright material such as music, videos, games or any type of software or files on company equipment.

12. Firewalls and Network Security

The Company's information systems and data are protected.

(a) Firewalls are installed at each internet connection on the internal company network and disaster recovery facility. A router configuration table is maintained and includes a list of external IP addresses mapped to services, protocols and ports being used by the Company.

(b) The Company will separate wireless users to a dedicated Internet connection even when they are in the building as if they were coming in from the Internet.

(c) Disclosure of private IP addresses to external entities should only be made with prior authorisation from the IT Manager.

13. System and Passwords

All employees (including 3rd parties, contractors and vendors with access to the Company's computer systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

(a) All vendor default accounts and passwords for any new systems must be changed at the time of provisioning a new device or system on to the Company's network. All unnecessary services and user/system accounts will be disabled;

(b) All unnecessary default accounts must be removed or disabled before installing a system on the network;

(c) Security parameter settings must be set appropriately on system components;

(d) All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.) must be removed;

(e) All unnecessary services such as protocols and daemons will be disabled if not in use;

(f) All employees must use a password to access the company network or any other electronic resources;

(g) All user IDs for terminated staff will be deactivated immediately;

(h) Any network ID will be locked out if there are more than three unsuccessful attempts. Locked user accounts are deactivated until the account is released by the IT administrator;

(i) It is necessary to change passwords regularly.

(j) When new employees join the Company, the account will be set to prompt for a change of password on first login;

(k) System services and parameters will be configured to prevent the use of un-secure technologies like telnet and other remote login commands;

(l) The responsibility of selecting a password that is hard to guess falls to each staff member. A strong password will:

(i) be as long as possible (never shorter than 6 characters);

(ii) include mixed-case letters; and

(iii) include digits (numbers) and punctuation marks.

14. Anti-virus and Malware Protection

In order to avoid system downtime or loss of data, all Company computers will be configured to run the latest anti-virus software as approved by the IT Manager.

(a) Whichever system is in place will be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus software should have periodic scanning enabled for all the systems;

(b) The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits);

(c) All removable media should be scanned for viruses before being used;

(d) E-mail with attachments coming from suspicious or unknown sources should not be opened. Employees are responsible for reporting any suspicious emails or activity, including Phishing attempts. No one should forward any e-mail which is suspected of containing a virus;

(e) The Company will provide employees with cyber security training and also send out regular updates on cybersecurity news and events to encourage vigilance against cyber threats throughout the company. Employees must complete their Red Dot Cyber Security awareness training on time.

15. Patch/Update Management

All workstations, servers, software, system components, and mobile devices have up-to-date system security patches installed to protect the asset from known vulnerabilities.

Where possible, all systems and software should have automatic updates enabled for system patches released from their respective vendors.

16. **Access Management – New User Procedure**

Access to the Company's computer systems is controlled through a formal user registration process beginning with a notification as follows:

(a) Each employee is identified by a unique user ID so that employees can be linked to and made responsible for their actions. The Company will assign the user ID when creating the account;

(b) There is a standard level of access; other services can be accessed when specifically authorised by IT Director / HR Director and Management;

(c) The job function of staff members dictates the level of access to network services and applications;

(d) A request for service must be made with the IT service portal by the employee's line manager or HR . The request must state:

(i) the name of person making request;

(ii) job title of the newcomer(s) and workgroup;

(iii) start date;

(iv) Services required; and

(v) Computer hardware requirements.

17. **On Leaving**

All leavers must update their online profiles immediately upon the termination of their employment or contract with the Company such that the Company is not represented as being the leaver's current employer.

On the termination of your employment for whatever reason, you will be required to return to the Company, without delay, all files, correspondence, records, data, computer files, specifications, models, notes, formulations, lists, papers, reports and other documents and all copies thereof of whatever nature and other property belonging to the Company or relating to its business affairs or dealings which are in your possession or under your control.

18. **Security Access Control**

Access control systems are in place to protect the interests of all employees by providing a safe, secure and readily accessible environment in which to work. Employees will be provided with the access they need to carry out their responsibilities in an effective and efficient manner within the following guidelines:

(a) Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place;

(b) The allocation of privileged rights (e.g. local administrator, domain administrator, super-user, root access) will be restricted and controlled, and authorisation provided jointly by the system owner and IT Services;

(c) Access rights will be accorded following the principles of least privilege and need to know;

(d) Staff members should report instances of non-compliance to the IT Manager; and

(e) Access to confidential, restricted and protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.

19. **Wireless, Hotspotting and Mobile Device Management**

Wireless, hot-spotting, wi-fi, and mobile data affords valuable efficiencies for the Company's employees and beneficial business advantages, but increases the Company's exposure to potential security breaches. With this in mind:

(a) unauthorised installation of any wireless on the Company's computer network is prohibited;

(b) tests are performed continuously to ensure that no wireless access points are connected to the network;

(c) any devices which support wireless communication should have this feature disabled when the device is connected to the Company's network; and

(d) staff should not attempt to modify (or jailbreak) the mobile devices to circumvent the systems in place on their company owned equipment.