Shorcontrol Safety	Document Title	**Cyber-Security Policy**		
	Doc. Number	GEN-POL-012	Doc. Owner	General Manager
	Author	Angela Byrne	Revision	Rev. 02
	Reviewed by	Angela Byrne	Approved by	Fiona Spillane
	Next Review Date	26/07/2026	Approved Date	26/07/2025

1. Policy Statement

At Shorcontrol Safety we are committed to ensuring the confidentiality, integrity, and availability of our information assets. Management will demonstrate leadership and commitment to this by establishing, implementing, maintaining, and continually working to improve our information security management system, through the use of an external information technology support provider.

Shorcontrol Safety will establish, maintain, and review this information security policy so that it aligns with our objectives. This policy will be communicated to all relevant stakeholders.

2. Purpose

The purpose of this policy is to establish and maintain an effective approach to managing information security for Shorcontrol Safety.

3. Scope

The scope of this policy applies to all employees, contractors, third party users who have access to Shorcontrol Safety's information assets, including but not limited to information systems, networks, and data.

4. Definitions

Term	Definition
Cyber-security	The process of protecting information systems and networks from malicious attacks. Also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing.
Information security	The process of protecting the integrity and privacy of data, both in storage and in transit.

5. General Policy Guidelines

Types of cyber threats

The threats countered by cyber-security are mainly threefold:

- **Cybercrime:** this includes single actors or groups targeting systems for financial gain or to cause disruption.
- **Cyber-attack:** often include politically motivated information gathering.
- **Cyberterrorism:** is intended to undermine electronic systems to cause panic or fear.

Common methods used to threaten cyber-security include but are not limited to the following:

1. **Malware** means malicious software. One of the most common cyber threats, malware is software that a cybercriminal of hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment of legitimate looking download,

malware may be used by cyber criminals to make money or in politically motivated cyber-attacks. The following are different types of malwares:

- Virus: a self-replicating programme that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- Trojans: a type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading trojans onto their computer which can cause damage or collect data.
- Spyware: a programme that secretly records what a user does, so that cybercriminals can make use of this information, for example, spyware could capture credit card details.
- Ransomware: malware that looks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- Adware: advertising software which can be used to spread malware.
- Botnets: networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

2. **Structured Language Query injection** (SQL) is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to sensitive information contained in the database.
3. **Phishing** is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data or other personal information.
4. **Man in the middle attack** is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure network, an attacked could intercept data being passed from the victims' device and the network.
5. **Denial of service attack** is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organisation from carrying out vital functions.

5.1 Risk Management

- Regular risk assessments will be conducted to identify and assess information security risks.
- The results of the risk assessments will be documented and used to make informed decisions about risk treatment and mitigation.
- A risk treatment plan will be developed and implemented as required to address identified risks.
- The plan will include appropriate risk mitigation measures, controls, and monitoring activities.

5.2 Information security controls

- Shorcontrol Safety will implement a set of information security controls which will be selected and customised based on the results of the risk assessments and company requirements.
- Access to information assets will be controlled based on business and security requirements.
- Access rights will be granted, modified, or revoked in a timely manner, and access to sensitive information will be restricted to authorised persons.

5.3 Information security incident management

- All employees and contractors are responsible for reporting information security incidents promptly to the IT provider to respond to promptly.
- Incident reports will include details about the incident, impact, and any actions taken.
- Shorcontrol Safety will maintain an incident response plan that outlines the procedures for identifying, responding to, and recovering from information security incidents.
- The plan will be regularly reviewed, tested, and updated to ensure its effectiveness.

5.4 Communication and training

- Shorcontrol Safety will provide information security awareness and training for all our employees, contractors, and third-party users.
- Training will cover the company's information security policies, procedures, and best practices.
- Effective communication mechanisms will be established to ensure that relevant information regarding information security is disseminated to all stakeholders in a timely and secure manner.

5.5 Monitoring and Measurement

- Shorcontrol Safety will implement a monitoring process to detect and respond to information security events.
- Monitoring activities will include regular reviews of security controls, systems logs, and incident reports.
- Metrics may be implemented to assess the effectiveness of the information security management system.
- These measurements may be used to identify opportunities for improvement and demonstrate the company's commitment to information security.

5.6 Compliance

- Shorcontrol Safety will identify and monitor legal and regulatory requirements related to information security.
- The company will ensure that information security controls are in compliance with applicable laws and regulations.
- Periodic audits will be conducted to assess the compliance of the information security management system and the effectiveness of controls.
- Audit results will be documented, and corrective actions will be implemented as necessary.

5.7 Password protection

Password Creation

- Passwords must be at least 12 characters long.
- Must include uppercase, lowercase, numbers, and special characters.
- Avoid using dictionary words, personal information, or reused passwords.

Password Management

- Passwords must be changed every 90 days.
- Users must not reuse the last 5 passwords.
- Passwords must not be shared or written down.
- Use of password managers is encouraged for secure storage.

Multi-Factor Authentication (MFA)

- MFA is mandatory for access to:
    - Email systems
    - Remote access (VPN)
    - Cloud services
    - Administrative accounts

Account Lockout

- Accounts will be locked after 5 failed login attempts.
- Locked accounts must be reset by the IT department.

System Requirements

- All systems must enforce password complexity and expiration rules.
- Default passwords must be changed before deployment.

5.8 Tips to protect against cyberattacks

- Update your software and operating system.
- Use anti-virus software.
- Keep your software updated for the best level of protection.
- Use strong passwords: Ensure your passwords are not easily guessable.
- Do not open email attachments from unknown senders: These could be infected with malware.
- Do not click on links in emails from unknown senders or unfamiliar websites: This is a common way that malware is spread.
- Avoid using unsecure Wi-Fi networks in public places: Unsecure networks leave you vulnerable to man-in-the-middle attacks.

6. Responsibilities

Employee Title/Classification	Responsibility
Directors, Top Management & Senior Management	To ensure the necessary resources are available within the organisation for the implementation of this policy. To ensure the contents of this policy are implemented effectively. To investigate and act upon any breaches or violations which may arise or be reported from individuals citing behaviour related to this policy.
Employees/ Staff/ Instructors/ Sub-contractors	To adhere to the requirements set out in this policy. To report any breaches or violation of this policy to top/senior management for investigation and resolution.

7. Enforcement

Employee Title/Classification	Responsibility
General Manager	Has the discretion of determining the repercussion on the discovery of any member of staff, tutors, managers, visitors, or subcontractor's unacceptable behaviour related to this policy. Has the discretion of determining the repercussions on the discovery of a manager or assigned responsible personnel's failure to enforce or follow this policy or its procedures.
Managers and Heads of Departments	Has the discretion of determining the repercussions on the discovery of any subordinate or learner's unacceptable behaviour related to this policy.

8. Related Information and Documents

Document ID	Title
GEN-POL-007	Email, Internet & Social Media Use Policy
GEN-POL-010	Data Protection & Privacy Policy

GEN-POL-015	Careful Communications Policy

9. Policy Review

This policy shall be reviewed when:

- There is a change of General Manager at Shorcontrol Safety.
- There is a change in any of the related policies or procedures found in section 8. *'Related Information & Documentation'* of this document.
- As prescribed in Shorcontrol Safety's policy and procedure review schedule.
- As determined or requested by the General Manager at Shorcontrol Safety.

Revision Date	Author with Title	Description
07/12/2023	Angela Byrne, QHSM	Initial creation and release of policy.
09/10/2024	Angela Byrne, QHSM	Review – no changes.
26/07/2025	Angela Byrne, QHSM	Inclusion of password protection in section 5.