Cyber Security Policy

Statement

The risk of data theft, scams, and security breaches can have a detrimental impact on our systems, technology infrastructure, and reputation. As a result, we have created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose

The purpose of this policy is to (a) protect our data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for business and personal use, and (d) outline our disciplinary process for policy violations.

Scope

This policy applies to all our remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential data

We define "confidential data" as:

- Unreleased and classified financial information
- Customer, supplier, and shareholder information
- Customer leads and sales-related data
- Patents, business processes, and/or new technologies
- Your passwords, assignments, and personal information
- Our contracts and legal records

Device security

Business use

To ensure the security of all our devices and information, you are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters)
- Secure all relevant devices before leaving your desk
- Obtain authorisation from the office manager and/or inventory manager before removing devices from company premises
- Refrain from sharing private passwords with co-workers, personal acquaintances, senior personnel, and/or shareholders
- Regularly update devices with the latest security software

Personal use

We recognise that you may be required to use personal devices to access company systems. In these cases, you must report this information to management for record-keeping purposes. To ensure company systems are protected, you are required to:

- Keep all devices password-protected (minimum of 8 characters)
- Ensure all personal devices used to access company-related systems are password protected
- Install full-featured antivirus software
- Regularly upgrade antivirus software
- Lock all devices if left unattended
- Ensure all devices are protected at all times
- Always use secure and private networks

Email security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. We require all employees to:

- Verify the legitimacy of each email, including the email address and sender name
- Avoid opening suspicious emails, attachments, and clicking on links
- Look for any significant grammatical errors
- Avoid clickbait titles and links
- Contact the IT department regarding any suspicious emails

Transferring data

We recognise the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, all employees should:

- Refrain from transferring classified information to colleagues and outside parties
- Only transfer confidential data over our networks
- Obtain the necessary authorisation from senior management
- Check the recipient of the information and ensure they have the appropriate security measures in place
- Follow our data protection processes and confidentiality agreement
- Immediately alert the IT department of any breaches, malicious software, and / or scams

Disciplinary action.

Breach of this policy may lead to disciplinary action, up to and including termination.

Any disciplinary outcome will depend on the severity of the breach. Unintentional breaches only warrant a verbal warning, frequent breaches of the same nature may lead to a written

warning, and intentional breaches may lead to suspension and/or termination, depending on the case circumstances.

Policy Issue Date	Director Signature
23th April 2025