Cyber Security policy

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation.

This policy applies to all Jays employees, contractors, volunteers and anyone who has permanent or temporary access to the company’s systems and hardware.

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

Confidential Data.

Jays defines "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.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Device Security:

Company Use.

To ensure the security of all company-issued devices and information, employees are required to:

Keep all company-issued devices password-protected (minimum of 8 characters). This includes tablets, computers, and mobile devices.

We recognize the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

Refrain from transferring classified information to employees and outside parties.

Only transfer confidential data over secure networks.

Obtain the necessary authorization from senior management.

Verify the recipient of the information and ensure they have the appropriate security measures in place.

Adhere to data protection law and confidentiality agreement.

Version: Jays SC 1	Review Date: 03-01-2026
Reviewer: S GUMM	Approver: M.BEAVAN

Immediately alert the IT department regarding any breaches, malicious software, and/or scams.

Disciplinary Action.

Violation of this policy can lead to disciplinary action, up to and including termination. Jays disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

How to implement cyber security

Cyber security helps protect businesses from scams, breaches, and hackers that target confidential and unreleased information.

- Employees that have digital devices are to:
- Keep all passwords protected
- Ensure all antivirus software is kept up to date
- Not leave devices exposed or unattended
- Log into company accounts and systems using a secure and private network
- Avoid accessing internal systems from other peoples devices
- Do not lend company devices to other people
- Avoid transferring sensitive data (eg customer information, employee records) to other devices unless absolutely necessary
- Report any scams, privacy breaches and hacking attempts to the RTK IT team
- Secure devices before leaving your desk
- Laptops and other mobile devices should be kept secure at all times this include transfer from office to home

M.BEAVAN

Operations Director