

Cyber Security Policy

Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, The A1 Group has 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 The A1 Group's 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.

Scope

This policy applies to all of The A1 Group's 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

The A1 Group 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, The A1 Group employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 12 characters). A full password policy is also available.
- Secure all relevant devices before leaving their desk.
- Obtain authorisation from their manager before removing devices from company premises.
- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.

Personal Use

The A1 Group recognises that employees may be required to use personal devices to access company systems, only outlook emails are able to be access from non-company devices. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 12 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. Therefore, The A1 Group requires 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.

The A1 Group recognises 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 The A1 Group 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 A1 Group's data protection policy.
- Immediately alert the IT department of any breaches, malicious software, and/or scams

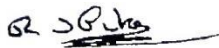
Disciplinary Action.

Violation of this policy can lead to disciplinary action, up to and including termination. A1Group's 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.

Revision

The Company will make all employees aware of this Company Policy.

Signed:



Date: 1/1/24

Russell Pike - **Managing Director A1 Group**

Next Review date 1st January 2025