CALLEN CONSTRUCTIONS

CYBER SECURITY

Introduction

This policy applies to all of Callen Constructions workers, permanent, and part-time employees, contractors, suppliers, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.
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, Callen Constructions has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

The purpose of this policy is to

a) protect Callen Constructions 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.
e) Facilitate a 'security aware' culture across the company & promote that Cyber Security is everyone's responsibility.

Confidential Data.

Callen Constructions 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, responsibilities, and personal information.
- Company contracts and legal records.

Password Requirements

- Ensure all personal devices used to access company-related systems are password protected (minimum of 8 characters).
- Passwords shall be changed every 6 weeks.
- Two-Factor Authentication should always be used where available.
- Passwords are not to be shared unless requested by senior management or director.
- Passwords should not be a term related to the company or location/item being used.
- Date of birth, pin numbers, phone numbers should not be used.
- Randomising passwords is best practice.

Device Security

Company Use.

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

- Keep all company-issued devices password-protected (minimum of 8 characters). This includes tablets, computers, and mobile devices.
- Passwords shall be changed every 6 weeks
- Two-Factor Authentication should always be used where available.
- Secure all relevant devices before leaving their desk.
- Obtain authorization from the Office Manager and/or Director 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.

Callen Constructions recognizes that employees may be required to use personal devices to access company systems. To ensure company systems are protected, all employees are required to:

- Ensure all personal devices used to access company-related systems are password protected (minimum of 8 characters).
- Passwords shall be changed every 6 weeks
- Two-Factor Authentication should always be used where available.
- 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.

If a Callen Constructions device, or a personal device containing Callen Construction systems is misplaced, the Office Manager is to be contacted immediately. The misplaced device will be unlinked and removed from all Callen Construction systems via the company portal and remotely wiped. Personal devices are to be remotely wiped where possible.

Callen Constructions does not permit the saving of critical data or files on personal devices, any files that are accessed from the mainframe/server and worked on must be saved back on the mainframe/server before the close of business each day so back up can be actioned. Contractors that have staff working remote to the office must write in a process for the backing up of files on those remote computer resources.

Email & SMS Security.
Protecting email & smart phone systems is a high priority as emails and texts can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, Callen Constructions requires all employees to:

- Verify the legitimacy of each email or text, including the email address or phone number and sender name.
  - When links or zipped files are sent from a known, verified sender, a verbal verification should be sought from the sender or a known contact within that company.
  - If an email or text requests to add or alter a customers, employees or suppliers financial, or membership details, a verbal verification must take place.
- Avoid opening suspicious emails. texts, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the Office Manager regarding any suspicious emails.

Transferring Data.
Callen Constructions recognizes 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 Callen Constructions 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 Callen Constructions data protection law and confidentiality agreement.
- Immediately alert the Management regarding any breaches, malicious software, and/or scams.

Disciplinary Action.
Violation of this policy can lead to disciplinary action, up to and including termination. Callen Constructions' 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.