Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches.

Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise our company’s reputation.

For this reason, we have implemented a number of security measures.

We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

**Password Requirements**

Manage passwords properly password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

* Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
* Remember passwords instead of writing them down.
* If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
* Exchange credentials only when absolutely necessary.
* When exchanging them in-person isn’t possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
* Change their passwords every two months.

Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

**Email Security Measures**

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

* Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
* Be suspicious of clickbait titles (e.g. offering prizes, advice.)
* Check email and names of people they received a message from to ensure they are legitimate.
* Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive

**Handling of Sensitive data**

Confidential/Sensitive data is secret and valuable. Common examples are:

* Unpublished financial information
* Data of customers/partners/vendors
* Patents, formulas or new technologies
* Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

**Transfer data securely** Transferring data introduces security risk. Employees must:

* Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask IT for help.
* Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
* Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
* Report scams, privacy breaches and hacking attempts.

Our IT specialist computer Wizard Darren need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our [IT Specialists/ Network Engineers] must investigate promptly, resolve the issue and send a companywide alert when necessary. Our Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

**Protect personal and company devices**

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company issued computer, tablet and cell phone secure. They can do this if they:

* Keep all devices password protected. Choose and upgrade a complete antivirus software.
* Ensure they do not leave their devices exposed or unattended. Install security updates of browsers and systems monthly or as soon as updates are available.
* Log into company accounts and systems through secure and private networks only.

We also advising our employees to avoid accessing internal systems and accounts from other people’s devices or lending their own devices to others.

**Social Media**

All parties identified in the scope of this policy are required to maintain the good reputation of Stagg Plumbing & Heating when using the Internet, email and social media. Any such use which brings Stagg Plumbing & Heating into disrepute may result in removal of internet, email and company social media access and disciplinary action may be taken against employees where necessary.

**Additional measures**

To reduce the likelihood of security breaches, we also instruct our employees to:

* Turn off their screens and lock their devices when leaving their desks.
* Report stolen or damaged equipment as soon as possible to IT.
* Change all account passwords at once when a device is stolen.
* Report a perceived threat or possible security weakness in company systems.
* Refrain from downloading suspicious, unauthorised or illegal software on their company equipment.
* Avoid accessing suspicious websites.

Take security seriously Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

In the event of an incident, first point of contact is Darren Coley (IT Wizard) who will take the lead putting into action the recovery procedures and any next steps.

Signed:



Managing Director December 2023