Entier Company Cyber Security Policy

1.0 POLICY BRIEF & PURPOSE

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

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

1.3 Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

1.4 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.

2.0 SCOPE

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

3.0 CONFIDENTIAL DATA

3.1 Confidential data is secret and valuable. Common examples are:

- Unpublished financial information;
- Data of customers/partners/vendors;
- Internal and external email communications
- Patents, formulas or new technologies;
- Customer lists (existing and prospective).

3.1.1 This list is not exhaustive, and employees should be vigilant about sharing any company related information or data.

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

4.0 PROTECT PERSONAL AND COMPANY DEVICES

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

- Keep all devices password protected.
- Ensure devices are not 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.
- Do not leave the device in vehicles overtly seen or overnight (this will also protect the device from harm as some devices do not do well in cold weather).

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

4.3 When new hires receive company-issued equipment they will already be configured with:

- Up to date antivirus software;
- A secure password;
- Locked down to prevent software installation without an administrator password;
- Rebooting machines periodically will also allow software updates and this is also healthy for computer, tablet and mobile phone and will allow the hardware to last longer;
- BitLocker to be enabled on all laptops to ensure they are encrypted. This prevents unauthorised action in the event of theft or loss of a company device.

4.4 Everyone should follow instructions to protect their devices and refer to our IT Partner, G5 Technologies, if they have any questions.

5.0 KEEP E-MAILS SAFE

5.1 E-Mails 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 address 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 number of exclamation marks.)
- Employees should not use their company email to sign up for personal online subscriptions.
- Entier emails should not be used for personal reasons and should remain professional at all times.

5.2 If an employee is not sure that an e-mail they received is safe, they should send to hseq@entier-services.com

6.0 MANAGE PASSWORDS PROPERLY

6.1 Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not 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.) Using a phrase for a password holds less risk, however numbers and symbols should still be used
- 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.
- Avoid using the same password in multiple locations.
- Exchange credentials only when absolutely necessary. When exchanging them in-person is not possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every quarter or as soon as they suspect someone else knows their password.

7.0 TRANSFER DATA SECURELY

7.1 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 our IT Helpdesk 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
- Data should not be transferred to pen drives or other removable storage unless authorised by CEO or CCO.

7.2 Our IT helpdesk 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 IT helpdesk must investigate promptly, resolve the issue and send a companywide alert when necessary.

7.3 Our IT Partner, G5 Technologies, and induction trainers 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.

8.0 ADDITIONAL MEASURES

8.1 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 their line manager.
- 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.
- Avoid accessing company systems on public Wi-Fi networks e.g. Wi-Fi in a café

8.2 We also expect our employees to comply with our social media and internet usage policy. Company provided devices and networks should only be used for work and you should avoid:

- Accessing social media.
- Opening personal emails as malicious content can get through public email services easier than the company provided email service.
- Online shopping or gambling.
- Accessing unsecure websites (look for the padlock icon in the address bar).
- Accessing pornographic or other indecent sites.

8.3 Employees are responsible for ensuring there are sufficient security measures in place on personal devices they use to access company resources such as:

- A secure password.
- An auto lock policy to secure the device when it has been left untouched for a period of time.
- Up to date antivirus software.

- If devices are lost or stolen this should be reported to the IT Helpdesk as soon as possible.

8.4 If someone has been a victim of online crime and accounts have been hacked DO NOT use the personal device to access the company network until such times as the threat has been completely eradicated and the device is secure. If users have been a victim of online crime they should immediately change passwords on all personal and company accounts from another device.

8.5 Home broadband routers should have a password to access and provide an extra layer of security when using a device at home.

8.6 Our IT Partner, G5 Technologies, will:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.
- Advise on upgrades to firewall, antivirus software and other security products.

8.7 Our company will have all physical and digital shields to protect information.

9.0 REMOTE EMPLOYEES

9.1 Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

9.2 We encourage them to seek advice from G5 Technologies.

10.0 DISCIPLINARY ACTION

10.1 Where an employee's conduct and actions have been identified as having caused a serious breach in security or where their conduct or actions could have had the potential to cause a serious breach in security then the employees may be subject to summary dismissal for gross misconduct under the company disciplinary policy.

10.2 Any employee who feels that any of their colleagues are not following company guidelines then they should report to line manager.

11.0 TAKE SECURITY SERIOUSLY

11.1 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.

11.2 Entier will strive to keep employees informed of current threats that are evident within the cybercrime space through alerts etc. However, due to cyber criminality changing daily these updates will not be exhaustive therefore, staff must remain alert when conducting daily business.

11.3 Computer devices provided by Entier remain company property and Entier maintain the right to forensically analyse if deemed necessary, therefore personal information should not be stored.