St. Pauly Textile, Inc.

St. Pauly Textile Cyber Security Policy

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

This policy applies to all our employees, contractors and anyone who has permanent or temporary access to our systems and hardware. Remote employees must follow all data encryption, protection standards and settings, and ensure their private network is secure.

Confidential Data

Confidential data is secret and valuable. All employees are obliged to protect this data. Confidential data includes, but is not limited to:

- Financial information
- Data of employees, customers, partners, and vendors
- Customer lists (existing and prospective)

Protect Personal and Company Devices

When employees use their digital devices to access company emails or accounts, they introduce a potential security risk to company data. Employees should keep both their personal and company-issued computer, tablet and/or cell phone secure. Ways to secure devices include, but are not limited to:

- Keeping all devices password protected
- Installing antivirus software
- Ensuring devices are not exposed or left unattended
- Installing security updates of browsers and systems as they become available
- Log into company accounts and systems using secure and private networks

Keep Emails Safe

Emails often host scams and malicious software. 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
- Be suspicious of clickbait titles (ie. Offering prizes, advice, etc.)
- Check email and names of people you receive messages from to ensure they are legitimate
- Look for inconsistencies or give-aways (ie. Grammar mistakes, capital letter, excessive number of exclamation marks, etc.)

If an employee isn't sure that an email is safe, they should delete it without opening.

St. Pauly Textile, Inc.

St. Pauly Textile Cyber Security Policy

Manage Passwords Properly

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

- Choose passwords that are strong and avoid information that can be easily guessed
- Remember passwords instead of writing them down. If employees need to write their passwords down, 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. Do not send passwords to people you do not know or trust
- Change passwords regularly

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
- 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, unauthorized or illegal software on company equipment
- Avoid accessing suspicious websites

I have read and understand the guidelines above. I will follow all guidelines and implement any changes that are necessary to be compliant with these guidelines.

____ ______________________________

Name Date