A logo for a company

Description automatically generatedIT Cyber Training Policy

This policy is informed by [NIST.SP.800-53r5.](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)

V.1.4

Updated 03 October 2023

Written by Jackson Duong

**Business Level Information**

Consider these suggestions for helping to improve your business’s cybersecurity awareness:

All new employees should complete cyber security training before finishing their onboarding.

Training material should cover these categories:

* **Unauthorized Personnel**- Understand who can access restricted areas and other essential needs for regular business operations.
* **Social Engineering**- The process of gaining sensitive information and data by using multiple techniques to disrupt or cause harm to the business.
* **Phishing** (a form of social engineering)- Where an attacker tries to impersonate a reputable entity, usually via email, to reveal important information about the victim. Management can send fake phishing attempts to their employees periodically and should have a plan of action when their employees suspect a potential phishing scam.
* **Insider Threat**- The potential harm that employees can intentionally or unintentionally bring upon the business.
* **Password Requirements**- Proper password use can go a long way to turning significantly higher-risk employees into minimal-risk employees. It will help protect the company by understanding the do’s and do nots when creating a password. Consider training all employees on proper password use and selection. It is strongly recommended that businesses implement a password manager such as Bitwarden.
* **Securing Confidential Documents**- Define what constitutes confidential information for your business and how to secure it properly.

Current employees should conduct cyber security training refreshers monthly to reinforce the skills learned.

Leaders can conduct training via presentations, online courses, one-on-one, or other means.

Training should be documented for future reference of all employees within the company.

**Background**

Cyber training aims to teach employees the skills to perform their jobs more securely. Management or a designated trainer should conduct training so employees are aware of known threats to secure company assets. All company personnel should get training to understand the steps needed to prevent ongoing security threats before they occur.

**Objective**

This policy aims to define the company's rules regarding cybersecurity training.

**Scope**

The scope of this policy applies to all company personnel and has guidelines to help secure essential assets. This policy aims to protect against known threats and help navigate future cybersecurity concerns.

**Policy**

All employees should complete all the necessary cyber security training.

Topics include but are not limited to:

* **Unauthorized Personnel**- Employees will interact with unknown personnel and escort them to designated safe areas of operation. Employees will report these incidents to management.
* **Insider Threat**- Employees will take the necessary steps to report potential threats from within the company to management.
* **Password Requirements**- Employee passwords will contain a minimum of 16 characters that they will never share with anyone else. All passwords will be stored in a password manager (Bitwarden) and changed only when the account has been potentially compromised.
* **Securing Confidential Documents**- Employees will dispose of all confidential documents properly and lock them up when not in use.
* **Social Engineering** – Employees are actively engaged in training to understand the ways a hacker will gain information to harm the business. This training will cover the different methods used to collect sensitive information, usually by manipulation. All employees will use the knowledge gained to address social engineering attempts appropriately.

**Social Engineering Specifics**

* **Phishing**- Employees will never open links sent to the user, reply to unknown email addresses, or open attachments. They are mindful of the emails they receive and the information they send out.
* **Quid Pro Quo**- "This for that." Employees will never exchange/trade/sell sensitive information to anybody for personal gain. They will report those incidents immediately after the event has occurred.
* **Tailgating**- Employees are aware of their surroundings and will never prop or hold locked doors open at any time for anybody, even if they "know" the person has access.
* **Social Media**- Employees should not share any business information or details online without specific permission from management. Avoid social media applications during working hours and do not link a company email address to social media accounts.

Employees should complete the cyber training requirements as the final steps in their onboarding process.

Employees need to keep track of their completed training.

Current employees must review cybersecurity training monthly to ensure they are up-to-date with new security threats.

**\*All company personnel are to report any suspicious activity to management. \***

Employee Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Trainer/Manager Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Current Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_