A logo for a company

Description automatically generatedIT Email Policy

This policy is informed by [NIST.SP.800-177r1.](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf)

V.1.4

Updated 17 October 2023

Written by Jackson Duong

**Business Level Information**

Consider these suggestions to improve your business’s email security:

Have a Domain Name server (DNS) installed and adjust your privacy and security settings to prevent attacks such as:

DNS tunneling- The attacker tries to compromise hardware by sending a request through the DNS with a fake domain name attached with malware to try and pass through the firewall and infect its target.

DNS amplification attacks, also referred to as distributed denial of service (DDoS) attack- A process where the attacker overloads the DNS with unwanted requests to overwhelm the server from completing legitimate ones.

DNS hijacking- The hacker tries to intercept queries sent to the victim's DNS server or send the request directly to the attacker's DNS server.

Add security that encrypts email transmissions with SMTP (Simple Mail Transfer Protocol).

Use email spam filters.

Train all company personnel to identify phishing attempts and have ways for employees to report those incidents.

Management should send out emails in attempts that their employees spot and report the phishing attempt.

Constantly update software to the latest version.

Use multi-factor authentication and password managers such as Bitwarden.

Management must delete email accounts immediately when an employee has been terminated from the company.

**Background**

Emails are used to transfer information across the web with little effort. Electronic mail is a tool that can be effective when used appropriately. There are inappropriate uses with all tools, and we want to help our employees understand the security risks associated with using their email.

**Objective**

This policy aims to define the company's rules regarding the appropriate use of emails.

**Scope**

The scope of this policy applies to all company personnel and has guidelines to help secure network security concerning emails. This policy aims to protect against known threats and help recognize, avoid, and report email-based attacks.

**Policy**

Employees are responsible for creating user password that meets the company's criteria when setting up their email account.

Employees will never share their passwords and use Bitwarden (password manager) for added security.

Employees will sign up for 2FA to verify their company email login.

Employees will reset their password if they think their account has been compromised.

Employees understand phishing (hackers try to impersonate a reputable entity in hopes of attaining personal information about the victim) and will report all incidents to management when suspected of any attempts.

Employees will never click any links or attachments sent to them by anyone unless management approves.

Employees will not sign up to third-party websites and only use company email related to work.

Employees will log out of their accounts after each work day or any inactivity when they are away.

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

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

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

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