# Cybersecurity for Humans

## Standard Operating Procedure (SOP) for Secure Use of Company Systems

**Version 1.1 | September 2025 | Prepared by Tiffany Smith**

[Maintained by IT Security Team]

# Purpose

This document is intended to enable all personnel to protect company systems and data by following the outlined security practices. This document addresses passwords, email safety, and data storage, as well as reporting suspicious activity.

# Scope

The procedures outlined in this document apply to all company personnel using company systems including, but not limited to:

- All employees, contractors, and interns.
- All company-issued devices (laptops, desktops, phones, tablets).
- All access to company networks, cloud platforms, and applications.

**Note:** This SOP does not cover advanced security operations, penetration testing, or IT administrative procedures.

# Roles & Responsibilities

- **Employees & Contractors:** Follow this **SOP** daily and report suspicious activity.
- **Managers:** Reinforce secure practices and ensure teams comply with company policy.
- **IT/Security Team:** Provide tools and support to maintain secure operations.

# Standard Procedures

### 1. Passwords & Authentication

- Use unique passwords (minimum 12 characters).
- Enable multi-factor authentication (MFA) wherever available.

- Never share your password with anyone, including coworkers.
- Do not reuse personal passwords for company accounts.

**2. Email & Phishing Safety**

- Verify the sender before opening attachments or clicking links.
- Report suspicious emails to IT using the “Report Phish” tool.
- Never provide login credentials or sensitive data over email.

**3. Data Storage & Sharing**

- Store company files only on approved drives (cloud or network).
- Do not save work files on personal devices or external USBs. This can expose company data to unauthorized access.
- Share data through approved company platforms (e.g., Teams, Slack, SharePoint) only.

**4. Device Security**

- Lock your screen when away from your workstation.
- Install updates when prompted — do not delay.
- Report lost or stolen devices to IT immediately.

**5. Reporting Incidents**

- If you suspect **malware**, **phishing**, or **data loss**:
    a. Disconnect from the internet.
    b. Contact IT/security immediately.
    c. Do not attempt to troubleshoot on your own. Report any incidents immediately to IT so they can contain the issue.

## Accessibility & Compliance

- This **SOP** is written in plain language and formatted for screen reader compatibility.
- Print and PDF versions are available through office coordinators.
- Key terms are **bolded** for quick scanning, and numbered steps follow a logical order.
- Follows NIST Cybersecurity Framework guidelines where applicable.

## Glossary

- **SOP:** Standard Operating Procedure.
- **MFA:** Multi-Factor Authentication. Extra security layer requiring a code or device in addition to your password.
- **Incident:** Any event that threatens the confidentiality, integrity, or security of company systems.
- **Phishing:** A fraudulent attempt (usually via email) to trick someone into giving away sensitive information.
- **Malware:** Software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
- **Data Loss:** The accidental or unintentional deletion or corruption of data from electronic devices or systems.

## References & Related Docs

- Company Acceptable Use Policy
- Employee Handbook
- NIST Cybersecurity Framework (2024 edition)

# Revision History

- v1.0 (August 2025) – Initial release.
- V.1.1 (September 2025) - Revised for clarity