Lassine Guindo

Lethia Jackson

CTEC450

February 18, 2025

Security Guidelines Document

1. Introduction

At this organization, maintaining strong software security is essential to protecting our company's data, customers, and reputation. Cyber threats such as phishing, malware, and unauthorized access can lead to **financial losses, data breaches, and legal consequences**. This document outlines the key security guidelines all employees should follow to ensure a safe and secure working environment.

---

2. General Security Guidelines (For All Employees)

Password Security

✔ Use **strong passwords** (at least 12 characters, mix of letters, numbers, and symbols).
✔ Never reuse passwords across multiple accounts.
✔ Enable **Multi-Factor Authentication (MFA)** for all work-related accounts.
✔ Store passwords securely using a **password manager**, not in notes or emails.

Example of a strong password: T8&zB!9pR3vQ

Email Security

✔ Be cautious of **unexpected emails** requesting login credentials or payment details.

✔ Verify the sender before clicking on links or downloading attachments.
✔ Look for **warning signs of phishing**, such as: Urgent requests (“Your account will be locked!”).

- Misspelled email addresses or fake domains (support@companny.com).
  ✔ If unsure, **report suspicious emails** to the IT team.

Device Security

✔ Keep all company devices **updated with the latest security patches**.
✔ Install and maintain **antivirus software**.
✔ Lock your screen when stepping away from your device.
✔ Do not install unauthorized software or apps on company devices.

Data Protection

✔ Store sensitive data only in **approved, secure locations** (e.g., encrypted drives, cloud storage).
✔ Never share customer or internal company data via **personal email or messaging apps**.
✔ Use **encryption** when handling confidential information.
✔ Dispose of confidential documents securely (shredding for paper, deletion for digital files).

Incident Reporting

✔ If you notice **suspicious activity**, **report it immediately** to IT at **[IT Helpdesk Email/Phone]**.
✔ Report incidents such as:

- Phishing attempts
- Unauthorized access to company data

- Lost or stolen devices
  ✔ The sooner an issue is reported, the **faster IT can prevent damage**.

---

3. Technical Security Guidelines (For Developers & IT Teams)

Secure Coding Practices

✔ Validate all **user input** to prevent attacks like **SQL injection and Cross-Site Scripting (XSS)**.
✔ Never store **hard coded credentials** (e.g., API keys, passwords) in source code.
✔ Follow **least privilege principles** – limit user permissions to only necessary data access.
✔ Implement proper **error handling** to avoid exposing system details to attackers.

Vulnerability Testing

✔ Regularly perform **security testing** using tools like **OWASP ZAP, Burp Suite, or static code analysis tools**.
✔ Conduct **penetration tests** before deploying major updates.
✔ Monitor applications for **suspicious activity and logs** to detect potential breaches.

Patch Management

✔ Always **update software and libraries** to fix security vulnerabilities.
✔ Automate **patch deployment** where possible to reduce delays.
✔ Remove **outdated or unsupported software** that may pose a security risk.

Data Encryption

✔ Use **SSL/TLS encryption** for all sensitive data transmissions.
✔ Encrypt **databases, backups, and cloud storage** with strong encryption algorithms (e.g., AES-256).
✔ Do not store **unencrypted sensitive information** on local machines.

---

4. Remote Work Security (If Applicable)

Securing Home Networks

✔ Use **strong Wi-Fi passwords** and enable **WPA3 encryption** on home routers.
✔ Disable **default admin credentials** on home networking devices.

Using VPNs for Secure Access

✔ Always connect to the **company VPN** when accessing internal systems remotely.
✔ Do not use **public Wi-Fi** (e.g., coffee shops, airports) for work without a **VPN**.

Handling Company Data Remotely

✔ Store work files on **company-approved cloud services**, not personal devices.
✔ Lock devices when unattended and **enable remote wipe features** for security.
✔ Avoid discussing sensitive company matters in **public locations**.

---

5. Summary

Following these security guidelines helps protect company data, employees, and customers from cyber threats. Security is a shared responsibility, and every employee plays a role in safeguarding our systems.

For any security concerns, contact **[IT Security Team Email/Phone]**.