Kerin Quintero

Ctech 450

Dr. Jackson

2/23/25

### **Security Guidelines Document**

Security is essential to our company’s success because it protects our important information, maintains our reputation, and keeps our operations running smoothly. In today's digital world, threats are constantly changing, and every employee plays a vital role in keeping our systems secure. By following clear security policies, we reduce risks, protect customer data, and ensure our systems can withstand potential attacks.

All employees must use strong password security. This means creating strong, unique passwords for each account and using multi-factor authentication when possible. For example, instead of a simple password like “password123,” you should choose a mix of letters, numbers, and symbols that is much harder to guess. Employees must also be cautious with emails, as phishing attempts often mimic legitimate messages. Always check sender addresses carefully and report any suspicious emails to the IT department immediately. In addition, every device used for work should have the latest operating system updates, security patches, and antivirus software installed. Protecting sensitive customer and company information also means using encryption for storing and transmitting data and following secure storage practices. Finally, any security incidents or unusual activities should be reported to IT immediately so they can be dealt with quickly.

Developers and IT teams have extra responsibilities for technical security. They need to use secure coding practices, which include validating user inputs, avoiding hardcoded credentials, and following industry standards to prevent issues like SQL injection and cross-site scripting. Regular vulnerability testing using tools like OWASP ZAP is essential to find and fix weaknesses before attackers can exploit them. Keeping software, systems, and libraries up-to-date through patch management is also critical. For example, if a new security flaw is discovered, the necessary patches must be applied immediately. Moreover, all sensitive data transfers should use strong encryption methods like SSL/TLS to keep the information confidential, even if it is intercepted.

Remote work is increasingly common, so remote employees must follow specific security guidelines. When working from home or another location, secure your network by changing your router's default settings, using strong Wi-Fi passwords, and enabling encryption. Always use a virtual private network when accessing company resources, as it creates a secure, encrypted connection. Remote employees should also store sensitive files only on company-approved devices and use encrypted storage solutions. For example, avoid using public Wi-Fi and connect through a VPN to lower the risk of data interception by hackers.

By following these guidelines, every employee helps build a secure and resilient work environment. Whether through strong password practices, secure coding, or using VPNs for remote work, everyone contributes to defending our company against cyber threats. These security practices not only protect our digital assets and customer information but also uphold our reputation as a trusted and responsible organization. Staying alert and adhering to these procedures will ensure we continue to operate safely and effectively, even as new threats emerge.