**Cyber Best Practices   
Project**  
  
*Created by: Harsh Patel*

*Date: January 31, 2025*

**Introduction**

As the Cyber Security Manager, it is my responsibility to ensure the safety and security of the company’s digital infrastructure. This report outlines fundamental security practices that must be implemented to protect employees and sensitive company information from cyber threats. The recommendations align with industry standards and best practices.

**Security Measures and Their Implementation**

1. **Strong Passwords**

* **Why?** Weak passwords are a primary attack vector for cybercriminals, leading to unauthorized access.
* **Implementation:**
  + Require passwords to be at least 12-16 characters long.
  + Include uppercase and lowercase letters, numbers, and special characters.
  + Implement password blacklisting to prevent commonly used passwords.
  + Educate employees on password security best practices.
  + Utilize enterprise-grade password managers to store credentials securely.

1. **Password Expiration Policy**

* **Why?** Frequent password changes mitigate risks associated with credential leaks.
* **Implementation:**
  + Enforce a 90-day password expiration policy.
  + Prevent password reuse through history tracking.
  + Implement just-in-time (JIT) access for highly sensitive systems.
  + Monitor for compromised credentials using breach detection tools.

1. **Multi-Factor Authentication (MFA)**

* **Why?** MFA adds an additional layer of security beyond passwords, reducing the likelihood of unauthorized access.
* **Implementation:**
  + Require MFA for all company accounts, especially for remote access.
  + Prioritize authenticator apps (e.g., Microsoft Authenticator, Google Authenticator) over SMS-based MFA.
  + Enforce biometric authentication where possible (e.g., fingerprint or facial recognition).
  + Implement adaptive MFA that adjusts security requirements based on user behavior and location.

1. **Secure Email with Personal Certificates**

* **Why?** Email is a common attack vector for phishing and business email compromise (BEC) attacks.
* **Implementation:**
  + Deploy Secure/Multipurpose Internet Mail Extensions (S/MIME) for email encryption and digital signatures.
  + Implement Domain-based Message Authentication, Reporting & Conformance (DMARC) alongside SPF and DKIM.
  + Conduct periodic phishing simulations and employee awareness training.
  + Monitor email traffic for anomalous behavior using AI-based threat detection tools.

1. **VPN IPSec for Laptops**

* **Why?** VPNs secure remote connections and prevent data interception over public networks.
* **Implementation:**
  + Enforce the use of IPSec VPN for remote employees and traveling executives.
  + Implement always-on VPN policies to ensure encrypted communication at all times.
  + Restrict access based on user roles and device compliance.
  + Regularly audit VPN logs and analyze user activity for anomalies.

1. **Encrypted Hard Drives and Flash Disks**

* **Why?** Data encryption ensures that sensitive information remains secure even if devices are lost or stolen.
* **Implementation:**
  + Mandate full-disk encryption using BitLocker (Windows) and FileVault (macOS).
  + Require hardware-encrypted USB drives for transferring sensitive data.
  + Enable remote wipe capabilities through Mobile Device Management (MDM) solutions.
  + Implement strict policies for removable media usage to prevent data leaks.

**Cybersecurity Policy Review and Employee Awareness**

As part of the cybersecurity policy review, the company must establish:

* **Encryption Standards:**
  + AES-256 encryption for all stored data, including laptops, servers, and USB drives.
  + TLS 1.3 for secure email communication and web traffic.
* **Access Control Policies:**
  + Role-based access control to minimize insider threats.
  + Just-in-time access for privileged accounts.
* **Employee Security Awareness Programs:**
  + Regular cybersecurity training covering phishing threats, password hygiene, and data protection.
  + Simulated phishing exercises to improve user awareness and incident response.

**Conclusion**

Implementing these fundamental cybersecurity measures significantly strengthens the company’s security posture. By enforcing strong authentication, encryption, and secure email protocols, we can effectively mitigate cyber risks and protect both employees and company data from evolving threats.

***References***

Sadadow. (n.d.). *Security hub - Security*. Microsoft Learn. <https://learn.microsoft.com/en-us/security/>

Zbrog, B. M. (2024b, March 14). *A guide to digital forensics and cybersecurity tools*. Forensics Colleges. <https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>

*CIS Critical Security Controls*. (n.d.). CIS. <https://www.cisecurity.org/controls>

*Cybersecurity Framework | NIST*. (2025, January 14). NIST. <https://www.nist.gov/cyberframework>

Masas, R. (2023, December 20). *What is Information Security | Policy, Principles & Threats | Imperva*. Learning Center. <https://www.imperva.com/learn/data-security/information-security-infosec/#:~:text=of%20Digital%20Transformation.-,What%20are%20the%203%20Principles%20of%20Information%20Security%3F,are%20called%20the%20CIA%20Triad>.