Lighthouse Labs Best Cybersecurity Practices

Violet Figueroa

Executive Summary
Strong Passwords: Building Your First Defense
Password Expiration Policy: A Strategic Approach
Multi-Factor Authentication: Beyond Password Protection
Secure Email with Personal Certificates
VPN IPSec on Laptops: Securing Remote Connections
Encrypted Hard Drives / Flash Disks: Protecting Mobile Data
Implementation Strategy
Phase 1 (Immediate - 30 days)
Phase 2 (31-90 days)
Phase 3 (91-180 days)
Conclusion
References

Executive Summary

In today's rapidly evolving threat landscape, organizations face increasingly sophisticated cyber attacks targeting both information assets and personnel. As the newly appointed Cybersecurity Manager, I have identified six critical security measures that form the foundation of a robust security posture: strong passwords, strategic password expiration protocols, multi-factor authentication, secure email certificates, VPN IPSec for remote connectivity, and encrypted storage for portable devices. Implementing these measures will create multiple layers of defense against common attack vectors while balancing security requirements with usability considerations.

Strong Passwords: Building Your First Defense

Strong passwords remain the foundation of digital security, serving as the primary barrier against unauthorized access to sensitive company information, financial data, and operational systems. Despite advances in attack methodologies, password-based authentication continues to be the most widely deployed security control across organizations (Whitman & Mattord, 2017).

The importance of strong passwords cannot be overstated. Data breaches frequently begin with compromised credentials, with weak passwords creating an easily exploitable vulnerability. Strong passwords help protect against unauthorized access to personal accounts, financial information, emails, and sensitive business data. They create a formidable barrier against attackers attempting to breach accounts through brute force attacks or other password-cracking methods.

Based on current NIST guidelines, our password policy should require passwords to be a minimum of 8 characters (though 15 characters is recommended for optimal security), with support for all ASCII characters, spaces, and Unicode characters. NIST specifically recommends against imposing composition rules that require mixtures of character types, as these often lead to predictable substitution patterns (National Cybersecurity Alliance, 2025).

Password Expiration Policy: A Strategic Approach

Password expiration policies, once ubiquitous in security frameworks, have undergone significant reconsideration in recent years. Understanding the evolution and current best practices of these policies is essential for developing an effective approach for our organization.

The traditional 90-day password reset standard originated from the time needed to crack hashed passwords through brute-force attacks. Organizations using Active Directory typically store passwords as cryptographic hashes, and attackers must use cracking methods that test possible passwords by running them through the hashing algorithm.

While some recent guidelines have questioned the value of regular password expiration, research indicates that "never expire" policies create extended opportunities for attackers. A concerning study by Enzoic revealed that 83% of compromised passwords satisfied standard length and complexity requirements, indicating that complexity alone is insufficient protection (Enzoic, 2024).

A balanced approach to password expiration should consider risk levels and access privileges. High-risk accounts with administrative access should maintain shorter expiration periods, while standard user accounts might have longer intervals. This strategy must be paired with prompt password resets following security incidents and continuous monitoring for compromised credentials.

Multi-Factor Authentication: Beyond Password Protection

Multi-Factor Authentication (MFA) provides an essential additional layer of security beyond passwords, requiring users to verify their identity through multiple verification methods. By combining something users know (password), something they have (device), or something they are (biometric), MFA significantly reduces the risk of unauthorized access even when credentials are compromised (SuperTokens, 2024).

The implementation of MFA has become increasingly critical as sophisticated threat actors continue to compromise traditional password-only systems. MFA requires attackers to overcome multiple security layers, dramatically increasing the difficulty of unauthorized access. This approach addresses the fundamental limitations of passwords while maintaining a user-friendly authentication process.

Our MFA strategy should prioritize privileged accounts and systems containing sensitive information while gradually expanding to all users. The selection of appropriate authentication factors should be based on risk profiles and usability considerations. Additionally, implementing time limitations on authentication requests and educating users about MFA fatigue attacks will enhance our defensive posture.

Secure Email with Personal Certificates

Email remains a critical business communication tool and a primary attack vector for threat actors. Implementing secure email with personal certificates addresses two essential security requirements: authentication of sender identity and protection of message content through encryption.

Secure Email certificates enable users to digitally sign and encrypt their emails, providing assurance that messages truly originate from the claimed sender while protecting sensitive content from interception during transmission. This technology is particularly valuable for communications containing confidential information, financial data, or personally identifiable information.

When implementing Secure Email certificates, organizations must select appropriate certificate profiles based on security and operational requirements. DigiCert offers Secure Email certificates for individuals, businesses, and organizations, each with specific validation processes (DigiCert, 2025).

VPN IPSec on Laptops: Securing Remote Connections

The expansion of remote and hybrid work models has dramatically increased the importance of securing connections between employee devices and corporate resources. VPN technologies using Internet Protocol Security (IPSec) provide robust protection for these connections, creating encrypted tunnels for data transmission regardless of the underlying network infrastructure.

IPSec functions at the IP layer (level 3) of the OSI hierarchy, allowing encryption to be applied across an entire network rather than just individual applications (NordVPN, 2025). This comprehensive approach creates a secure environment for all traffic between remote devices and corporate resources without requiring application-specific modifications.

For optimal security, our IPSec VPN implementation should use current recommended encryption algorithms, including Advanced Encryption Standard (AES) in Galois / Counter Mode (GCM) with 128-bit, 192-bit, or 256-bit keys. Key exchange should utilize strong Elliptic-Curve Diffie-Hellman groups, preferably 256-bit, 384-bit, or 521-bit Random ECP Groups.

Encrypted Hard Drives / Flash Disks: Protecting Mobile Data

Portable storage devices represent a significant security challenge for organizations, as they can easily be lost or stolen while containing sensitive information. Encryption of these devices is critical to protecting data even when physical security is compromised.

Two primary encryption methods exist for protecting data on storage devices:

1. Full Disk Encryption (FDE): Encrypts every sector of the drive, including all file content, metadata, file system information, and directory structure. This approach provides comprehensive protection for "data at rest" at a level close to the hardware.
2. File Level Encryption (FLE): Encrypts specific files or folders based on policy settings, providing granular control over which data receives encryption protection.

Industry best practices recommend implementing both approaches for maximum security. FDE provides baseline protection for all data, while FLE enables policy-based security for particularly sensitive information. DataLocker's encrypted storage solutions provide AES 256-bit encryption, protecting sensitive data from unauthorized access across all manufacturing systems (DataLocker, 2024).

Implementation Strategy

To maximize security benefits while minimizing operational disruption, I recommend a phased implementation approach based on industry best practices (MITRE, 2024):

Phase 1 (Immediate - 30 days)

- Strong password policy implementation
- MFA deployment for administrative and privileged accounts
- Initial education and awareness training

Phase 2 (31-90 days)

- Password expiration policy implementation
- Full Disk Encryption on executive and high-risk laptops
- VPN IPSec deployment for remote workers

Phase 3 (91-180 days)

- Secure Email certificates for sensitive departments
- Encryption of all remaining company laptops and portable devices
- Comprehensive security training program

Conclusion

The six security measures outlined in this report represent the foundation of a robust cybersecurity strategy for our organization. By implementing strong passwords, strategic password expiration policies, multi-factor authentication, secure email certificates, VPN IPSec, and encrypted storage devices, we can significantly reduce our exposure to common attack vectors while protecting our most sensitive information assets.

These measures balance security requirements with usability considerations, ensuring our employees can work efficiently while following secure practices. They also establish a strong baseline upon which we can build more advanced security capabilities as our security program matures.

With leadership support and appropriate resource allocation, we can complete full implementation within six months, significantly enhancing our security posture and demonstrating our commitment to protecting both company information and employee data.

References

- DataLocker. (2024, December 24). Leading USB Security Solutions \& Management. https://datalocker.com
- DigiCert. (2025, February 6). Order your Secure Email for Individual certificate. DigiCert Docs. https://docs.digicert.com/en/certcentral/manage-certificates/client-certificates-guide/secure-email-certificates/order-your-secure-email-for-individual-certificate.html
- DigiCert. (2025, February 11). Secure Email Certificates. DigiCert Docs. https://docs.digicert.com/en/certcentral/manage-certificates/client-certificates-guide/secure-email-certificates.html
- Enzoic. (2024, October 2). The High Cost of Password Expiration Policies. https://www.enzoic.com/blog/cost-password-expiration-policies/
- MITRE. (2024, December 20). Strong Password Policy - Technique D3-SPP. MITRE D3FEND. https://d3fend.mitre.org/technique/d3f:StrongPasswordPolicy/
- National Cybersecurity Alliance. (2025, January 13). Create and Use Strong Passwords. https://www.staysafeonline.org/articles/passwords
- NordVPN. (2025, January 28). What is the IPsec protocol? How IPsec VPNs work. https://nordvpn.com/blog/what-is-ipsec/
- SuperTokens. (2024, January 1). 10 Benefits of Multi-Factor Authentication (MFA). https://supertokens.com/blog/benefits-of-multi-factor-authentication
- Whitman, M., & Mattord, H. (2017). Principles of information security (6th ed.). CENGAGE Learning Custom Publishing