Cyber Best Practices

Prepared by: Anastasiya Gruneva
Date: January 31st, 2025

Table of Contents

Table of Contents.....2
Executive Summary.....3
Strong password.....5
Password expiration policy.....7
MFA.....8
Secure email with personal certificate.....10
VPN IPSec on the laptops.....12
Encrypted hard drives/flash disks to protect portable/mobile devices.....13
References.....15

Executive Summary

This report presents a comprehensive overview of best practices for strengthening cybersecurity in organizations, focusing on key areas such as strong password policies, multi-factor authentication (MFA), email security, and the protection of portable devices through encryption. By adopting these measures, companies can effectively mitigate risks associated with unauthorized access, data breaches, and cyber threats, while enhancing the overall security of sensitive information.

1. Strong Passwords:
The report emphasizes the importance of enforcing strong password policies to minimize the risk of unauthorized access. Adhering to the NIST guidelines (SP 800-63B), organizations should require long, random, and unique passwords for each account, along with the use of password managers to securely store credentials. Weak passwords, like those using simple sequences or personal details, leave systems vulnerable to cybercriminals.

2. Password Expiration Policy:
Following the NIST Special Publication 800-63B, the report advises against mandatory periodic password changes unless there is evidence of a security breach. Frequent password changes can often lead to weaker passwords, whereas resetting passwords only when necessary ensures better security.

3. Multi-Factor Authentication (MFA):
MFA is a critical component in protecting sensitive company data. The report highlights that by requiring additional verification factors beyond a password (e.g., biometrics or one-time codes), organizations can significantly reduce the risk of unauthorized access and credential theft, particularly for remote and hybrid workforces.

4. Secure Email with Personal Certificates:
The report underscores the use of S/MIME email certificates to secure email communications. These certificates enable email encryption and digital signatures, ensuring the confidentiality and authenticity of messages. NIST guidelines (SP 800-177) are referenced to illustrate the process and benefits of using encrypted email for sensitive data transmission.

5. VPN IPsec on Laptops:
To secure remote communications, the report advocates for implementing IPsec VPNs on laptops. IPsec provides encryption, integrity checks, and authentication to ensure that sensitive company data remains secure during transmission over public networks.

6. Encrypted Hard Drives/Flash Disks for Portable Devices:
The importance of encrypting portable devices such as USB drives and external hard drives is also emphasized. By using full-disk encryption (FDE), organizations can protect sensitive data, even in the event of device theft or loss. Following NIST guidelines (SP 800-111), encryption is crucial for compliance, risk reduction, and safeguarding employee data.

In conclusion, adopting these cybersecurity best practices will help organizations safeguard their employees, data, and reputation, ensuring compliance with regulatory standards and protecting against emerging cyber threats. The report draws upon the latest NIST publications and industry guidelines to provide a robust framework for implementing secure cybersecurity measures across various organizational functions.

Strong password

The primary objective of enforcing strong password policies is to strengthen cybersecurity, minimizing the risk of unauthorized access, data breaches, and identity theft.

Basic passwords like "12345" or easily guessed personal details (e.g., birthdays or pet names) do not provide sufficient protection for corporate accounts. Using weak passwords is comparable to locking your door but leaving the key in plain sight—cybercriminals can crack them in seconds.

The time required to break a password in 2024 depends on its length and complexity:

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

Figure 1. Time to crack passwords in 2024 (Neskey, 2025).

By following the NIST password guidelines, businesses can safeguard their information security assets, adhere to compliance requirements, and apply best practices recognized by the US and worldwide.

The NIST Password Guidelines (SP 800-63B) emphasize both password security and user behavior to improve authentication practices. According to CISA's Secure Our World initiative, strong passwords should be:

- **long** (at least 16 characters),
- **random** (mix of letters, numbers, and symbols or a passphrase),
- and **unique** for each account.

Using a **password manager** is recommended to securely generate and store complex passwords, reducing the risk of cyber threats (CISA, 2025).

Password expiration policy

According to NIST Special Publication 800-63B (part of NIST SP 800-63-3 Digital Identity Guidelines), password expiration policies should not require users to change passwords regularly unless there is evidence of compromise. Key points here are:

1. No Mandatory Periodic Expiration
    - Forcing users to change passwords at regular intervals (e.g., every 90 days) is not recommended unless a security breach has occurred.
    - Frequent password changes often lead to weaker passwords (e.g., users creating predictable variations of old passwords).
2. Password Changes Only When Necessary
    - Users should change their passwords immediately if there is evidence of compromise (e.g., leaked credentials, phishing attack).
    - Organizations should monitor for credential breaches and notify users when a reset is required.

MFA

Multi-factor authentication (MFA) is a layered security approach that enhances account protection by requiring users to provide additional verification beyond just a password. This process may include entering a one-time code sent to an email, responding to a security question, or using biometric authentication such as a fingerprint scan. By incorporating a second authentication factor, MFA significantly reduces the risk of unauthorized access, even if a password has been compromised.

The NIST in Password Guidelines (SP 800-63B) emphasizes the importance of MFA as a critical security measure that requires users to verify their identity through multiple factors beyond just a username and password. This approach enhances security by combining two or more of the following factors:

- Something you know (e.g., a password)
- Something you have (e.g., a security token or smartphone)
- Something you are (e.g., biometric verification)

MFA enhances security for a company's employees and sensitive information by adding extra layers of protection beyond just a password. Here is how MFA helps:

Table 1. How MFA Protects Employees and Company Information

Benefit	How It Helps
Prevents Unauthorized Access	Even if a password is stolen, a second authentication factor is required, blocking attackers.
Reduces the Risk of Credential Theft	Stolen passwords alone cannot grant access, reducing the impact of data breaches.
Protects Sensitive Data	Ensures only authorized personnel can access confidential company information.
Secures Remote and Hybrid Workforces	Provides an extra layer of security for employees accessing systems from different locations.
Mitigates Phishing and Social Engineering Attacks	Adds a verification step, stopping hackers even if passwords are leaked.
Ensures Compliance with Security Regulations	Helps meet security standards such as NIST, GDPR, and HIPAA, avoiding penalties.

Builds a Stronger Security Culture	Encourages employees to be more security-conscious and proactive about protecting accounts.

Secure email with personal certificate

The NIST provides guidelines for securing email communications using personal certificates through the implementation of Secure/Multipurpose Internet Mail Extensions (S/MIME). S/MIME enhances email security by enabling encryption and digital signatures, ensuring both the confidentiality and authenticity of email messages.

In NIST Special Publication 800-177, NIST recommends the use of S/MIME for email content security. This involves encrypting and authenticating message content using S/MIME, along with associated certificate and key distribution protocols.

By adopting S/MIME with personal certificates, organizations can protect sensitive information transmitted via email, ensuring that only intended recipients can access the content and verifying the sender's identity through digital signatures.

Imagine you need to email a colleague regarding company financial data. Here's a comparison of how the process works when sending the email with and without an email security certificate:

Table 2. Comparison of Sending Emails With and Without an S/MIME Email Certificate

Without an S/MIME Email Certificate Installed	With an S/MIME Email Certificate Installed
• You create a new email in Outlook. • You draft the content of the email and attach an Excel spreadsheet. • You hit "Send" to send the plaintext email from Outlook. • The email is sent from your email platform to the email server via an unencrypted channel. • The email content (and the spreadsheet attachment) are sent from the email server to the internet. • The email data is then sent from the internet to the recipient's email server.	• You create a new email in Outlook. • You draft the content of the email and attach an Excel spreadsheet. • You hit "Send" to send the plaintext email from Outlook. • Before the message leaves Outlook, the S/MIME email certificate automatically: 1. digitally signs the email to verify your identity as the sender. 2. encrypts the plaintext email data using asymmetric encryption (a public key). • The secure, encrypted email moves from your email platform to the server via

• The recipient receives an unsigned, unencrypted email from you, an unverified sender. They open the email and read its plaintext message and access its plaintext Excel spreadsheet.	an unencrypted channel. • The encrypted email content and attachment are sent from the email server to the internet. • The email data is then sent from the internet to the recipient’s email server. • The recipient receives the encrypted email, which is digitally signed to verify your identity as the sender. • When they open the email, the private key automatically decrypts the content and email attachment so they can read it in plaintext.

This highlights the importance of an email security certificate. In the first case, without an encryption certificate, the sender transmits a plaintext email through an unprotected server and across the internet. This makes both the message and its attachments susceptible to interception by cybercriminals who can access and decipher the data.

In contrast, in the second scenario, the sender uses an email security certificate, encrypting the message before it travels through the unsecured server and internet. As a result, even if an attacker intercepts the email, they cannot decrypt its contents without the private key. Additionally, once the email arrives at the recipient's device, it remains encrypted until properly accessed. This encryption process ensures data security both in transit and at rest.

VPN IPSec on the laptops

Implementing IPsec (Internet Protocol Security) VPNs on laptops is an essential measure for protecting company data and ensuring secure remote access.
An IPsec VPN uses the IPsec protocol suite to establish and maintain secure communication between devices, applications, or networks over the public internet.

How IPsec helps protect employees and information:

- Confidentiality and Encryption: IPsec employs strong encryption algorithms to safeguard data in transit, ensuring that sensitive corporate information, such as login credentials and financial data, remains secure from interception by unauthorized users (NIST SP 800-77).
- Data Integrity: IPsec performs integrity checks to confirm that data has not been altered during transmission (NIST SP 800-53).
- Authentication: IPsec verifies the identity of users and devices, allowing only authorized individuals to establish secure connections with the network and reducing the risk of unauthorized access to sensitive systems (NIST SP 800-77).

By using an IPsec VPN, organizations can significantly strengthen their security posture, enabling employees to access necessary resources securely while maintaining the confidentiality and integrity of company data.

Encrypted hard drives/flash disks to protect portable/mobile devices

Encrypting data on portable devices such as hard drives and flash disks is a critical measure to safeguard confidential company information and ensure secure access for employees. It helps minimize the risks of data breaches, unauthorized access, and device theft.

NIST emphasizes the importance of encrypting portable devices like USB drives, external hard drives, and flash drives to protect sensitive data. It recommends using full-disk encryption (FDE), which automatically encrypts all data on the device. This ensures data protection even in the event of device loss or theft (NIST SP 800-111).

Encryption Algorithms for Data at Rest:

Data at rest refers to stored data on physical media (hard drives, flash disks, servers). For encrypting data at rest, strong encryption algorithms are essential:

- AES (Advanced Encryption Standard) with key lengths of 256 bits is the most widely recommended and used standard for full-disk encryption and file-level encryption. (NIST FIPS 197)
- RSA is used in some cases for encrypting encryption keys themselves (key wrapping), though not commonly for bulk data encryption.
- XTS-AES mode is commonly used in modern full-disk encryption solutions (e.g., BitLocker) to enhance protection against certain attack vectors (IEEE Std 1619-2007).

Encryption Algorithms for Data in Transit:

Data in transit refers to data being transferred over networks. To protect this data from interception and tampering, robust encryption protocols and algorithms are used:

- TLS (Transport Layer Security) protocols with strong cipher suites, using AES-GCM or AES-CCM for symmetric encryption, RSA or ECDSA for authentication, and ECDHE for key exchange (RFC 5246, RFC 8446).
- IPsec (Internet Protocol Security) for secure communication over IP networks, using algorithms like AES and SHA-2 for integrity (NIST SP 800-77).
- SSH (Secure Shell) uses asymmetric algorithms (RSA, ECDSA) for key exchange and AES for bulk data encryption (RFC 4251).

How Encryption Helps Protect Employees and Information:

- Confidentiality:
  Encryption ensures that even if a device is lost or stolen, the data remains inaccessible without the decryption key. This protects sensitive company information (NIST SP 800-111).
- Compliance:
  Many industries require the protection of sensitive data. Encrypting portable devices helps organizations meet regulatory requirements and avoid potential penalties (NIST SP 800-53).
- Risk Reduction:
  By encrypting data on portable devices, organizations minimize the risk of unauthorized access and potential data breaches, helping to prevent financial and reputational damage (NIST SP 800-171).

By using encryption on portable devices, organizations can strengthen their overall security strategy, ensuring that employees can securely work with necessary resources while maintaining the confidentiality and integrity of company data.

References

Neskey, C. (retrieved 2025, January 31). Are Your Passwords in the Green? https://www.hivesystems.com/blog/are-your-passwords-in-the-green

NIST Digital Identity Guidelines. (retrieved 2025, January 31). https://pages.nist.gov/800-63-3/sp800-63-3.html

CISA, Use Strong Passwords. (retrieved 2025, January 31). https://www.cisa.gov/secure-our-world/use-strong-passwords

NIST Trustworthy Email. (retrieved 2025, January 31). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf

NIST Guide to IPsec VPNs. (retrieved 2025, January 31). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

NIST Security and Privacy Controls for Information Systems and Organizations. (retrieved 2025, January 31). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST Guide to Storage Encryption Technologies for End User Devices. (retrieved 2025, January 31). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

NIST Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (retrieved 2025, January 31). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf

Vicente, V. (2024, May 3). NIST Password Guidelines. https://www.auditboard.com/blog/nist-password-guidelines/

Government of Canada. Why multi-factor authentication is an essential part of cyber security. (2020, February 17). https://www.getcybersafe.gc.ca/en/blogs/why-multi-factor-authentication-essential-part-cyber-security

Martinez, J. (2024, June 4). The Importance of Multi-Factor Authentication (How It Works). https://www.strongdm.com/blog/why-mfa-is-important

NSA. Configuring IPsec Virtual Private Networks. (retrieved 2025, January 31). https://media.defense.gov/2021/Sep/16/2002855928/-1/-1/0/CONFIGURING_IPSEC_VIRTUAL_PRIVATE_NETWORKS_2020_07_01_FINAL_RELEASE.PDF