

# NIST password guidelines 2024: 15 rules to follow

## Understanding NIST's 2024 guidelines

The [National Institute of Standards and Technology \(NIST\)](#) recently released its guidelines for 2024, which provide valuable insights and recommendations for various industries. These guidelines aim to enhance cybersecurity practices and promote the adoption of secure technologies. Understanding NIST's guidelines is crucial for organizations to ensure they are following best practices and protecting their sensitive data effectively.

The guidelines cover a wide range of topics, including risk management, data protection, authentication methods, and incident response. By carefully studying and implementing these guidelines, organizations can strengthen their cybersecurity posture and reduce the risk of cyberattacks and data breaches. It is essential for businesses to stay updated with NIST's guidelines to remain resilient in the face of evolving cyber threats.

The NIST's 2024 guidelines are the culmination of extensive research and industry collaboration, aimed at providing a robust framework for password security. These guidelines serve as a beacon, illuminating the path towards a more secure digital ecosystem. By adhering to these meticulously crafted rules, you can significantly reduce the risk of unauthorized access, data breaches, and other cyber threats that plague the modern world.

Read our [GRC Launchpad](#) article: [NIST CSF Overview and Guides](#) for more information.

## NIST password guidelines: introduction

The NIST password management system is used to enhance security and reduce the risk of unauthorized access. NIST's password guidelines emphasize the importance of creating strong, complex passwords that are difficult for attackers to guess or crack. This includes using a combination of upper- and lower-case letters, numbers, and special characters. Additionally, NIST recommends avoiding common words, phrases, or patterns that are easily guessable.

Furthermore, NIST advocates for the use of passphrases, which are longer, easier-to-remember phrases composed of multiple words or characters. Passphrases offer increased security compared to traditional passwords and are less susceptible to brute-force attacks.

Moreover, NIST advises against forced password changes at regular intervals, as this can lead to users choosing weaker passwords or recycling old ones. Instead, NIST suggests encouraging users to change passwords only in response to security incidents or when there is evidence of compromise.

Overall, NIST's password guidelines aim to promote strong, user-friendly password practices that enhance security without sacrificing usability. By following these recommendations, organizations can strengthen their password security posture and mitigate the risk of unauthorized access and data breaches.

In today's digital age, where cyber threats are becoming increasingly sophisticated, it is essential to prioritize the security of our online accounts. Passwords play a crucial role in protecting our sensitive information from unauthorized access.

The National Institute of Standards and Technology (NIST) has long been at the forefront of

establishing guidelines to ensure password security. In this article, we will explore the NIST Password Guidelines for 2024 and discuss 15 rules that you should follow to enhance your password security.

## The importance of strong passwords

Passwords serve as the first line of defense against unauthorized access to your personal and professional accounts. Weak passwords can be easily cracked by hackers, leaving your sensitive data vulnerable to theft and misuse.

Strong passwords play a crucial role in enhancing cybersecurity and protecting sensitive information in accordance with the National Institute of Standards and Technology (NIST) guidelines. NIST emphasizes the significance of strong passwords as a fundamental component of effective security measures to mitigate the risk of unauthorized access and data breaches.

They are characterized by complexity, randomness, and uniqueness, making them more resistant to brute-force attacks and password guessing techniques. NIST recommends the use of passwords that are at least eight characters long and include a combination of uppercase and lowercase letters, numbers, and special characters.

By adhering to NIST's guidelines for strong passwords, organizations can significantly reduce the likelihood of unauthorized access to systems, networks, and sensitive data. Strong passwords serve as a critical barrier against cyber threats, safeguarding against potential security breaches and protecting the confidentiality, integrity, and availability of valuable information assets.

The importance of strong passwords in NIST underscores their role as a foundational security measure in safeguarding digital assets and promoting a robust cybersecurity posture across organizations and industries. It's crucial to understand the significance of strong passwords and the role they play in safeguarding your online presence.

## Key changes in 2024 guidelines

The 2024 guidelines have brought about significant changes that will impact various industries and sectors. One key change is the implementation of stricter regulations on data privacy and protection. With the increasing number of data breaches and cyberattacks, it has become crucial for organizations to prioritize the security of personal and sensitive information.

The new guidelines provide detailed instructions on how to handle, store, and transmit data securely, ensuring that individuals' privacy rights are protected. Another important change in the 2024 guidelines is the emphasis on sustainable practices. As the world grapples with the effects of climate change and strives to achieve environmental sustainability, businesses are being urged to adopt eco-friendly measures. The guidelines encourage organizations to reduce their carbon footprint, promote renewable energy sources, and implement waste management strategies. This shift towards sustainability reflects a growing recognition of the need to balance economic growth with environmental responsibility.

Furthermore, the 2024 guidelines also address the issue of diversity and inclusion in the workplace. It is now recognized that diverse teams contribute to innovation, creativity, and overall organizational success. The guidelines provide recommendations for promoting diversity at all levels of the workforce, including recruitment practices, career development opportunities, and inclusive policies. By creating a more inclusive environment, organizations can harness the full potential of their employees and foster a culture of equality and fairness.

In addition to these changes, the 2024 guidelines also stress the importance of continuous learning and upskilling. With advancements in technology and evolving market trends, it is vital for

professionals to stay updated with the latest knowledge and skills. The guidelines encourage individuals to engage in lifelong learning through various means, such as attending workshops, pursuing online courses, or participating in industry conferences. By prioritizing continuous learning, individuals can enhance their employability and adapt to the ever-changing demands of the modern workplace.

Overall, the key changes in the 2024 guidelines reflect the evolving needs and challenges of today's world. From data privacy to sustainability and diversity, these guidelines aim to create a framework for organizations to thrive while upholding ethical standards and societal responsibilities. Embracing these changes will not only benefit businesses but also contribute to a more inclusive, sustainable, and secure future.

The National Institute of Standards and Technology (NIST) periodically updates its guidelines to improve security practices. The 2024 updates to NIST password guidelines focus on enhancing security while simplifying the user experience. Here are the key changes:

### 1. Elimination of Periodic Password Changes

1. **Previous Requirement:** Users were often required to change their passwords periodically (e.g., every 90 days).
2. **2024 Update:** NIST now recommends against periodic password changes unless there is evidence of a compromise. Frequent changes can lead to weaker passwords, as users may create simple, predictable patterns.

### 2. Longer Passwords Over Complexity

1. **Previous Requirement:** Emphasis was on password complexity (mix of uppercase, lowercase, numbers, and special characters).
2. **2024 Update:** NIST emphasizes allowing longer passwords (up to 64 characters) over complex ones. Users can create passphrases that are easier to remember and harder to crack.

### 3. Screening Against Common Password Lists

1. **Previous Requirement:** Passwords were checked primarily for length and character requirements.

2. **2024 Update:** Organizations should screen new passwords against lists of commonly used, expected, or compromised passwords. This reduces the likelihood of users choosing easily guessable passwords.

#### 4. Encouraging Password Managers

1. **Previous Requirement:** Limited guidance on the use of password managers.
2. **2024 Update:** NIST recommends the use of password managers to create and store strong, unique passwords for each account. This practice enhances security by reducing password reuse and simplifying password management for users.

#### 5. Multi-Factor Authentication (MFA)

1. **Previous Requirement:** MFA was recommended but not emphasized for all accounts.
2. **2024 Update:** Strong emphasis on the use of MFA for an added layer of security, particularly for sensitive accounts and systems. MFA significantly reduces the risk of unauthorized access, even if a password is compromised.

#### 6. No Composition Rules

1. **Previous Requirement:** Strict composition rules (e.g., must include special characters, numbers, and mixed cases) were often enforced.
2. **2024 Update:** NIST advises against mandatory composition rules. Instead, it recommends allowing users to create passphrases and only enforcing rules that prevent common or easily guessable passwords.

#### 7. Password Hint and Knowledge-Based Authentication

1. **Previous Requirement:** Password hints and knowledge-based authentication (e.g., security questions) were common.
2. **2024 Update:** NIST advises against the use of password hints and security questions as they often provide weak security and can be easily guessed or researched.

#### 8. Rate Limiting and Lockouts

1. **Previous Requirement:** Account lockouts after several failed login attempts were commonly implemented.
2. **2024 Update:** NIST recommends rate limiting (delaying responses after failed attempts) rather than lockouts. This approach helps mitigate brute force attacks while reducing the risk of denial-of-service conditions where users are locked out of their accounts.

The 2024 NIST password guidelines focus on improving security by simplifying the user experience and leveraging modern technologies such as password managers and MFA. By emphasizing longer passwords, screening against common password lists, and reducing the reliance on frequent changes and complex composition rules, NIST aims to make password security more effective and user-friendly.

## Impact on cybersecurity

The impact of these updated guidelines on cybersecurity is substantial. By encouraging longer and more unique passwords, organizations reduce the odds of breaches due to guessable or common passwords. Moreover, eliminating the forced periodic changes reduces the tendency to create

simple, predictable passwords, which are easier to compromise. Overall, the new NIST guidelines aim not only to simplify the user's security process but to fortify it against evolving cyber threats.

## Overview of the NIST password guidelines 2024

As of 2024, the National Institute of Standards and Technology (NIST) continues to provide updated guidelines for password management to address evolving cybersecurity threats and enhance the resilience of digital systems. NIST's password guidelines for 2024 emphasize the importance of adopting password practices that balance security with usability.

One key aspect of the updated guidelines is the encouragement of the use of passphrase-based authentication. Passphrases, which are longer and composed of multiple words or characters, offer increased security compared to traditional passwords while being easier to remember for users. NIST recommends using passphrases as an alternative to complex passwords, promoting user-friendly security practices.

Furthermore, NIST advises against periodic password changes unless there is evidence of compromise or security incidents. Instead, organizations are encouraged to implement multi-factor authentication (MFA) and other robust authentication mechanisms to supplement password-based security.

Overall, NIST's password guidelines for 2024 aim to promote a pragmatic approach to password management that prioritizes strong security while minimizing user burden. By adopting these guidelines, organizations can enhance their cybersecurity posture and mitigate the risk of unauthorized access and data breaches in today's evolving threat landscape.

The NIST Password Guidelines for 2024 are a set of recommendations and best practices designed to ensure robust password security. These guidelines are continually updated to address emerging threats and incorporate the latest advancements in technology. Adhering to these guidelines can significantly reduce the risk of password-related security breaches.

Let's now delve into the 15 rules outlined in the NIST Password Guidelines 2024.

- 1. Use passwords that are at least 12 characters long.**

Longer passwords are inherently more secure than shorter ones. The NIST Password Guidelines recommend using passwords that are at least 12 characters long.

Longer passwords provide more entropy, making them harder to crack through brute-force attacks. It is crucial to choose a combination of upper-case and lower-case letters, numbers, and special characters to enhance the complexity of your password.

## **2. Avoid commonly used passwords**

Avoid using commonly used passwords such as “password,” “123456,” or “qwerty.” These passwords are incredibly weak and are often the first choices for hackers attempting to gain unauthorized access. Instead, opt for unique passwords that are not easily guessable. Consider using a combination of random words or phrases to create a strong and memorable password.

## **3. Implement two-factor authentication**

Two-factor authentication (2FA) provides an additional layer of security by requiring users to provide two forms of identification before accessing an account. This typically involves a password and a unique verification code sent to a trusted device.

Implementing 2FA significantly reduces the risk of unauthorized access, even if your password is compromised.

## **4. Use a password manager**

With the increasing number of online accounts we have today, remembering unique and complex passwords for each one can be challenging. Password managers are invaluable tools that securely store all your passwords in one place.

They can generate strong passwords and even automatically fill them in for you. Using a password manager simplifies the process of managing multiple passwords while ensuring their security.

## **5. Regularly update passwords**

It's important to periodically update your passwords to minimize the risk of unauthorized access. The NIST Password Guidelines recommend changing your passwords every six months, or sooner if you suspect any compromise. Regularly updating your passwords helps mitigate the potential damage caused by a password breach and ensures the continued security of your accounts.

## **6. Avoid using personal information in passwords**

Using personal information such as your name, birthdate, or address in your passwords is a common mistake that can compromise your account security. Hackers can easily obtain this information through social engineering or data breaches. It is crucial to choose passwords that are unrelated to your personal life and difficult for others to guess.

## **7. Implement password complexity requirements**

Implementing password complexity requirements adds an extra layer of security to your accounts. The NIST Password Guidelines recommend using a mix of uppercase and lowercase letters, numbers, and special characters in your passwords.

This combination increases the complexity and makes it more challenging for hackers to crack your password.

## **8. Educate employees on password security**

In a corporate setting, employees are often the weakest link in the security chain. It is essential to educate and train employees on password security best practices. This includes teaching them about the importance of strong passwords, how to create and manage passwords securely, and the risks associated with password reuse.

Regular training sessions and awareness campaigns can significantly enhance the overall security posture of an organization.

## **9. Implement password expiration policies**

Password expiration policies require users to change their passwords after a set period.

While this practice has been debated in recent years, it is still recommended as a security measure. The NIST Password Guidelines suggest a maximum password expiration period of 60 days.

However, it's essential to strike a balance between security and usability to avoid password fatigue among users.

## **10. Monitor for password breaches**

Constant monitoring for password breaches is crucial to identifying potential vulnerabilities and taking appropriate action promptly. Organizations should invest in robust security measures that detect and notify administrators when passwords

associated with their domain appear in public breach databases.

Promptly resetting compromised passwords and notifying affected users can prevent unauthorized access and mitigate potential damage.

**11. Use biometric authentication when possible**

Biometric authentication, such as fingerprint or facial recognition, provides an additional layer of security and convenience. Biometric data is unique to each individual and difficult to replicate, making it an effective method of authentication.

Whenever possible, leverage biometric authentication alongside traditional password-based systems to enhance the security of your accounts.

**12. Implement secure password storage**

Storing passwords securely is essential to prevent unauthorized access to sensitive information. Organizations should utilize robust encryption algorithms to store passwords securely. Additionally, implementing measures such as salting, hashing, and key stretching can further enhance password storage security.

It's important to regularly assess and update password storage practices to align with the latest security standards.

**13. Encrypt passwords in transit**

When transmitting passwords over the internet, it's crucial to encrypt them to prevent interception by malicious actors. Implementing secure communication protocols, such as HTTPS, ensures that passwords are encrypted during transmission.

This protects sensitive information from being intercepted and reduces the risk of password compromise.

**14. Regularly audit password security**

Regularly auditing password security is a proactive measure to identify weaknesses and ensure compliance with established guidelines. Conducting periodic password security audits can help identify accounts with weak passwords, detect potential password reuse, and enforce password complexity requirements.

It is crucial to address any vulnerabilities promptly to maintain a robust security posture.

**15. Continuously update password guidelines**

As cyber threats continue to evolve, it is essential to keep up with the latest developments in password security. The NIST Password Guidelines are continuously updated to address emerging threats and incorporate advancements in technology. It is imperative to stay informed and adapt your password security practices accordingly.

## Conclusion

Implementing strong password security measures is crucial in today's digital landscape. Following the NIST Password Guidelines for 2024 and adhering to the 15 rules outlined in this article will significantly enhance the security of your online accounts. Remember to use long, complex passwords, avoid common choices, and regularly update your passwords.

Implement two-factor authentication, use a password manager, and educate yourself and others about password security best practices. By following these guidelines, you can take control of your online security and protect your sensitive information from unauthorized access.

At TrustCloud, we offer tailored solutions and expert guidance to help you develop and implement a proactive compliance management strategy, assuring trust among your stakeholders. [Sign up](#) today to learn more about how we can help you navigate the complex regulatory landscape with confidence.

Explore our [GRC launchpad](#) to gain expertise on numerous GRC topics and compliance standards.