NIST Password Guidelines: 9 Rules to Follow [Updated in 2024]

Editor's note: This post was originally published on October 17, 2022 and has been revised for clarity and comprehensiveness.

How do your organization's current practices measure up against the latest standards? Are you sure your password guidelines can thwart evolving digital threats?

With cyber threats becoming more sophisticated, following the National Institute of Standards and Technology's (NIST) cybersecurity guidelines will help safeguard your digital assets.

If you haven't had the chance to explore these new guidelines in depth, we understand. As a managed security service provider (MSSP), we are responsible for keeping our clients informed about the latest cybersecurity trends.

And so, we've investigated the guidelines for you and listed the **password standards** you should follow. By the end of the article, you should have a solid starting point for creating strong password policies for you and your organization.

RELATED: *What is the NIST Cybersecurity Framework?*

1. Password length matters the most.

The updated guidelines emphasize the importance of password length, not password complexity. **User-generated passwords should be at least eight (8) characters, while machine-generated passwords should be at least six (6) characters.**

If you have a website or platform that requires logins, you should also allow users to **see** the password while creating it instead of limiting visibility to a series of asterisks.

2. Allow 64-character Passwords

Building off rule #1, allow passwords with at least 64 characters. Having 64-character passwords supports the use of unique passphrases, enabling easier memorization. However, users should still carefully avoid the characteristics mentioned in the next rule.

3. Check passwords against a blacklist.

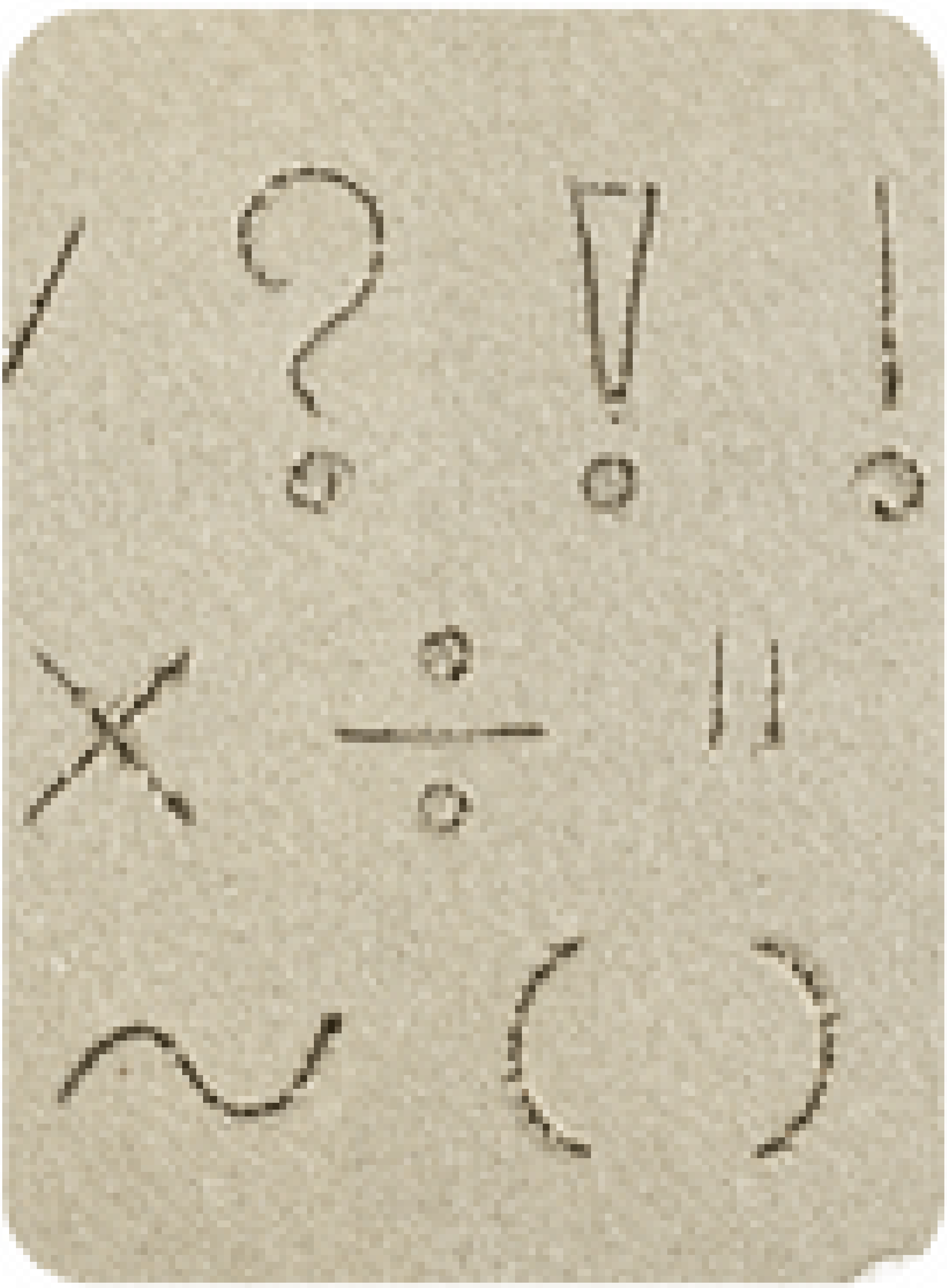
When creating a password, it should not have any of the following characteristics:

- In previous password breaches
- Dictionary words
- Repetitive or sequential (e.g., 'uuuuuu,' '1234abcd')
- Context-specific (e.g., derivatives of the name of the service or the username)

Each organization should have a mini "blacklist" composing passwords with these qualities. **Use it as a reference whenever someone creates a new password and rejects passwords that overlap with the list.**

However, your blacklist shouldn’t include every possible password or dictionary word; you’ll end up with frustrated users. Instead, analyze the most used passwords, dictionary words, and character combinations. Use this analysis as the foundation for your blacklist and build it up from there.

4. Make special character rules optional.



Rules like including an uppercase, lowercase, or special character (e.g., !@#$%^) in passwords are no longer necessary.

NIST claims adding these rules isn’t necessary because they make it more likely for users to create weaker passwords.

“Analyses of breached password databases reveal that the benefit of [special character] rules is not nearly as significant as initially thought,” the NIST guidelines state, “although the impact on usability and memorability is severe.”

Users often default to one or two phrases and slightly adjust them according to each website’s requirements. **Promoting unconnected and lengthy passwords is more important in the current tech environment.**

However, this doesn’t mean users shouldn’t use special characters. Special characters are still acceptable if you **don’t** default to one phrase for all your accounts with slightly changed special characters or capitalization.

5. Provide feedback explaining password rejections.

Providing clear, meaningful, actionable feedback is necessary for handling user passwords. You can do this by:

- Implementing password-strength meters
- Limiting the number of password attempts
- Allowing users to see their password (instead of seeing only dots/asterisks)

When a user attempts to create a password that doesn't meet your standards, you need to explain which rule it violates. This helps users create passwords that protect their account and your database.

6. Remove hints and security questions.

Never allow users to request a password hint or answer “security questions” (like “What was the name of your first pet?”) to recover account access.

Instead, offer ways to verify their identity and reset their password. NIST recommends users undergo another authentication process if they lose all access to their accounts.

7. Use password managers safely.

Many people use password managers, and **while NIST doesn't explicitly recommend their use, they encourage account managers to allow a copy-paste functionality to accommodate password managers.**

NIST also laid out the following recommendations for using a password manager:

- Choose a long passphrase you can memorize.
- Create unique passwords for all accounts in the password manager.

- Avoid password managers that allow recovery of the master password.
- Use MFA (Multi-factor Authentication) for your password manager.
- Generate random, complex answers for online security questions.

RELATED: *2FA vs. Password Manager*

8. Change passwords only when necessary.

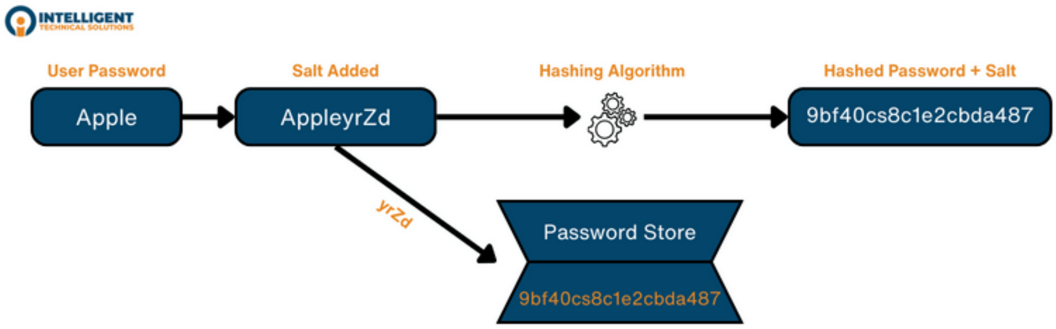
Gone are the days of periodically changing passwords. Instead, **NIST recommends initiating password changes only for user requests or evidence of authenticator compromise.**

They claim constantly changing passwords only frustrates users and encourages them to use weaker passwords to aid memorization. When changing often, people also tend to conform to a pattern, making it easier for cybercriminals to guess the new password.

That said, **it’s better to leave passwords alone until a change is necessary.**

9. Store passwords in offline-attack-resistant forms.

Password breaches are common. In SP 800-63B Section 5.1.1.2, NIST recommends that password information be salted and hashed using a suitable one-way key derivation function. Salting and hashing passwords are the first steps in keeping data safe from offline attacks.



Ready to Implement the NIST Password Guidelines?

The NIST password recommendations emphasize randomization, lengthiness, and secure storage.

But even though the concepts are clear, implementing them for your business is another story. It’s challenging to stay aware of current cybersecurity guidelines and even more difficult to follow them. You need an expert IT team, watertight processes, and up-to-date IT infrastructure.

However, having someone guide you through the security process can make a world of difference. For example, our clients at ITS have their systems on the latest cybersecurity guidelines while focusing on their primary business objectives.

Schedule a meeting with our experts today to learn how to implement these NIST password guidelines for your business. You can also read related resources on password management and cybersecurity: