NIST Password Guidelines 2022: 9 Rules to Follow

itsasap.com/blog/nist-password-guidelines

Are you keeping up with NIST's (National Institute of Standards and Technology's) cybersecurity guidelines?

In March 2022, NIST, a non-regulatory agency of the United States Department of Commerce, released the third revision of Special Publication 800-63 (NIST SP 800-63-3).

NIST SP 800-63 explains the requirements for federal agencies implementing digital identity services. It covers registration, authentication, management, and tools for creating user accounts.

SP 800-63 is divided into four sections:

1. Digital Identity Guidelines (SP 800-63-3)
2. Guidelines for Enrollment and Identity Proofing (SP 800-63A)
3. Guidelines for Authentication and Lifecycle Management (SP 800-63B)
4. Guidelines for Federation and Assertions (SP 800-63C).

Aside from these guidelines, NIST also created implementation resources. Multiple checklists, criteria, and documents are available to help organizations - federal or not - evaluate their cybersecurity.

If you haven't had the chance to dive into the nitty gritty of these new guidelines, we understand. It's getting harder to stay aware of new security standards due to the rapid pace of technology. And as a Managed Security Service Provider (MSSP), it's our job to keep our clients informed about the new cybersecurity trends.

9 Password Guidelines to Follow

You need new, easy-to-implement information. To get that, here are the nine rules you should follow from NIST's new guidelines:

1. Monitor password length.

The updated guidelines emphasize the importance of password length. User-generated passwords should be **at least eight (8) characters**, while machine-generated passwords should be **at least six (6) characters**.

2. 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 who behave predictably. Instead, analyze the most commonly used passwords, dictionary words, and character combinations. Use this analysis as the foundation for your blacklist and build it up from there.

3. Make special character rules optional.

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

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

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

However, this doesn’t mean users shouldn’t use special characters. There is still room for these characters when generating randomized passwords. Strict rules are discouraged, and special characters are not.

4. Allow 64-character passwords.

Building off #3, **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 Rule #2.

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.

Never allow users to request a password hint. 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.

Read: “2FA vs. Password Manager”

8. Change passwords only when necessary.

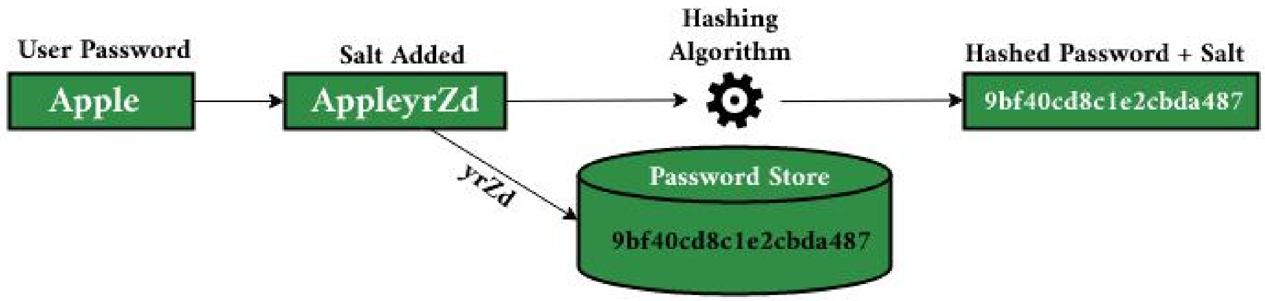
Gone are the days of periodically changing passwords. Instead, **NIST recommends initiating password changes only for user requests or evidence of authenticator compromise.**

They claim constantly changing passwords only frustrates users and encourages them to use weaker passwords to aid memorization. It also widens a criminal’s window of opportunity to hijack an account, as regular password changes are common occurrences.

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 a common occurrence. 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.



Source: GeeksforGeeks

Need Help Implementing NIST Password Guidelines for Your Business?

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 you can implement these NIST password guidelines for your business. Alternatively, you can read our downloadable guide on What Businesses Need to Know About Managed Cybersecurity Services to learn more about other ways to protect your business data.