NIST Password Guidelines: All You Need to Know

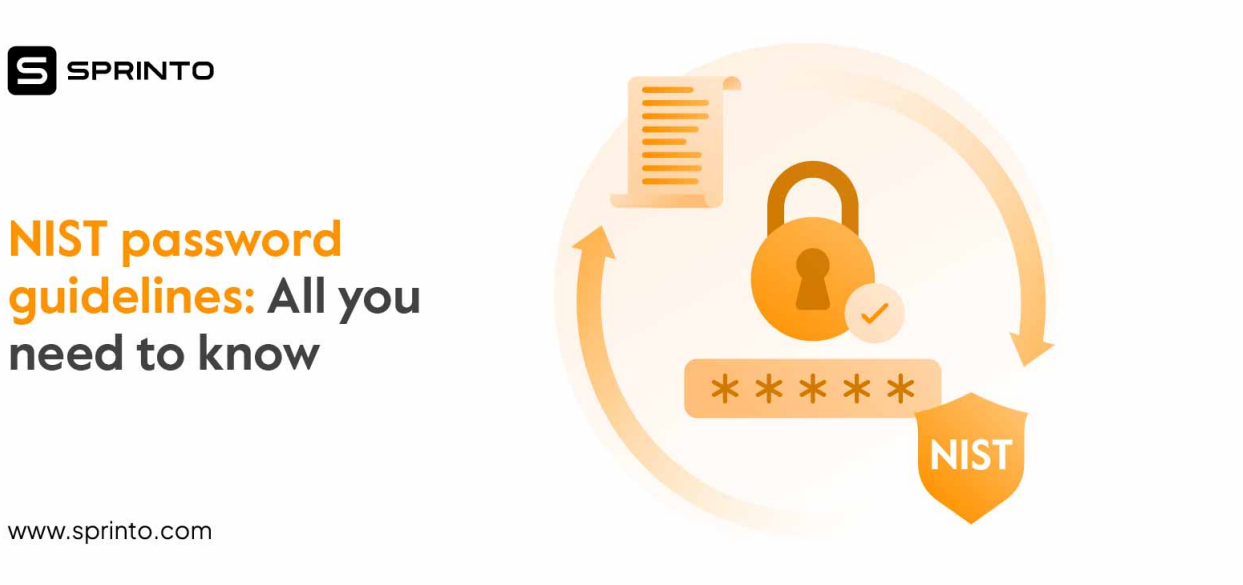
Did you know that more than 60% of Americans tend to use the same password for multiple accounts? The underlying logic behind this practice is that it's easier to remember. However, the million-dollar question arises: is this convenience enough to safeguard sensitive information? Absolutely not.

While many traditional practices surrounding password security may seem intuitive, a significant number of them need to be more accurate, updated, and counterproductive.

This is where the NIST password guidelines (National Institute of Standards and Technology), specifically NIST Special Publication 800-63B, come into play.

Although these guidelines are mandatory only for federal agencies, they have earned the reputation of being the gold standard for password security. Experts highly regard them for their extensive research, thorough vetting, and broad applicability.

Let's dive in to learn more about NIST password requirements.



Why NIST password guidelines are crucial?

NIST password guidelines protect your information assets and comply with security standards requirements. They represent a set of internationally recognized best practices endorsed worldwide to enhance cybersecurity.

NIST SP 800-63-3 password guidelines are important as the number of password-cracking attempts increases. When attackers gain valid credentials, they can access your systems and escalate their privileges to an administrator or superuser level, resulting in a security breach.

This breach can have severe consequences, from compromising your organization's security posture to damaging your reputation and financial stability. To avert this, passwords serve as the first line of defense against cyber threats. Following the NIST SP 800-63-3 guidelines fortifies your information security infrastructure.

NIST password guidelines

The NIST Password Guideline Standards were first published in 2017 and last updated in 2020, can be found in NIST Special Publication 800-63B. NIST SP 800-63-3 guidelines and is a major component of NIST's Digital Identity Guidelines.

These password best practices from NIST SP 800-63-3 guidelines don't just emphasize the strength of passwords but also consider the behavior of the individuals creating these passwords while recommending a fortifying method.

The goal is to provide recommendations on various aspects of password management, including creation, authentication, implementation, storage, and regular updates.

Here are the 11 rules for NIST Password guidelines are as follow:

1. Use a password manager

Boosting your password strength is easier than you think. According to NIST SP 800-63-3 guidelines, one effective way is by using a password manager. It's a tool that effortlessly encrypts your passwords and conjures up robust ones.

Here, reducing human error is key. Password managers automatically whip up NIST SP 800-63-3 guidelines for password length and potent passwords or passphrases, sparing you the headache of crafting them manually.

Studies have also revealed that user behavior plays a significant role in password security. Many folks recycle weak passwords rather than fashion new ones that adhere to security guidelines.

This practice opens up multiple vulnerabilities, especially when the same strong password is used across various platforms.

The solution? Equip your team with a password manager like the 1 password tool and give them the know-how.

hands-on workshop

From Manual To Maverick: For Security Professionals

All about Compliance Automation!
RSVP NOW

2. Password length is always greater than complexity

There's a surprising twist to user-created passwords: it's not complexity but length that genuinely matters. You might think that a complex password filled with symbols, numbers, and uppercase letters is the way to go, but the length makes a big difference too.

Longer or maximum passwords are tough to breach even if someone gets their hands on them.

Insisting on complexity, like throwing in special characters or uppercase letters, can sometimes backfire. People take shortcuts, like capitalizing the first letter or adding a predictable "1" or "!" to the end.

While this adds some difficulty, experienced password-crackers anticipate this rookie moves with easy phishing attacks. That's why the NIST SP 800-63-3 guidelines demand a minimum of 8 characters for standard passwords as a part of the risk management process or privacy risk assessment. Don't use the same single character or consecutive characters for all your passwords.

3. Choose the "Show Password While Typing" option

Making typos while entering passwords is as common as a cup of morning coffee. When those characters instantly turn into those mysterious dots, it's easy to lose track of where you went wrong.

This can be frustrating and push you to pick shorter, simpler passwords, especially on websites that limit login attempts and make it easy for unauthorized access.

If you can toggle the option to show your password recommendations as you type from your password lists or passwords against lists. You'll be much more confident entering those long, complex common passwords correctly on the first attempt, making your online life much smoother with distinct authentication factors.

4. Breached password protection

According to NIST SP 800-63-3 guidelines, every time you create a new password with some password recommendations, it gets a thorough check against a "blacklist." This list includes no-nos like common dictionary words or simple passwords, repetitive or easily guessable strings,

passwords compromised in previous security breaches, and even sneaky variations on the site's name.

Basically, it looks out for all the tricks cybercriminals might try.

For example, some, like Auth, go beyond the usual checks and continuously monitor login attempts in real-time against this blacklist. So, even if your password lists somehow end up in the wrong hands, you're still safe with a strong authentication process.

5. Keep your password safe with salting and hashing

To keep your secrets safe and sound, NIST SP 800-63-3 guidelines lay down some essential rules. First, when someone creates a lengthy password with lower or upper case letters, it should immediately disappear from the server or primary channel. You can do this using techniques like the zero-knowledge password protocol or zeroization.

You can also do this with Hashing. NIST defines it as a way to transform a plain password into a code, a fixed-length string that looks like a jumble of letters and numbers. Imagine turning "password123" into something like "m8kj94r2l3p8b7l1 for your secure storage."

So, instead of storing actual passwords, you store these secret codes, known as password hashes, with proper security standards. If hackers try to break in, they only see these codes, not the real passwords.

NIST certification also recommends "salting." Nope, it's not your kitchen salt, but adding some extra info to passwords before hashing them. This extra bit makes it even trickier for hackers to crack the code or dry dictionary attacks from their password databases.

For example: Password value is mnc123. The salt value is saltQwoptyu@123. However, make sure to conduct period password resets.

6. Don't use "Password Hints"

Some companies offer hints or ask personal questions to help users remember their tricky passwords.

But thanks to social media and tricks like social engineering, it's become easy for attackers to find those answers.

That means they can sneak into your user's accounts without breaking a sweat. So, guess what? NIST Special Publication security experts say this practice is a no-go for any service provider. It's off the list now because it's just not safe.

7. Don't change passwords frequently

The old idea of regularly switching them out has evolved. Now, NIST suggests periodic password resets only when there's a good reason, like when a user asks for it or if there's real proof that someone might have cracked it.

Why the change? Well, it turns out that making people constantly change their passwords with password complexity requirements makes them frustrated. It's a hassle, often leading to them picking simpler passwords they can remember. It gives hackers more chances to sneak in because frequent password changes are expected.

8. Limit the number of password attempts

Some bad actors like to guess secure passwords repeatedly until they get lucky (we call this a brute-force attack). You can cap how many tries they get in the repetition of passwords before the account locks up.

Attackers usually need way more tries than someone who makes a typo occasionally. Setting a limit or adding a delay will make it hard for the attacker. It'll take them so long to crack it that it's not worth their time.

9. Use Multi-Factor Authentication

MFA is also known as two-factor authentication (2FA). Here's how it works: to log in, you need to prove two things out of three categories:

- There's "something you know," like a password. You've got that covered
- There's "something you have," like a phone. You might have an app or a code on your phone
- There's "something you are," like a fingerprint. That's your unique biometric signature

NIST says MFA is a must for protecting personal info online. But they're picky about what counts as a valid form of authentication.

For example, email and voice-over-internet protocol (VoIP) don't cut it because they're not considered out-of-band (OOB) authenticators.

10. Give feedback explaining why you rejected a password

It's important to help users understand why their passwords might be rejected. Here's how you can do it:

- You can use password-strength meters. These little helpers show users how strong or weak your secure password is.
- Consider limiting the number of secure password tries. This doesn't give way to endless guessing.
- Let users see their secure password as they type it instead of just showing dots or asterisks. This makes it easier for them to spot mistakes.

When a user tries to create a password that doesn't meet your standards, explaining which rule it breaks is a good idea.

This way, they can fix it and create a password that keeps their account and your database safe.

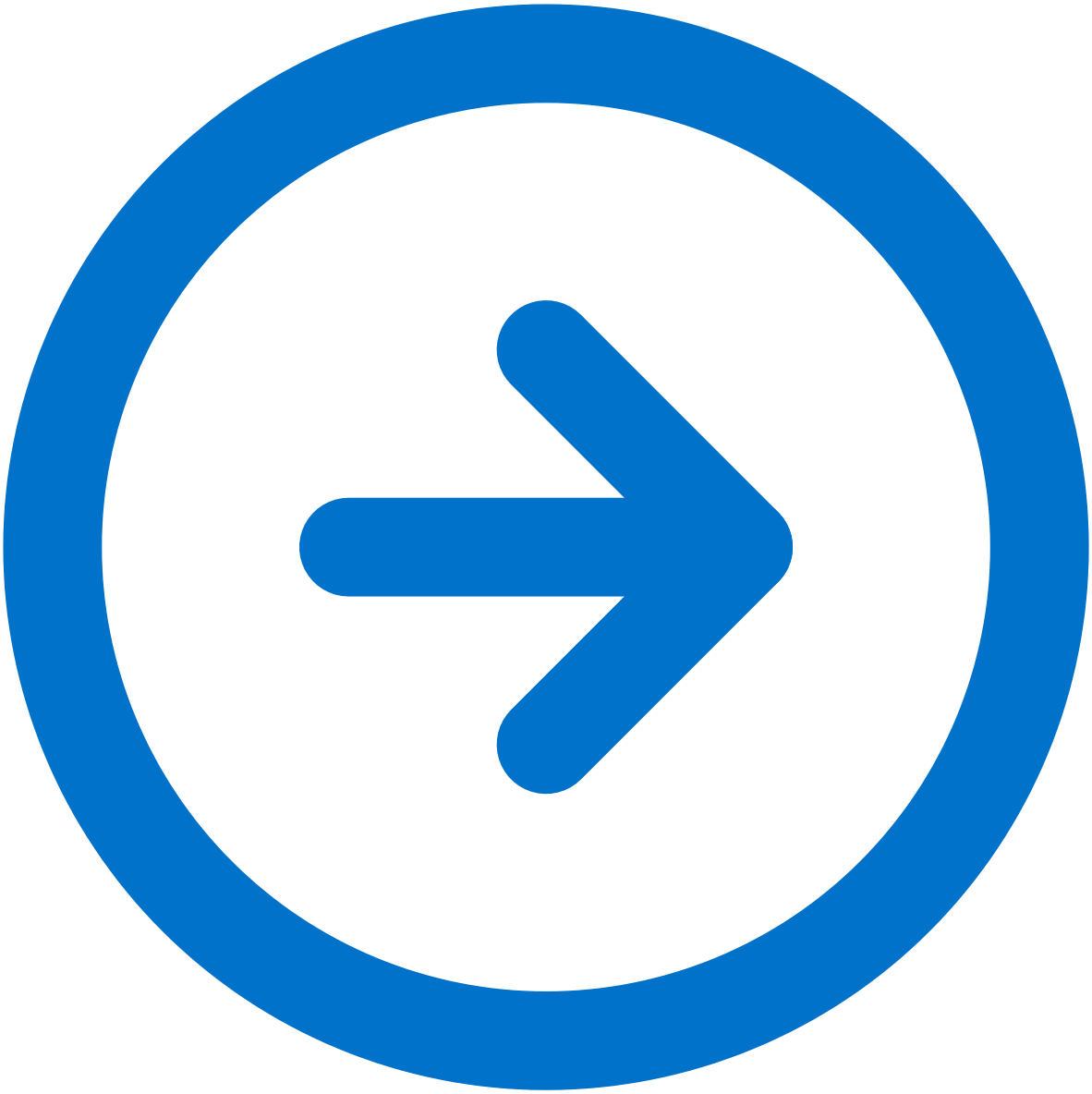
11. Keep special character rules in passwords

NIST says you don't have to worry about including uppercase letters, lowercase letters, or special characters (like !@#$%^) in your passwords. Why? These rules can lead users to create weaker passwords.

Instead of making secure passwords stronger, people often use the same old phrases and slightly tweak them for each website's requirements.

What's more important now is promoting longer and more secure passwords in today's tech world.

But don’t get us wrong, using special characters is still a good idea, especially when creating random passwords. The key is to not give strict rules and be more flexible about including special characters.



NIST recommendations for setting up passwords

Not every organization must follow NIST recommendations for setting up passwords, but many choose to do so voluntarily. These guidelines give you a solid foundation for managing your digital identities securely. Here’s a brief rundown of what they suggest as a part of your privacy controls:

- For user-generated passwords, aim for at least 8 characters; for machine-generated ones, go with at least 6 characters
- Always store passwords securely by hashing and salting them without cutting them off
- Don’t allow sequential characters (like “1234”) or repeated ones (like “aaaa”)
- Skip complexity requirements, like needing special characters or numbers
- Don’t use knowledge-based questions (like “Your first pet’s name”) for authentication
- Give users 10 tries before locking them out after failed login attempts
- Don’t let users use context-specific words, like the service name or their username, in their passwords. Keep it unique and secure

- Users should be free to create long passwords, up to 64 characters, using any ASCII/Unicode characters, even emojis and spaces
- Before accepting a password, check if it's been part of any data breaches and reject it if it matches
- Forget about password expiration dates; they're out
- Don't go to SMS for codes when using two-factor authentication (2FA); it's not the safest option
- Ditch password hints; they won't help

As a bonus, we have collated the NIST 800-53 Controls List to help you with the risk assessment. Take a look:

Download Your NIST 800-53 Controls List
First name*
Email*

- Are you currently evaluating cyber compliance automation?

NIST recommendations on password changes

NIST has a smart recommendation for businesses regarding password expiration and resets. Instead of forcing users to change their passwords frequently, they suggest doing it under two specific conditions.

- A password reset should happen when there's clear evidence of a security breach or a known compromise.
- Consider resetting passwords every 365 days, which is roughly once a year. The goal isn't to hassle users; it's to nudge them toward creating longer, more complex passwords.

What if the password gets compromised?

When the password is compromised, organizations should stop making users change their passwords arbitrarily, like on a set schedule. Instead, a password change should only be required when there's solid evidence that the password has been compromised.

When you change a compromised password, make sure you change all variations. And, whatever you do, never use that compromised password or any variation of it again. Because cybercriminals know that users often revert to their old passwords, they'll keep trying that compromised password, or variations of it, for years to come.

Need Help Implementing NIST Password Guidelines for Your Business?

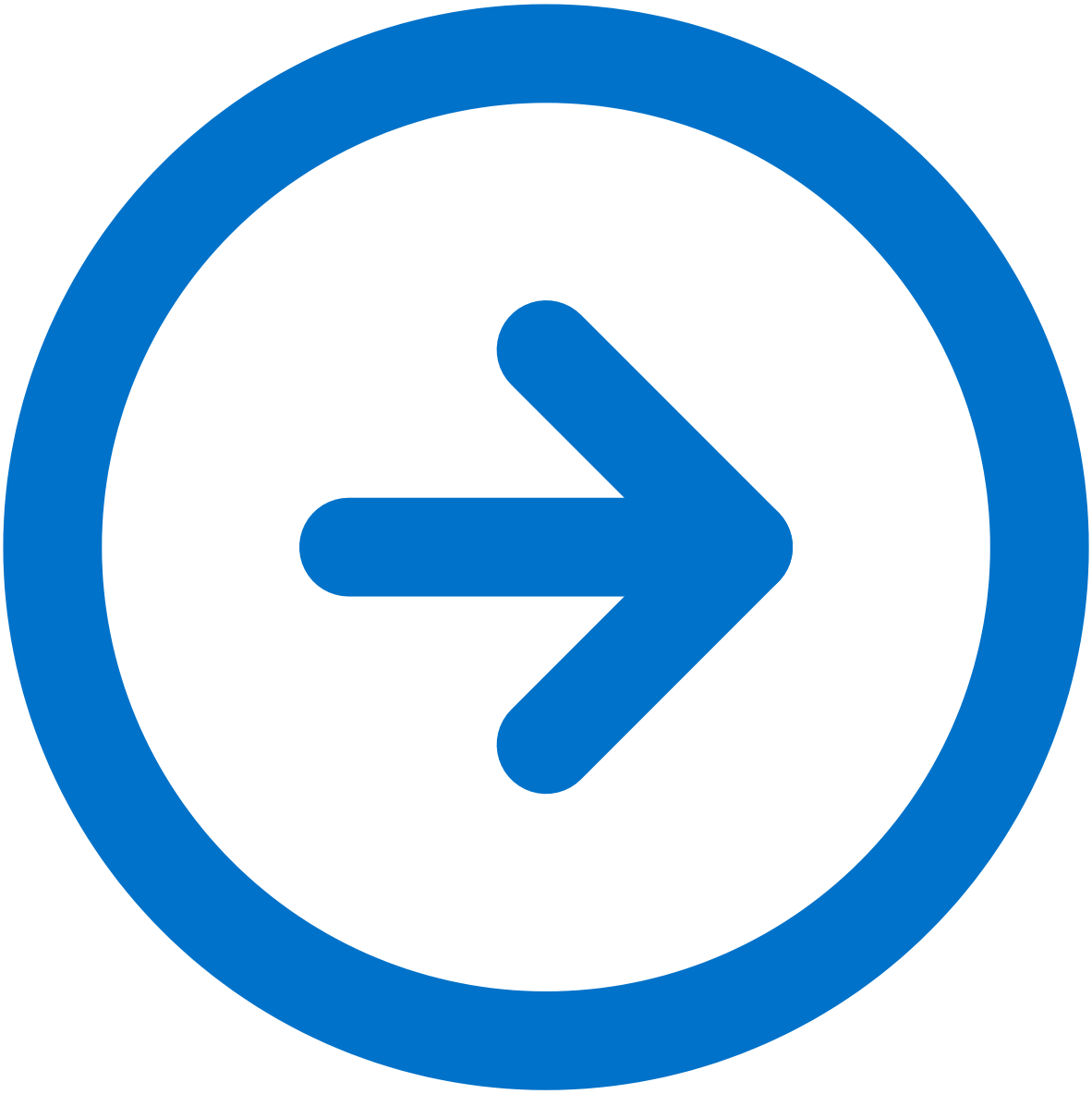
You're not alone if you're wondering how to implement NIST's password guidelines for your business. We know that balancing cybersecurity and regulations is a challenging task. But NIST upholds that strong security should enhance, not hinder, your progress.

That's where compliance automation software, like Sprinto, comes into play. It simplifies the process, helps your business follow best practices, and maintains a secure IT infrastructure.

However, having expert guidance from an actual expert will change your trajectory. Our clients at Sprinto have aligned their systems with the latest cybersecurity standards while keeping their focus

on core business progress.

If you're ready to take a step toward implementing NIST's password guidelines for your business.



Schedule a meeting with our security experts today.

FAQs

1. How safe is a 12-character password?

A 12-character password is extremely safe because they are impossible to guess for a person and is considered the best safeguard against threat actors. Combining lowercase letters, uppercase letters, numbers, and symbols will make it much better for you.

2. What are the password rules for NIST?

According to the password rules of NIST, user-generated passwords should be at least 8 characters, while machine-generated passwords can get away with 64 characters in length.

3. Does NIST require password expiration?

No, it’s important to note that NIST recommends resetting passwords only when necessary. While many organizations traditionally enforce a NIST password policy where passwords expire every 60 to 90 days, NIST diverges from this approach. NIST does not recommend password expiration as a general practice.

4. What is the strongest password?

The strongest password is one that includes numbers, symbols, and a mix of uppercase and lowercase letters. Avoid using common dictionary words in your password.