Summary of the NIST Password Recommendations

The National Institute of Standards and Technology (NIST) has created password guidance for federal agencies to ensure passwords achieve their intended purpose – preventing unauthorized account access. The NIST password recommendations were updated recently to include new password best practices and some of the long-standing best practices for password security have now been scrapped as, in practice, they were having a negative effect.

The NIST password recommendations are detailed in Special Publication 800-63B – Digital Identity Guidelines. The document is considered the gold standard for password security and must be followed by federal agencies, although the NIST password recommendations can – and should – be followed by all businesses when setting password policies, and by all individuals who want to ensure the security of their accounts and personal data.

Summary of 2021 NIST Password Recommendations

Special Publication 800-63B is 79 pages long, so to save you some time, we have provided a summary of the NIST password recommendations.

Password length is more important than password complexity

NIST has moved away from password complexity and now recommends longer passwords. Enforcing complex passwords that contain upper- and lower-case letters, numbers, and special characters will ensure strong passwords are created in theory, but in practice, these requirements result in weak passwords being created – Password123! for instance, would meet complexity requirements but is not a strong password. Instead, encourage the use of passphrases and set the maximum password field length at 64 characters. Password length, character for character, is more important than password complexity.

Do not enforce regular password resets

Humans are generally bad at creating passwords, so making employees change passwords regularly really doesn't help. What tends to happen is employees will create new passwords that are virtually identical to the last and will follow predictable patterns when creating new passwords that threat actors can guess. Alternatively, they will choose commonly used passwords or weaker passwords each time a change is required. Password resets should only be performed if it is suspected a password has been compromised.

Screen all new passwords against lists of commonly used and compromised passwords

It doesn't matter how complex a password is, if it is known by anyone other than the account holder it is not secure. You should screen all new passwords and ensure they are not included in lists of commonly used passwords, are not dictionary words, sequential strings of numbers or letters, and check they are not included in lists of passwords compromised in data breaches.

Allow the pasting of passwords

Preventing the pasting of passwords is hugely frustrating, especially when combined with password complexity requirements. It slows down account creation and logging in and encourages users to set weak passwords. By allowing the pasting of passwords, it means password managers can autofill the fields which makes life much easier.

Enable show password while typing

If a user types in a complex password and makes a typo, they will not know where the mistake has been made and will have to start again from scratch. If you allow passwords to be shown, it makes it much easier for users. They will be able to decide whether there is someone shoulder surfing and whether or not to display the password. Don't allow this and it encourages weak passwords to be created.

Limit the number of failed password attempts before account lockout

Brute force attacks to guess passwords are much more likely to succeed if there are no limits placed on the number of failed login attempts. By setting an account lockout after 3 or 5 failed password attempts, brute force attacks will be harder as the hacker will have fewer attempts to guess the password.

Implement 2-factor authentication

Make sure 2-factor is implemented on accounts. This requires an additional method of identification in addition to the password. If the password is compromised, in a phishing attack for example, without the other factor, account access will not be granted.

Salt and hash passwords

The NIST password recommendations now include a requirement to salt passwords with at least 32 bits of data and to ensure they are hashed with a one-way key derivation function.

The NIST password recommendations are a good basis for HIPAA compliance regarding passwords.