FALKLANDS IT

Best Practices for Password Policies

NIST Guidelines

The first line of defence in securing your data and systems against unwanted intruders is a robust password policy. The National Institute of Standards and Technology (NIST) offer digital identity guidelines

Password Complexity

Most organizations require that their passwords be a combination of symbols, with at least one number, lower- and upper-case letters, and one or more special characters. These types of requirements make the passwords much harder for the user to type and remember, and this leads to less than optimal security habits, including writing down the password, as well as more help desk calls for reset purposes. Post-it notes, some stuck to the screens, or notebooks are often found full of complex passwords.

In response, NIST does not favour strong password complexity but instead focuses on the length of the password. Something to keep in mind, however, is that offering a password manager to it's employees enables a business to keep its complexity requirements without having to sacrifice security or productivity.

Using a password manager to create, store and enter credentials makes it easier to enforce strong password management policies, since people do not need to even know their passwords.

Password Length

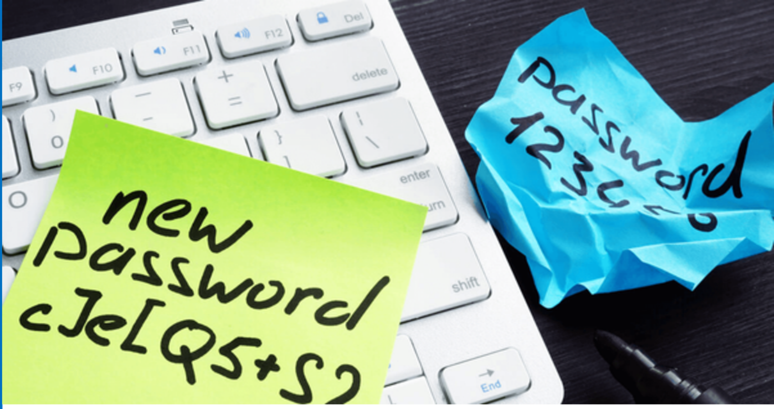
Password length is one of the most important factors in password strength. A long coherent passphrase is actually better than a short password that uses many types of characters, since short passwords can be guessed or cracked much faster.

long passphrases are easier to remember than short strings of gibberish, reducing the risk of users writing them down or suffering account lockouts. The NIST password length recommendations state that passwords should be at least 64 characters long.

Multi Factor Authentication

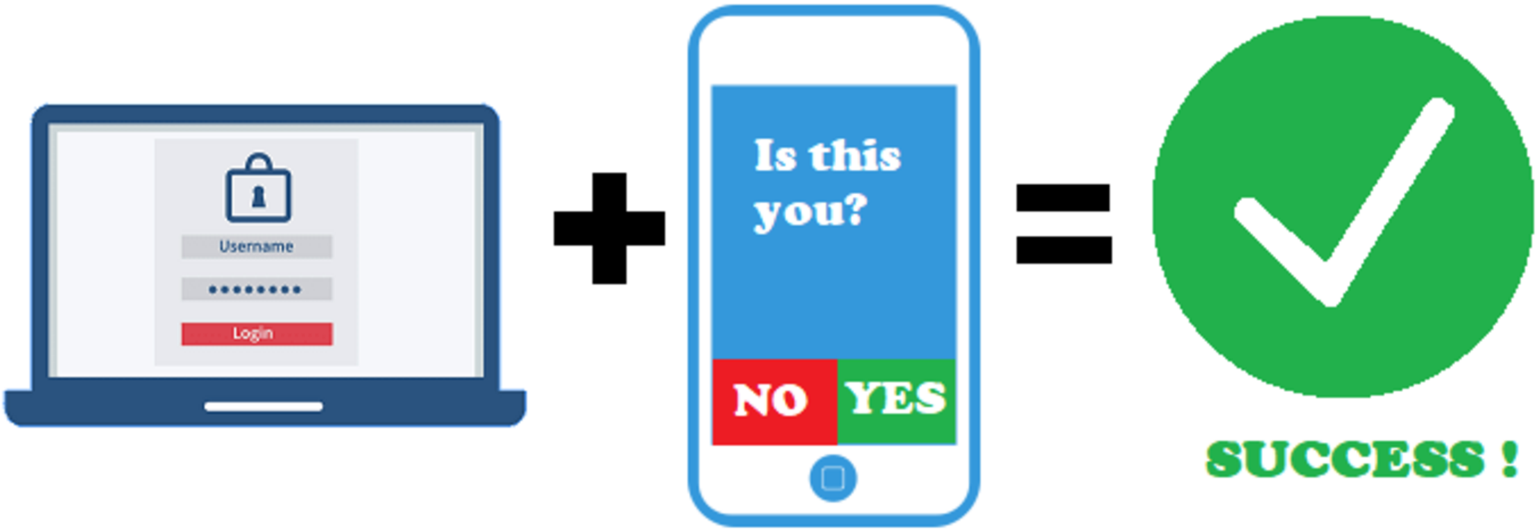
Implementing multi factor authentication (MFA) improves security by making stolen or cracked passwords far less useful to adversaries.

NIST recommends implementing MFA only when the company can use Google Authenticator, Microsoft Authenticator or another authentication process that doesn't involve SMS.



Password expiration

Previous NIST password change policy best practices recommended forcing users to change their passwords every 90 days (180 days for passphrases). Requiring users to change their passwords all the time can lead them to pick weak passwords or write their passwords down, which hurts your information security posture so NIST no longer recommend this. Instead, they recommend requiring user to create new passwords only in cases of suspected unauthorized access or breaches that result in personal credentials being published on the dark web, where they can be used in future cyberattacks.



Brute Force Attacks

A brute force attack is a hacking method where an attacker systematically tries every possible combination of passwords or encryption keys until they find the correct one. This attack is typically used to gain unauthorized access to accounts, systems, or encrypted data.

Types of Brute Force Attacks:

- Simple Brute Force Attack – Tries all possible passwords without any pre-defined list.
- Dictionary Attack – Uses a list of commonly used passwords or words to speed up the process.
- Hybrid Attack – Combines dictionary attacks with small modifications (e.g., adding numbers to common words).
- Credential Stuffing – Uses leaked username-password pairs from data breaches.
- Reverse Brute Force Attack – Starts with a known password and tries it on multiple usernames.

Passwords susceptible to brute-force attacks

- Easy-to-guess passwords, especially the string “password”
- A series of numbers or letters in order, like “1234” or “abcd”
- A string of characters in the order in which they appear on the keyboard, like “@#$%^&”
- The same character typed multiple times, like “zzzzzz”
- A user’s given name, the name of a partner or child, or other names
- Other information easily obtained about a user, such as their address, phone number, car registration, or family member’s birth date
- Words that can be found in a dictionary
- Default or suggested passwords, even if they seem strong
- Usernames or host names
- Any of the above followed or preceded by a single digit
- A new password that simply increments a number or character at the beginning or end of the previous password

For Password Users

- It is vital to remember your password without writing it down somewhere, so choose a strong password or passphrase that you will easily remember. If you use a password management tool, choose a strong master key and remember it.
- Be aware of how passwords are sent across the internet. URLs (web addresses) that begin with “https://” rather than “http://” are more likely to be secure for use of your password.
- If you suspect that someone else may know your current password, change it immediately.
- Don’t type your password while anyone is watching.
- Do not use the same password for multiple websites containing sensitive information

Best Practice for Password Policies

- Configure a minimum password length.
- Enforce password history policy with at least 10 previous passwords remembered.
- Set a minimum password age of 3 days.
- Require passwords to meet complexity requirements. This setting can be disabled for passphrases, but it is not recommended.
- Reset local admin passwords every 180 days.
- Reset service account passwords once a year during maintenance.
- For Domain Admin accounts, use strong passphrases with a minimum of 15 characters.
- Create email notifications for password expiration.
- Instead of editing the default settings in domain policy, create granular password policies and link them to specific organisational units.
- When employees leave the organization, change the passwords for their accounts even if you disable the accounts.
- Enterprise applications must protect stored and transferred passwords with encryption to help keep hackers from cracking them.