Authentication and Password Policy

Purpose

This policy describes <Company Name>'s requirements with regards to account authentication, including how passwords should be generated, used, and protected.

Scope

The policy applies to all employees and contractors, and the accounts they use in connection with fulfilling their responsibilities to <Company Name>.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

The overall intent of the policy is to ensure that employees use strong credentials, leverage Single Sign-on (SSO) to reduce the need to maintain one set of credentials for each system, store them securely, and use Multi-factor authentication (MFA) at least for the most sensitive systems.

Single sign-on (SSO)

The company leverages SSO authentication for sensitive systems, wherever available.

<Company Name>'s main Identity Provider is used as its SSO provider.

SSO usage reduces risk by centralizing authentication requirements and enforcement points. It improves employee productivity by reducing the number of credentials they must manage.

Multi-factor authentication (MFA)

Access to sensitive systems requires multi-factor authentication.

Multi-factor (or two-factor) authentication (MFA) has been designated as the preferred method of authentication by NIST (800-63 Digital Identity Guidelines https://pages.nist.gov/800-63-3/) since 2017. MFA strengthens security by requiring at least one additional factor, in addition to a password, to verify identity. The additional factor is something the user has (such as their phone) or something they are (such as their fingerprint). Since a password is no longer the only means of authentication, and since these other factors are inherently different in nature from memorized secrets, MFA significantly increases the difficulty bar for executing a successful attack. In addition, by not relying solely on password verification for authentication, MFA eliminates the need for periodic password rotation and reduces password fatigue.

Multi-factor authentication is, at a minimum, required for all systems classified to contain sensitive data as per the Data Classification Policy, and strongly recommended for all other systems.

MFA support is a requirement for the adoption of new systems expected to store sensitive data.

For systems storing customer PII and other regulated data, MFA must be enforced: users should not be able to disable the second factor and retain access to these systems, and access to these systems without a second factor should not be possible.

Password management tool

All users with privileged access to sensitive systems are required to use a password management solution.

Password management software improves both convenience and security. A master password is more likely to be long and unique, since only that password needs to be remembered in order for the user to gain easy access to all their other other accounts and passwords.

In addition, password managers facilitate generating and using passwords that are unique for each account and significantly stronger than those the typical human can remember.

A user's master password should be memorized and never recorded or shared. Since a password management system is only as secure as the master password used to unlock it, this password should be as long as possible, and should never be reused.

Some password managers also allow secure sharing of credentials, for cases where unique credentials are not required or available. While unique credentials are always preferred, using these sharing mechanisms is encouraged over sharing credentials through other, less secure channels.

Unique User IDs

Individual accounts are required for access to systems storing or processing sensitive information. Unique IDs allow for granular, least-privilege access which minimizes the impact of any single compromised user account. They also improve accountability since every action in an audit trail can be directly associated with a unique individual.

User IDs and passwords are used to control access to <Company Name> systems and may not be disclosed to any other employee for any reason.

Sharing of credentials is only permitted for systems storing data with low sensitivity as per the Data Classification Policy, or upon the explicit approval of the Security Officer. Access must still be restricted to the smallest teams and there must be an established business needs. Any shared credentials must be rotated upon the departure of any employee in the share group. Sharing is best done using a Password Management system or a secure password vault.

Password Configurations

Password configuration settings are managed in compliance with the company's Password Policy.

Strong passwords are defined as:

- Having minimum length of 12 characters, maximum length not shorter than 64 characters.
- Containing multiple character types, such as numbers, uppercase, lowercase, and special characters, though these are not required and should not be enforced, and longer passwords are preferred over more complex ones.
- "Longer is stronger". While special characters increase the strength of a password, length is ultimately the biggest contributing factor to its quality. Longer passwords have a greater number of possible combinations, thus making them harder to brute-force.
- Not appearing in a list of commonly-known weak passwords. One such list is maintained at https://cry.github.io/nbp/.
- Not having been previously used in this or any other systems. Systems should keep a history of previous password and disallow reuse; please refer to the Encryption Policy for details on how these can be securely stored and accessed.
- Not containing easily discoverable personal information such as birthdays, addresses, phone numbers, family names, pet names, friend names, company name, company slogans, co-worker names and favorite popular characters.
- Not containing personal information specified above with common modifications such as substituting '1' for 'i', '0' for 'o', or '@' for 'a'.

Strong passwords are required for all systems classified to contain sensitive data as per the Data Classification Policy, and strongly recommended for all other systems.

The ability to enforce or monitor for strong passwords is a requirement for the adoption of new systems expected to store sensitive data.

Password handling

Password storage must be encrypted. Passwords should not be written down physically (in notebooks, sticky notes, etc) or be stored unencrypted on any device.

Passwords must not be emailed or sent via other messaging and communication methods. Initial passwords for new accounts are exempt from this rule, but must be changed by the new account holder on first use, as detailed below.

Passwords submitted for authentication purposes must only be transmitted via encrypted channels.

Passwords may not be reused across multiple accounts, including between personal and work accounts. Any reused passwords increase the impact of a single compromised account.

Users who believe their account has been compromised are required to immediately reset their password and promptly report the incident to the Security Officer. Breached credentials must be changed and never used again.

In systems where a password is automatically generated upon account creation or password reset, the user is required to change their temporary password to a permanent one upon first login. To reduce the risk of a complete set of temporary credentials falling into the wrong hands, each part of the credential (password, email, username, etc) must be communicated out-of-band and in a separate channel.

Any pre-existing default passwords must be changed upon first use.

To mitigate the possibility for brute force attacks on passwords, systems must lock accounts after 3 failed authentication attempts.