PathwAI

# Password Policy

Version 1 - Approved by Abdullah Adeeb

# Password Policy

Most systems authenticate their users by a username + password combination. The passwords used here are secrets and must be managed with care to ensure they do not create security risks.

## Passwords are vulnerable

Passwords are shared secrets, and as such inherently vulnerable. Authentication methods that rely on shared secrets are less secure than ones that do not.

As a result, the best strategy is to minimize the use of passwords wherever possible. Please follow the guidelines below when using passwords to authenticate yourself with various systems

1. Use a single-sign-on mechanism to authenticate yourself wherever possible. This avoids the need to create new strong passwords. Please ensure that the password/authentication mechanism for the SSO system is secure.
2. Use multi-factor authentication (MFA) techniques to authenticate yourself wherever possible. This reduces the reliance on passwords and adds an additional barrier even if the password is compromised.
3. Unfortunately, passwords are still the most common and popular way to authenticate, and there will be scenarios where you will not be able to apply 1 or 2 above. In such cases, please use the following guidelines.

## Password Generation and Strength

1. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to critical data. A strong password should consists of at least 10 characters and should be randomly generated from an alphanumeric + special characters character set.
2. Complex passwords can be achieved in a couple of ways:
    1. Recommended: Generated by password managers
    2. An alternate strategy: Use a passphrase consisting of 5 or more dictionary words. This may be easier to remember while being equally hard to guess via brute-force. https://medium.com/peerio/how-to-build-a-billion-dollar-password-3d92568d9277#67c2
3. We strongly recommend against reusing passwords that are or were used elsewhere, e.g. passwords used for personal accounts. A common way attackers obtain access to corporate resources is by using employees' personal passwords that were obtained in breaches of other services.
4. To avoid creating and maintaining a large number of complex passwords, use "Login with Google Workspace", "Login with O365" or any other OAuth provider wherever feasible.
5. Enable multi-factor authentication in your accounts wherever it is available as a feature. For critical services, using multifactor authentication is mandatory.

## Non-Compliance

PathwAI Labs staff who violate this policy may face repercussions in proportion to the impact of their violation. PathwAI Labs management will determine how serious a staff member's offense is and decide the appropriate penalty. Penalties may include a warning (oral/written) or suspension or termination for more serious offenses.

## Questions

If you have any questions regarding this policy, please reach out to the policy owner.

---

End of Password Policy.For version history, please see the next page.

# Version History

| | Version | Log | Date |
|---|---|---|---|
| 1 | Current | Policy version approved by Abdullah Adeeb | 02 Dec, 2025 |
| 1 | | New policy version created | 02 Dec, 2025 |