# **Password Policy**

Sumary

[**Password Policy** 1](#_Toc109898301)

[**Introduction** 3](#_Toc109898302)

[**Scope** 3](#_Toc109898303)

[**Policy Statements** 3](#_Toc109898304)

[**Policy for constructing a password** 4](#_Toc109898305)

[**Password Protection Standards** 5](#_Toc109898306)

[**Password Deletion** 6](#_Toc109898307)

[**Roles and Responsabilities** 6](#_Toc109898308)

[**Password Vault** 7](#_Toc109898309)

[**Benefits of Using a Password Vault** 7](#_Toc109898310)

[**Solutions** 8](#_Toc109898311)

[**Additional Information - Tools** 8](#_Toc109898312)

## **Introduction**

This policy ver1.0 released 27 July, 2022 instructs all parties involved, including the program manager, data owner, information system owner, IT asset management team, vendors and other employees, to adhere to the standards specified in this document for creating secure passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

## **Scope**

The scope of this policy includes all end users and employees

who own or are responsible for an account (or any form of access that

supports or requires a password) on any system/service. This includes your desktop and third-party systems.

## **Policy Statements**

For users having accounts for accessing systems/services

Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.

All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every 45 days). Users shall not be able to reuse previous passwords.

Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.

All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.

All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.

Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.

Passwords shall not be revealed on questionnaires or security forms.

Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.

The same password must not be used for each of the systems/applications to which a user has been granted access, for example a separate password to be used by a Windows account and a UNIX account must be selected. The same thing applies to third-party and ERP systems.

The "Remember Password" feature of applications shall not be used.

Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

First time login to systems/services with administrator created passwords, should force changing of password by the user.

If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

For designers/developers of applications/sites

No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.

The backend database shall store hash of the individual passwords and never passwords in readable form.

Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

Users shall be required to change their passwords periodically and not be able to reuse previous passwords.

For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

## **Policy for constructing a password**

Be a minimum length of eight (8) characters on all systems.

ii. Not be a dictionary word or proper name.

iii. Not be the same as the User ID.

iv. Expire within a maximum of 45 calendar days.

v. Not be identical to the previous ten (10) passwords.

vi. Not be transmitted in the clear or plaintext outside the secure location.

vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized user.

Strong passwords have the following characteristics:

• Contain both upper and lower case characters (e.g., a-z, A-Z)

• Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&\*()\_+|~-

=\`{}[]:";'<>?,./)

• Are at least eight alphanumeric characters long.

• Are not a word in any language, slang, dialect, jargon, etc.

• Are not based on personal information, names of family, etc.

• Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, something totally random or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" other example “D0ll1nH0@2! or some other variation.

## **Password Protection Standards**

Do not use your User ID as your password. Do not share [agency name] passwords with anyone,

including administrative assistants or secretaries. All passwords are to be treated as sensitive,

Confidential [agency name] information.

Here is a list of “do not’s”

• Don’t reveal a password over the phone to anyone

• Don’t reveal a password in an mail message

• Don’t reveal a password to the boss

• Don’ talk about a password in front of others

• Don’t hint at the format of a password (e.g., “my family name”)

• Don’t reveal a password on questionnaires or security forms

• Don’t share a password with family members

• Don’t reveal a password to a co-worker while on vacation

• Don’t use the "Remember Password" feature of applications

• Don’t write passwords down and store them anywhere in your office.

• Don’t store passwords in a file on ANY computer system unencrypted.

## **Password Deletion**

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

• When a user retires, quits, is reassigned, released, dismissed, etc.

• Default passwords shall be changed immediately on all equipment.

• Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed (See User Account

Access Validtion Policy for additional information/requirements):

• Employee should notify his or her immediate supervisor.

• Contractor should inform his or her point-of-contact.

• Supervisor or POC should fill out a password deletion form and send it to Privacy and Security Team.

• The company responsible for the PoC will then delete the user’s password and delete or suspend the user’s account.

• A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.

• The password deletion form will be filed in a secure filing system.

## **Roles and Responsabilities**

All individual users with access accounts in systems/services, in addition to system and network access, must ensure the implementation of this policy.

All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

Personnel authorized as Internal Audit must periodically review the adequacy of such controls and their compliance. Auditing passwords and brute force attacks on registered system accounts.

Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.

## **Password Vault**

A password vault, password manager or password locker is a program that stores usernames and passwords for multiple applications securely, and in an encrypted format. Users can access the vault via a single “master” password. The vault then provides the password for the account they need to access.

A password vault is a key element of Privileged Access Management (PAM). It is ideal for organizations that need to securely protect user accounts in a centralized manner. The application is user-friendly, since users don’t have to remember multiple passwords. It also helps enforce password best practices, and protects the enterprise from outside threats.

PAM is best-suited for enterprises that need to monitor, manage and protect privileged accounts. PAM isolates the control and use of privileged accounts with granular Role-based Access Control (RBAC) to minimize the risks of accidental or malicious credential misuse. PAM also enables organizations to automatically create audit logs, and meet the compliance requirements set forth by GDPR, ISO/IEC 27001, etc.

### **Benefits of Using a Password Vault**

Safely store enterprise passwords. A password vault is a secure way to manage and store enterprise passwords. Some vaults can auto-generate strong, secure and unique passwords to protect applications.

User-friendly. Users don’t have to remember multiple passwords to log into multiple accounts, just the one strong master password that unlocks the vault.

Prevent account compromise and data breaches. Passwords are randomly generated, making them much more difficult to hack, and protecting accounts from credential abuse or breaches.

Easy password resets. It’s easy to reset or change passwords if an account is hacked or if a password is compromised.

Multiple login methods. Some password vaults include built-in multi-factor authentication (MFA), so even if the user forgets their master password, they can still log into the vault via a one-time password (OTP), a fingerprint, etc.

Threat alerts. Certain vaults alert users about potential phishing attempts, so they can avoid clicking on malicious links or downloading malicious attachments in spoofed emails.

Sync across devices. Some password managers sync credentials across multiple operating systems and devices, further simplifying the login process.

### **Solutions**

Linha do tempo

Descrição gerada automaticamente

Keeper Security - <https://www.keepersecurity.com/pt_BR/>

Dashlane - <https://www.dashlane.com/pt-br/>

1Password - <https://1password.com/>

Hitachi ID - <https://www.hitachi-id.com/>

Lastpass - <https://www.lastpass.com/>

Manage Engine - <https://www.manageengine.com/>

Nordpass - <https://nordpass.com/>

Bitwarden - <https://bitwarden.com/>

N-Able - <https://www.n-able.com/pt-br>

Delinea - <https://delinea.com/>

## **Additional Information - Tools**

<https://haveibeenpwned.com/> - Have I Been Pwned allows you to search across multiple data breaches to see if your email address or phone number has been compromised