Implementing a Password Manager: Policies & Best Practices

You've decided on a password manager - now what? This worksheet compiles password management best practices compiled from digital security experts, so you can confidently implement a password manager at your organization.

1. Questions to prepare for implementation

Explore the password manager administration settings and see if you can:

- Recover master passwords or accounts for users
    - How does an admin recover an account?
    - Can you designate an emergency contact who will be able to recover your admin account?
    - If the administrator cannot recover accounts if a user loses their password, how will user account passwords be safely backed up?
        - Printed & stored in a locked filing cabinet?
        - Printed & stored in a safe deposit box?
        - Placed in an envelope and given to a friend?
            - If the printout does not have the login username or name of the person who it's for, this can be a relatively secure option.
        - Divided in half, with each half given to a trusted contact?
- Force users to re-enter their master password:
    - Every 24 hours
    - At the start of a new browser session
- Require a minimum password length for:
    - Master passwords
    - Generated passwords
- Explore password auditing features
    - Familiarize yourself with the reporting features
- Keep logs on user activity
    - How often users log in, from which IP address, etc.
        - This will help if you ever need to investigate a suspicious login.
- Force logout/force the end of user sessions
    - This will be useful if anyone loses a device that they were logged into their password manager on.

2. Sample account & password policy

Adapted from SDA (Safe and Documented for Activism)

Once you are familiar with all the features of your password manager above, you're ready to establish policies to guide your rollout. You can adapt and build off of these sample policies.

Administrator will create and manage all accounts

All services that all multiple users will be administered by an administrator account. The administrator will create separate accounts for administration duties and for all other business.

Authorization to create new accounts must always fall to a person different from the one who has administrative access to the service and performs the creation of accounts.

Implementation of the principle of minimum privilege in the creation and configuration of user accounts

To manage the user accounts in the computer systems of the organization, the principle of minimum privilege will be followed, which imposes a system of access and permissions that enables users to have access to only that information and actions on it that are strictly necessary to carry out by their role or position. The action of enabling any user account to perform actions or access information that does not need to fulfill its functions is prohibited.

Use of administrative accounts

It is forbidden to use administrative accounts for activities other than those of the administration of systems and tools. In those cases, in which a member of the organization must use a system in which only has administrative account, you can create a secondary account with less privilege to do processes of daily operations, using the administrative account as little as possible and applying as many additional security measures in this as possible and relevant.

Mandatory use of individual accounts

Unless stated otherwise, all user accounts of computer systems in the organization are for individual use, and the sharing of user accounts is prohibited.

In those cases where it is necessary to share user accounts (for example, social networks of the organization), particular security measures will be established to avoid as far as possible those security vulnerabilities that come with the sharing of user credentials.

Mandatory use of institutional password manager

Passwords will be stored in the institutional password manager. Storing passwords elsewhere is prohibited.

If you have been using a browser-based password manager, you can find instructions for exporting and deleting password data and turning off password saving prompts here:

- Guide from 1Password to disabling password prompts for all operating systems and browsers: https://support.1password.com/disable-browser-password-manager/
- Chrome: export, delete, and disable passwords
- Firefox: exporting passwords, deleting passwords, disabling password manager

After importing passwords into the institutional password manager from a browser-based password manager, the file must be deleted from the desktop and the trash folder immediately.

Device security for use of password manager

Any device with the password manager installed must be protected by a unique PIN or password. The device must automatically logout after a certain period of time.

Devices logged into the password manager should not be shared. If you must log into the password manager on a shared device, you must log out of the password manager immediately after logging into the necessary accounts.

Password Guidelines

Passwords	Practices/general security recommendations...
Repetition	• It is strictly forbidden to repeat passwords between services or devices, all passwords managed by the members of the organization must be different, in addition to complying along with the other directives of this document.
Master passwords	• The master password for the institutional password manager must be at least 4 words and at least 20 characters. • The master password may be written down for the first week of use. After the first week, the written copy of the master password must be destroyed (shredder & placed in the trash). • The administrator will share backup and recovery procedures for master passwords.
Automatic logout	• The password manager will be configured so that users have to re-enter their master password every 24 hours or when a browser session is re-started, whichever is soonest.
Existence of physical copies	• It is forbidden to have physical copies of passwords anywhere, periodically checking: ◦ Notebooks ◦ Billboards ◦ Monitors ◦ Keyboards ◦ Post-it blocks

Password generation	• All web-based services must have passwords generated and handled by password managers, ensuring that the length, complexity and non-repetition specifications set forth in this document are met.
Length	• Passwords must be at least 16 characters in the services that allow it. • When generating a password using the password manager, aim for a length of at least 30 characters.
Complexity	• If passwords are less than 16 characters (only permitted when password length is limited by the service), they must contain uppercase, lowercase, numbers, and special characters. • There is no special requirement of complexity in the use of characters provided that the passwords are more than 16 characters. • Use of one word for the password is prohibited, as well as one name, even if the word or name is longer than 16 characters.
Expiration	• There is no expiration time of the passwords configured in devices or services of the organization. It is only required to change them when a user is offboarded or when there is suspicion of a compromise of the user account, the corresponding service or a device.
Sharing	• All user accounts of computer systems in the organization are for individual use, and the sharing of user accounts is prohibited, except where absolutely necessary (for example, Twitter account). • If a password must be shared, it will be shared in the password manager.

Sources:
Cybersecurity Campaign Playbook by the Belfer Center
SDA: Safe and Documented for Activism
Before You Use a Password Manager by Stuart Schechter

Additional resources:
https://usesoap.app/ - develop brief & easy to understand security policies for your organization