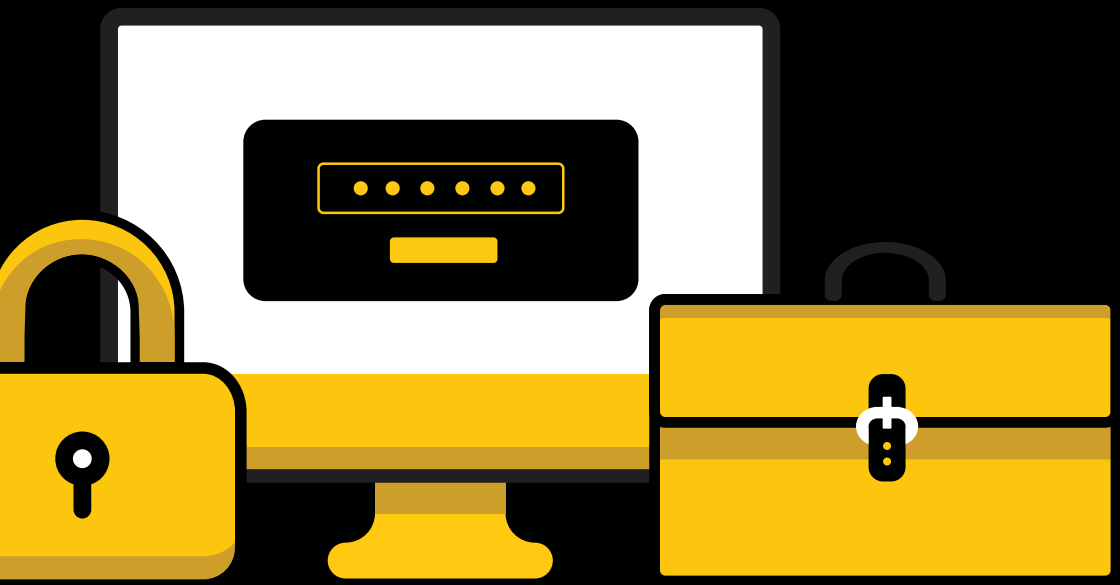


KEEPER®
Cybersecurity Starts Here™

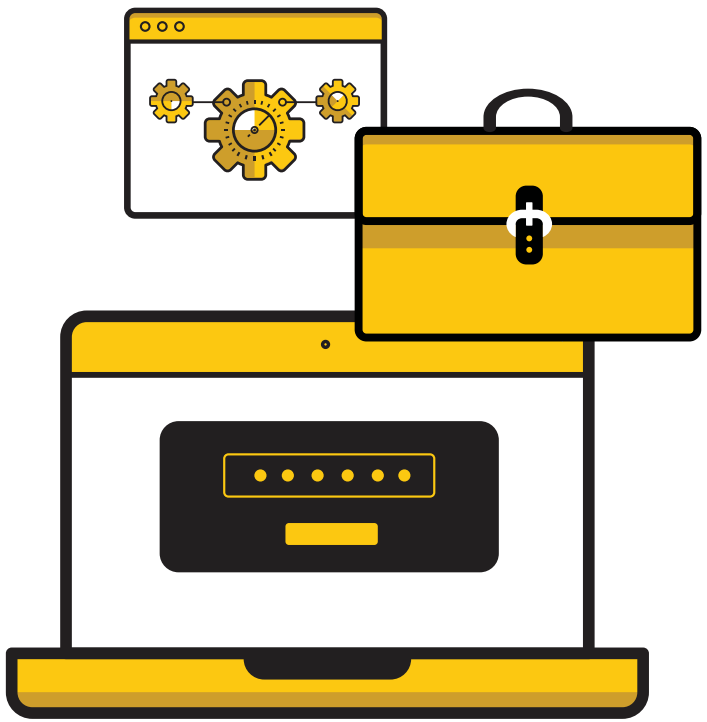
Password Security Best Practices for **Business**

Table of Contents

Password Security Standards & Policies for Business

Organizations spend millions of dollars on cybersecurity defenses and consultants. Beyond traditional tools like firewalls, anti-virus, and system information and event management (SIEM), it is easy to get caught up in sophisticated threat detection using artificial intelligence, machine learning, user behavior, and analytics. All of these tools have their place and are very valuable; however, one problem looms large:

Passwords are frequently the only thing protecting confidential business plans, intellectual property, communications, network access, employee census information and customer data. Due to human error, negligence, and simple lack of knowledge, passwords are the weakest link in security. Attacking those issues head on will provide maximum return on investment.



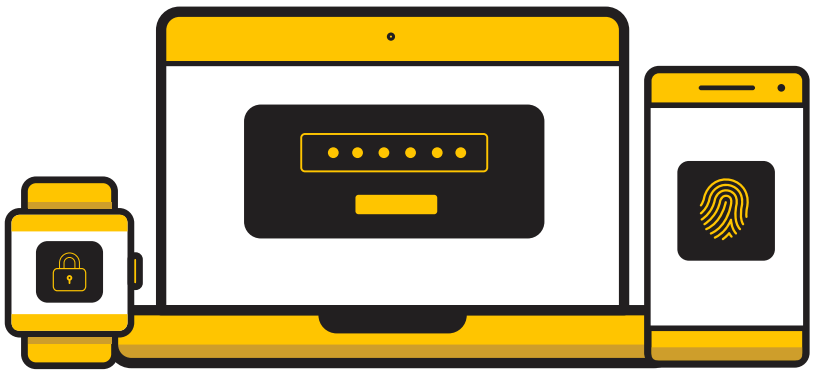
Go to Table of Contents

Implementing a Password Security Policy - A Two Step Process

The first step in virtually every cybersecurity framework is to take an inventory of your assets and then determine the risk of losing each of those assets.

The second step is to implement policies according to the risk levels assigned to those assets. The most critical part of these policies is access control.

Given that passwords will be an integral part of any access control policy, password security policies must be put into place. An effective password security policy entails making sure employees create strong passwords, do not reuse them, store passwords on authorized company devices, and implement 2FA. Using a password manager to store passwords for all applications is the only way this can currently be accomplished.



Use Two-Factor Authentication (2FA)

Passwords are your first authentication factor and should always be reinforced by using 2FA. 2FA enables you to strengthen access to your account by using two different forms of authentication methods to access an account or service. Keeper supports multiple 2FA programs including SMS, TOTP (Google Authenticator, Authy), FIDO U2F (YubiKey), Duo and RSA.

Enforcing Your Password Management Policy & Procedures

Most businesses have limited visibility into password practices of their employees which greatly increases cyber risk. 90% of employee passwords can be cracked in six hours or less making them a businesses number one internal security risk. The easiest way to improve employee password hygiene is though critical insight into password usage and compliance.

The ability to enforce policy controls, define access roles, and restrict sharing is critical for safe enterprise password management. Limiting employee access to a need-to-know basis ensures that employees only have company resources and logins that they need at the times that they need it. Assigning a delegated admin that is regularly monitoring, provisioning and deprovisioning access to users based on their role is highly recommended.

How Keeper Increases Compliance

Keeper provides comprehensive password reporting, auditing, analytics, and notifications through the Admin Console. By using the Keeper Security report in the admin console, security professionals can see employee password strength, password reuse, and two-factor authentication status. Access logs to Keeper vaults can be audited for compliance or forensics.

How Keeper Helps Enforce Password Management Procedures:

Master Password Complexity
Ensure employees utilize a strong master password to access their account.

Master Password Expiration
Schedule updates to master passwords.

Password Masking
Share passwords and permit their use by employees but prevent viewing or copying of the password. Keeper autofills passwords without revealing them.

Biometrics
Enforce use of biometrics when available.

2FA Enforcement
Define which authentication methods and vendors need to be utilized to access Keeper accounts.

Platforms Allowed
Define specific platforms allowed to access Keeper accounts. For example, only permit a specific browser.

Password Sharing and Exporting
Set Team permissions and define the organizational structure for sharing passwords and folders. Control exporting of vault contents.

IP Whitelisting
Prevent employees from accessing their Keeper account from outside the office

Logout Timers Across Platforms
Set limits from one to thirty minutes to automatically logout an employee.

How Keeper Protects Your Information

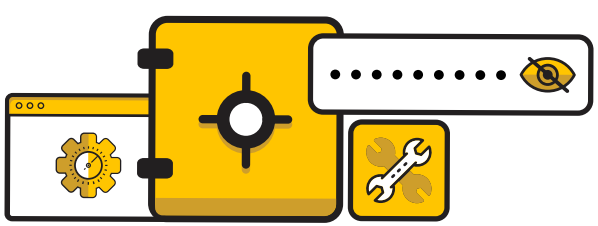
Keeper is a Zero-Knowledge Password Management solution. This means all information stored in Keeper is only accessible by the end-user. To access this information, users must enter their master password, the only password they need to remember. All information stored on Keeper is encrypted both in-transit (TLS) and at rest on Keeper's Infrastructure (AES-256.) The plaintext version of the data is never available to Keeper Security employees or any outside party.

Keeper uses the most advanced versions of cryptography available - PBKDF2, TLS and AES-256. Our systems are SOC 2 Type 2 audited and compliant.

Are Passwords Going Away?

A common misconception is that biometrics, such as fingerprint, iris or facial scans, can be used to eliminate traditional passwords. **Reasons why passwords are here to stay:**

- Touch ID is convenient but only as secure as the password or PIN associated with it.
- Despite most mobile devices adapting biometrics, a complete organization deployment means scanners have to be deployed to every computer and appliance and then be connected to a central authentication system. Integration and ongoing maintenance costs make this option cost-prohibitive.
- Biometrics can't be changed, so if the corresponding file is ever compromised, then the user has to revert back to passwords.
- Biometric files have to be accessible by the service provider. This means collecting and storing employee biometric files and/or providing them to vendors such as Google, Salesforce, Workday and more. That is a huge liability that no one wants.



Biometrics remain a great option to use in conjunction with passwords when strong (two-factor) authentication is required, but passwords are here to stay.

Save Time and Money

A password manager provides the most rapid ROI of any security measure your business can implement. Employee password habits are the greatest risk to security and Keeper is your best bet at modifying that behavior.

With Keeper, every employee is provided a vault to store passwords and sensitive information. Keeper generates strong, random passwords, and autofills them for users. This saves time and frustration and eliminates the need to reuse and remember multiple passwords. Keeper is accessible to employees from any device. This increases organization and password security and drastically decreases helpdesk calls.

A Gartner study showed that up to 50% of helpdesk calls center around password resets and that each call costs an average of $31. Forrester found that several large companies have allocated over $1 million annually for password related support.

Keeper Solution

Whether for personal or business use, our state-of-the-art password management system makes it easy for users to manage and store all of their passwords on a single and secure platform.

Join thousands of businesses using Keeper to protect vulnerable entry points to your business by improving password behavior and security.

For more information about our innovative password management solution, contact us today to **start a free trial** and **request a demo.**

For more information on Keeper for Business
visit **keepersecurity.com/business**