RESOURCE CENTER

A Guide to Enterprise Password Management Throughout the Employee Lifecycle

Get the full interactive view at https://bitwarden.com/resources/guide-enterprise-password-management-throughout-employee-lifecycle/

bitwarden

Defining the Employee Lifecycle for Password Management

New types of security challenges, or exploits to mitigate, arise every day, leading to a constantly evolving information technology (IT) stack. Fortunately, select security tools can easily integrate into your company's existing stack while improving employee productivity and security.

When adding new tools to your roster, consider how you will manage access throughout the employee lifecycle. For example, a new employee should gain access to specific systems from day one, and others may be introduced later. At the other end of the spectrum, access must be revoked immediately for a terminated employee.

Comprehensive password management enhances company and individual security and fosters collaboration and enhanced productivity. This guide illuminates how password management touches each stage of the employee lifecycle.

Stages of the Employee Lifecycle

Password management touches nearly every single part of your business and is most significant during three major stages of an employee's lifecycle.

- Onboarding
- Succession and Promotion
- Offboarding

Onboarding New Employees

From granting access to corporate and departmental systems, setting new employee milestones, or scheduling training, effective onboarding takes time and attention. Onboarding new employees efficiently speeds integration and helps the business deliver faster results.

In larger companies, human resources and IT teams might grant access to enterprise-wide systems, including options for Single Sign On (SSO) to select services. However, the universe of employee credentials often goes far beyond those within such systems. Also, mid-size companies may not have implemented an SSO system and have an even greater need for employees to get started with the proper digital security practices.

From the new employee's perspective, accessing and setting up the necessary software or applications without the right tools can cause friction and confusion, leading to poor practices. In the absence of a secure process, such as a password manager, sharing log-in credentials with new employees is often managed using at-risk methods, such as email or messaging apps.

The pressure to be successful at work, both for the individual and the team, often means co-workers are going to share necessary log-in information with one another; it's just a matter of whether or not they are enabled to do so safely.

A recent survey of IT decision-makers revealed nearly 60% of teams would share company passwords to colleagues through unsecure methods, despite the risk. And 80% of IT decision-makers want to mandate the use of an enterprise-wide password manager, with practicality being a major reason. Another critical factor is a password manager emphasizes data security as better password practices reduce risky behavior.

Introducing a password manager early in the onboarding process drives adoption and minimizes the friction of accessing new systems.

Succession and Promotion

Scaling your business also demands flexible technology for growth—including password management. Expansion might include increasing team sizes, creating new roles or departments, or acquisitions.

Sometimes existing employees will move into new roles, which might require a transition in software ownership or updating user access levels. With a password management system in place, moving transitioning employees into new groups with new shared folders or updating role access could just take a few clicks.

For one law firm, RMWBH, Attorneys and Counselors at Law, this often happens when managing a large caseload across attorneys and paralegals.

If one paralegal is working on a case with a huge trial date coming up, they can pass it off to the next paralegal without bothering the original user. Managing over 10,000 passwords is automated across a series of shared folders that enable automatic distribution, taking the process time down from days to just hours

Table of Contents

Offboarding Employees

When employees leave a company on their terms or through termination, the offboarding process includes concluding or transitioning projects and turning off system access.For some companies without a password management system, someone might change the passwords to all shared log-ins upon an employee's last day. Maybe this includes updating a spreadsheet of log-in credentials and sharing with other team members needing access. This can be compromising as unencrypted spreadsheets and shared documents lack the security and fine-grained access control to manage passwords.Companies want to maintain institutional knowledge in the event of an employee transition. Italian digital transformation company, Intesys, found themselves in search of a centralized solution. "We needed a centralized solution to manage provision and deprovision user access to credentials," Mirko Spezie, company senior system specialist, said. By leveraging shared folders called "collections" in their password management system, the Intesys team could easily and securely reassign access to the appropriate team members.

Beyond these password management examples at each stage of the employee lifecycle, it's important to note that not all password management systems are the same.

Case Study

Read the Intesys Case Study Here

Different Types of Password Managers

Password managers take many forms and come from different companies in the technology ecosystem. Across the spectrum, it's important to know the differences and what's best for your organization when picking the right password manager.

Password Managers for the Workplace	How it Works	Drawbacks
From Major Operating System Vendors	Microsoft, Apple, and Google offer convenience when using their platform and devices.	For truly cross-platform needs, these solutions fall short in comprehensive coverage. They further focus on individual credential management and not sharing across teams.
From Browser Providers	Browsers often prompt users to save their passwords as a function built-in within the browser.	Many employees use different browsers simultaneously across multiple projects. However, passwords can't be synced across browsers.
Proprietary	An independent proprietary system provides password management as a service.	Proprietary password managers can be more expensive and rigid, leaving little room to customize integrations or deployment options.

Password Managers for the Workplace	How it Works	Drawbacks
Open Source	An independent open source system provides flexibility, can be implemented in the cloud or self-hosted, and is 100% transparent regarding security since the code is open.	Some companies are still learning about the benefits of combining security and open source for infrastructure solutions.

Integration Between Password Managers, Identity and Access Management, and Identity Providers

The most useful password managers fit seamlessly with companies' existing Identity and Access Management strategies, as well as their existing Identity Providers.

Identity and Access Management (IAM)

According to CSOonline.com, IAM provides "...IT managers with tools and technologies for controlling user access to critical information within an organization." Typically, IAM describes access path levels to enterprise-wide tools and systems. Password management software is a foundational piece of an overall IAM approach, enabling team members to store and share log-in credentials.

Password management incorporates self-service enablement for security and collaboration, specifically for log-in credentials and sensitive information. For example, users could retain specific website subscriptions or hold credit card information or secure notes documenting procedures for particular credentials. Empowering employees to own their individual security fortifies the company's overall security stance.

Identity Providers (IdPs)

Identity providers (IdP) further complement password managers. Identity providers maintain centralized employee credentials, often combined with two-factor authentication, most commonly in the form of Single Sign On (SSO). Using this approach, enterprise-wide tools and systems simplify the log-in process for employees through the IdP.

With a goal to integrate with existing solutions, password managers using a company's existing Identity Provider provide a fast path to success. Password managers empower employees to manage and share credentials securely, including those that might be unique to individual employees or teams.

Understanding Password Management End-User Types

Introducing a new password management system to your organization requires understanding a range of prior experiences. This might include everything from prior password manager users to pen and paper users. Understanding end-user types, especially during employee onboarding, helps customize the rollout approach.

The Novice

They store passwords on a notepad, sticky notes, or on a spreadsheet. General password hygiene could be better, with many passwords being reused and shared through unsecured methods, such as chat messages or email. They might require some hand-holding at the beginning on how to use a password manager and on cybersecurity best practices in general. Getting them on board early and providing training will be key to retaining regular use of the password manager as intended.

The Password Management Aficionado

They've used the same free password manager for years and are incredibly familiar with the concept. They might have even mentioned it to the IT team once or twice before and probably use it to store their own work passwords. Getting them to use an enterprise password manager will be easy, and they might even show other team members how to use it. They might be an excellent champion to add to your training program.

The Team Lead

They currently have little to no oversight of how their team shares passwords. They want to quickly provide access to systems and sensitive information for their team and manage updates. Some team leads might have used a password manager before, having a good overall understanding of the concept and its benefits. They might need help organizing their team and passwords within the password management system itself.

The Executive User

They may or may not have used a password manager previously, but their biggest obstacle is time. They have packed schedules, with minimal openings to learn a new tool. If they don't personally see the value in a password manager early on, they might be hesitant to approve the continued use of one enterprise-wide. On the other hand, an executive brought into a security-first approach could become a power user and champion of employee empowerment for secure credentials management. The suitable secure sharing models easily allow an executive assistant to help with credential management for one or more senior executives.They may or may not have used a password manager previously, but their biggest obstacle is time. They have packed schedules, with minimal openings to learn a new tool. If they don't personally see the value in a password manager early on, they might be hesitant to approve the continued use of one enterprise-wide. On the other hand, an executive brought into a security-first approach could become a power user and champion of employee empowerment for secure credentials management. The suitable secure sharing models easily allow an executive assistant to help with credential management for one or more senior executives.

Evaluation of Password Management Functionality

Not all enterprise password management systems are the same. Some must-haves you should look out for include:

End-to-end encryption Data should be fully encrypted before it ever leaves your device.

Enterprise-grade security Look for regular third-party security audits and if the password manager is compliant with major privacy and security standards such as GDPR, CCPA, HIPAA, and SOC 2.

Flexible deployment options Look for the ability to leverage a cloud-based system to get up and running quickly and an option to self-host if that fits your needs.

Customizable approach You should be able to set password requirements and administrative policies that will empower employees to practice good password hygiene.

Easy syncing and integrations Streamline user onboarding and access management from your existing directory service and Identity Provider.

Scalability across the enterprise Access to critical data should be available across locations, browsers, and devices, with broad translations for a global audience.

Bitwarden offers many of these features and provides the advantage of being an open-source platform. Regular audits support this transparent foundation, with continuous improvements for enhanced security.

No matter your company's size, everyone benefits from using a password manager, especially one that allows you to address every part of the employee life cycle. Get started today with a free trial for your business.