

How to convince your management that NordPass is a necessary tool in your company

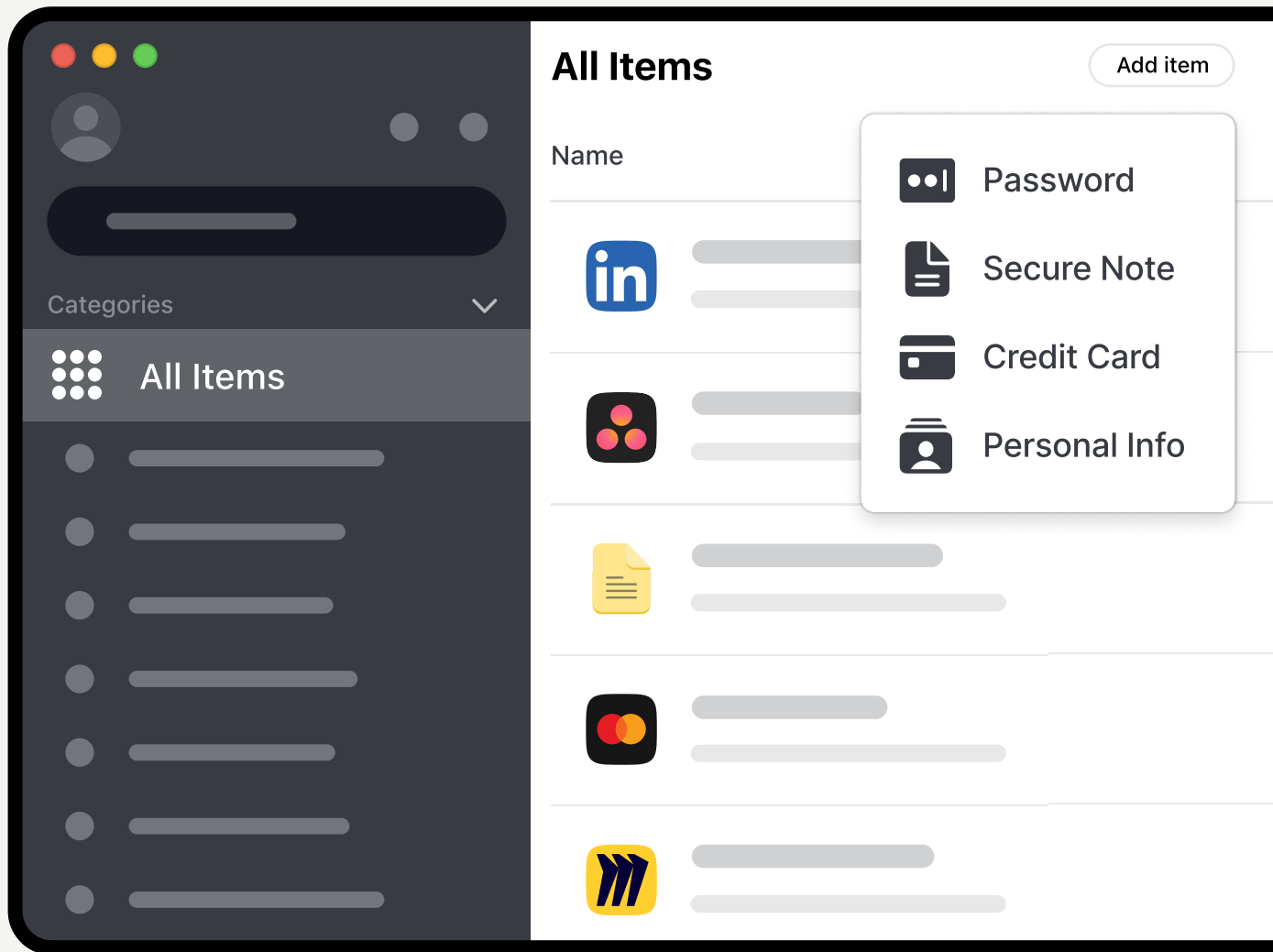


Introduction

In your organization, passwords are the first line of defense and the first target for bad actors. If the login credentials of anyone in the company are compromised, it can lead to dire consequences.

Using a password manager can help keep your company's sensitive data secure and greatly improve your company's productivity, saving you hours that would otherwise be wasted resetting and creating new passwords.

Your organization must stay ahead of the threats and maintain its productive daily work pace – that's where NordPass comes in.



1. The problem: Password management habits in the organization

High-profile data breaches can cause your company significant financial damages

35,900,145,035

known records were breached in 2024

\$4.88 million

the average cost of a data breach globally in 2024

95%

of data breaches involved human error

80%

of data breaches are related to passwords

Sources: [IT Governance](#), [IBM](#), [Mimecast](#), [DBIR](#)



Manual password management leads to wasted time and lost productivity



\$480 - value of productivity lost per employee due to password-related problems annually.



26 hours – average time an individual spends resetting passwords each year.

Insecure password sharing in your company is more common than you might think



46% of IT security and cybersecurity leaders still use insecure documents to store passwords.



Insecure password sharing methods:

- Printing out or writing down a list of passwords.
- Keeping a computer file labeled "Password".
- Sending a text or an email.

Revoking login access after employee departure might prove to be difficult for your company



5% of IT and cybersecurity leaders are confident exiting employees can't take login credentials with them.



7% of IT and cybersecurity leaders feel extremely confident they can transfer login credentials in the case of urgent contract termination.

Sources: [Beyond Identity](#), [FoneArena](#), [Bravura Security](#), [WEBIT](#)



2. The solution:

NordPass password manager

For IT & Security Departments



Encrypted business vault

Each member's vault uses end-to-end encryption with the ultra-secure XChaCha20 encryption algorithm, supporting zero-knowledge architecture. This means that no one – not even NordPass – has access to the information stored in your vault. NordPass is the only major password manager that uses state-of-the-art XChaCha20 technology. This measure significantly decreases the vulnerability of your company's data and reduces the risk of breaches or theft.



NordPass Authenticator

NordPass has an integrated two-factor authentication (2FA) solution. Unlike other password managers, NordPass secures your time-based one-time passcodes (TOTP) by leveraging biometric, possession, and knowledge factors, meeting the security standard for multi-factor authentication. With NordPass Authenticator, team members with shared access can generate their own two-factor codes, making adding an additional security layer to shared corporate accounts easy. TOTP codes are unlocked from within the NordPass app using the members' biometrics, thus eliminating the need to sync with the account owner to retrieve the code.



Easy and secure on - and offboarding

With NordPass, your IT colleagues can easily grant and revoke access without compromising efficiency and security. During onboarding, you can grant your colleagues access only to the necessary passwords and credentials. The offboarding procedure lets you remove access from departing employees with just one click of a button. You can easily transfer login details from a deleted member's account to an active member using the Items Transfer function, ensuring you are prepared for any changes in your team.



Dashboard

A single place that provides Owners and Admins with internal security insights relevant to the company. You can check for weak, old, reused, or exposed passwords using the Password Health tool, as well as run the Data Breach Scanner to find out if any of the corporate data has been compromised.



Activity Log

Serving as a crucial security and auditing tool, the Activity Log offers Admins and Owners a comprehensive overview of all password-related activities in employees' password vaults. It also provides details on actions within the Admin Panel. This includes details on login attempts, password updates, password autofill actions, and other security events. NordPass offers direct integration with Splunk® and Microsoft Sentinel, facilitating seamless data synchronization for companies using these platforms. Alternatively, NordPass customers can extract reports in JSON format via API and analyze them using other SIEM tools.

Company-wide settings

Many breaches occur because company managers don't have centralized control over employee credentials. With NordPass, you can establish granular policy controls for the whole organization, specific teams, or select employees. These controls ensure that users use multi-factor authentication, adhere to appropriate password strength standards, have autolock on devices with public access, and restrict outside sharing, thereby mitigating the risk of password-related incidents.

Additionally, you can turn on Offline Mode so your employees can access critical information when the internet connection is scarce, choose to set a time interval after which your teammates will have to log in to NordPass again, and block access to NordPass on rooted Android and jailbroken iOS devices to enhance your company's cybersecurity. NordPass also allows you to adjust and control what is shared within the organization and with external partners. Tailor these rules by role or individual to fit different needs—from single-item sharing to folder sharing.

Multi-factor authentication (MFA)

MFA is an extra line of defense to your NordPass encrypted vault. You can set a company-wide policy for all employees to enable MFA on their devices. Logging into MFA-protected accounts requires access to your smartphone, security token, or a different authorized authentication device, letting you feel even more secure as you handle your daily operations.

Sharing Hub

Keeping shared credentials in line can be complex and create entryways for security vulnerabilities. With NordPass' Sharing Hub, you can overview and manage all shared credentials in your organization, as well as those shared externally, allowing you to stay ahead of data security and prevent unauthorized access to company accounts.



For All Departments

Store credentials in one place

With NordPass, you don't need to search for login or payment information – simply store, access, manage, and share your passwords, passkeys, as well as personal and banking data, in one encrypted place, saving time from frequent password resets and letting you focus on the tasks at hand instead. Your saved items synchronize across your devices, so all your sensitive data is always within reach, and there's no need to worry about forgetting it.

Autofill and autosave

Autofill lets your team sign in and input information like usernames and passwords, credit card details, or addresses faster and stay productive throughout the day. NordPass will only autofill credentials on legitimate websites, ensuring your login details remain secure. NordPass' autosave detects new passwords and changed account details, letting you save and update them with one click, so you don't have to worry about forgetting them the next time you need them.

Secure sharing

Share passwords and other sensitive information with your colleagues without compromising security. For example, if you're going on holiday, you can quickly share encrypted login details, credit card information, and other items with your team. That way, you don't get stuck in a loop of resetting passwords each time someone new needs access. To reinforce the safety of your data, you can choose to share the items without granting editing access.



3. Why choose NordPass

If you're looking for a way to amp up your organization's security, you need the right tools at your disposal. With NordPass, you can secure your business and protect your teams with ease.



Industry-leading product

NordPass was created by the world's most trusted cybersecurity brand and creators of NordVPN — Nord Security.



Future ready

On the cutting edge of faster and safer technology, NordPass is the only password manager using the XChaCha20 encryption algorithm and benefits from machine learning for the autofill function.



More secure

NordPass' end-to-end encryption and zero-knowledge architecture ensure the finest standard of privacy and security for your business. NordPass has been audited by independent third-party institutions, has obtained multiple cybersecurity certifications, and offers a bug bounty program to detect and patch vulnerabilities.



Best-in-class tech support

Get help whenever you need it. Our tech-minded customer support team is available 24/7 to solve any issues at hand swiftly and smoothly. NordPass teams provide an effective communication, and personalized touch at every stage.



Cost-effective

Get more for less with 24/7 support, a simple-to-use interface, and a suite of advanced security features at a competitive price. NordPass offers more for less with no hidden costs.



Easier to use

A password manager can only work when it is widely adopted and properly used. That's why NordPass is user-friendly, free of endless menus and confusing jargon, and offers assistive materials for simpler onboarding processes.



Seamless deployment

Add NordPass to all company devices with ease, whether your employees are working from the office or remotely. NordPass is available as a browser extension for Chrome, Edge, Firefox, Opera, and Safari, as well as an app for iOS and Android devices.



4. Real-world success: Testimonials from NordPass clients

NordPass strives to build long-lasting success stories with our clients. Here's what our clients have said about NordPass:

“Impressive Administrative Capability: NordPass Business empowers administrators with robust tools to ensure secure user behavior, manage departing employees' credentials, track compromised passwords, and enforce effective password policies, maintaining our security standards.

User-Friendly Interface: NordPass Business offers a seamless and intuitive experience on both desktop and mobile. This accessibility boosts user adoption and adherence to security best practices.

Sleek and Responsive Design: The platform's appealing interface enhances user experience, with quick and efficient navigation.

Consistent Updates: NordPass Business consistently updates its desktop and mobile apps, prioritizing current security needs.

Flexible Credential Sharing: A standout feature is NordPass Business's advanced credential sharing. Users can securely share credentials, assigning different access levels, adding flexibility to security management.”

Cyrille (Asim) B.

Chief Technology Officer at small business

“NordPass Business is easy to deploy, from integrating SSO with Azure AD (Entra ID) to provisioning users and groups, you can be up and running within 15 minutes.

Being able to centrally deploy the Browser extension from GPO policies, with support for all major browsers, makes it easy to ensure that users have the software available to them when they receive their invite e-mail.

The browser extension is fast and detects more autofill opportunities than competitors, which means my users are more likely to use the software daily compared to the previous solution which they found cumbersome.

Customer Service was excellent with a response to an initial question about syncing groups being answered within minutes of sending the e-mail. They have extensive guides on getting setup.”

Anthony R.

IT Technical Project Manager at small business



5. Questions and concerns

Are password managers a costly investment?

Most password managers have different plans and may require users to pay additional fees for individual features, e.g., the breach scanner or activity log. In some instances, they may even charge for services like live customer support. However, NordPass is a cost-effective solution that offers more for less without any hidden costs. Starting at 1.79/month per user and with no extra charges, you receive 24/7 support, a simple-to-use interface, and a suite of advanced security features.

In what ways can a password manager be useful for the different departments in my company?

HR department

NordPass gives your HR department a secure way to organize, protect and share access to highly sensitive data, such as employment contracts, salaries, and visa applications, without exposing it to external risks.

Sales

NordPass enables sales professionals to get secure and quick access to internal accounts and sensitive client information anytime, anywhere – whether they are in the office or closing big deals on the go.

Marketing

NordPass helps your marketing teams safely store and handle sensitive data related to cross-departmental projects and tasks while enabling secure and easy sharing of login credentials and saving time on every sign-in, form fill, and ad payment. There's no need to sacrifice security in time-sensitive situations.

Finance

NordPass keeps credentials and payment information safely encrypted while letting finance professionals securely and efficiently share items with their team on demand.

IT and Operations

NordPass provides the necessary tools to empower your IT and Operations teams with a more secure and efficient onboarding strategy by organizing sensitive data by category, department, or both.

NordPass also ensures security while improving collaboration between different departments. For example, you can create groups of members from different departments who are working together on a project, and enable them to share sensitive information more quickly and easily.



Why do you need a password manager if you use single sign-on (SSO)?

While SSOs are an effective solution to centralizing access, they do not cover applications without SSO support, opening up security risks. NordPass helps secure and manage accounts that are not covered by SSO by enabling you to create and manage strong, unique passwords, mitigating password-related vulnerabilities.

NordPass offers additional password policy options and adds extra encryption to safeguard your vault, even if the SSO credentials are breached.

How will the password manager be integrated into our existing cybersecurity system and toolkit?

NordPass is compatible with major identity providers, including Microsoft, Google, and Okta. Thanks to this compatibility, your organization can centrally manage users' access to their vaults. NordPass' integrations with Vanta, Splunk®, and Microsoft Sentinel allow you to synchronize active members' data and monitor user activity. This allows you to optimize compliance processes and gain insights into potential risks. These integrations contribute an additional layer of security and productivity to your company's cybersecurity toolkit, helping regulate access. NordPass also easily and efficiently streamlines employee onboarding and offboarding.

How does the onboarding process work?

The onboarding includes videos showing the process of setting up the necessary settings, as well as supplementary materials, including an introductory PDF. Employees will also access videos from the User's perspective explaining how NordPass works. Larger companies are provided with dedicated account managers and face-to-face onboarding.

Will our organization receive ongoing support while using NordPass?

Yes, NordPass offers 24/7 support that can help you if you have any additional questions or encounter any problems while using our service.

Where is the NordPass data stored?

NordPass customers can choose to store their data either in the US or the EU data centers.

Is NordPass safe to use?

Yes, NordPass is a secure encryption-based service that uses public-key cryptography to protect all your organization's sensitive data and enable account recovery. We use the XChaCha20 algorithm to ensure fast, safe, and simple connections for our users. NordPass Business is ISO 27001 and SOC 2 Type 2 certified, independently audited by Cure53, and meets the objectives outlined in the HIPAA Security and Privacy Rules.



Can NordPass contribute to meeting cybersecurity compliance standards in my company?

Yes. Here's how NordPass can improve your compliance posture:



NordPass uses secure XChaCha20 encryption to ensure the confidentiality, integrity, and availability of all credentials, passwords, personal information, and notes in the company.



NordPass can help you control access to sensitive data and corporate accounts. The process of granting, revoking, and reassigning access is swift, simple, and secure. Administrators can ensure that each team member only has access to what they need. For additional privacy, members can share credentials without reading or editing access, and limit the duration of this access.



NordPass helps enforce a secure password policy. Our Password Generator makes creating strong, hard-to-hack credentials seamless and offers multi-factor authentication — which are two common compliance standards.



NordPass can help you prevent and mitigate the damage of data breaches. The Data Breach Scanner detects whether your corporate credentials, payment information, or domains have been breached. Your colleagues will receive immediate notifications if their credentials appear in a data breach. This helps discover breaches faster and gives more time to mitigate the damages and adhere to cybersecurity compliance standards. Password Health allows you to track old, reused, weak, and exposed passwords and update them accordingly.



NordPass provides supplementary information on how to prepare your business for compliance with regulations like the [NIS2](#), [ISO 27001](#), [NIST](#), [SOC 2](#), and [CIS](#).



Why is NordPass better than browser password managers?

	NordPass	Browsers
Zero-knowledge architecture	✓	✗
xChaCha20 encryption	✓	✗
Access on any device and browser	✓	✗
Device protection with Autolock	✓	✗
TOTP-reinforced security	✓	✗
Password generator set to company policies	✓	✗
Secure sharing within and outside organizations	✓	✗
Built-in domain leak monitoring	✓	✗
Detailed activity logs	✓	✗
Company password health overview	✓	✗
Overview and management of shared credentials	✓	✗
Granular policy controls for company-wide settings	✓	✗



Contact our experts

✉ sales@nordsecurity.com

