NordPass Business Privacy Notice
Effective from: January 3, 2024

The General Privacy Policy describes the privacy practices of Nord's Business Services, applications, and Websites, which also apply to the NordPass Business product. Nevertheless, the provision of Services related to NordPass Business ("NordPass Business Services") also involves the processing of additional personal data. Please continue reading for more information below.

GENERAL REMARKS

NordPass Business has no technical means to access your encrypted passwords, secure notes, or other items stored in your vaults (where the End User's items are stored; "Vault") because we built NordPass Business based on zero-knowledge architecture. Zero- knowledge architecture means that we do not have any access to what is stored in the Vault. In cryptography, it refers to being able to prove something you know without revealing what that is. As such, our zero-knowledge password manager keeps the proof that you have the key, but not the key itself, making it very safe. No one else can see the organization's passwords, credit card details, or notes. We also don't have the organization's End Users' Master Passwords, so the encrypted data will stay secure even if someone breaches our servers.

To understand more about NordPass Business specifications and technical features, please see the NordPass Business Whitepaper, where you can also find a description of the roles of NordPass Business account End Users, owners and admins.

ADDITIONAL NOTICE TO END USERS WHEN USING NORDPASS BUSINESS SERVICES

When the End Users use NordPass Business Services with the Vault provided by an organization (our Customer), that organization can:

- Control and administer the End Users' Vault, including controlling privacy-related settings and/or features.

- Access and process End Users' personal data, including the interaction data, diagnostic data, and the contents of End Users' communications with us.
- See when End Users accessed the application, and how they used the items within the Vault (e.g., shared with others, auto-filled, deleted, etc.).
- See other available information, such as the End User's email, timestamp, item name (available only to owners, as it is specified in the NordPass Business Whitepaper), receivers of items (where applicable), etc.
- See if End Users have been breached (this info is also available for End Users; see more in Section "Data Breach Scanner").
- View End Users' password health stats (without details of items themselves) and see how many old/weak/reused passwords the End User has stored in their Vault.
- Reassign the End User's items to another End User after the End User's account and Vault is deleted. All items within that Vault will be inherited by another End User to whom the Vault is reassigned.
- Delete all items in the End User's Vault at its own discretion.

Every item in the NordPass Business Vault has two types of data: metadata (title, website address, cardholder name, etc.) and secret data (login credentials, items (e.g., passwords, notes' content, credit card number, comments, etc.).The organization cannot see secret data. However, the End Users' items stored in the Vault are accessible by the organization via indirect ways, e.g., after deletion of the End User account. Therefore, please note that the NordPass Business Vault should only be used to store items related to the organization, and we highly recommend End Users not to keep any personal information there or to delete such personal information before leaving the organization/ceasing to use the NordPass Business Services.

If the End User is invited to join the NordPass Business account administered by an organization (by NordPass Business account owners or admins) and the End User already has one's own personal NordPass account registered with the same email address, the End User's items will be transferred to the organization, which will become the controller of this data as foreseen by the applicable legal acts. If the End User does not want their personal items to be transferred to the organization (to which NordPass Business account the End User is joining), we strongly advise deleting or exporting all items and adding them to another personal NordPass account (i.e., the NordPass

version for non-business users) created with another email address before accepting the invite to join the organization on NordPass Business.

NORDPASS BUSINESS AS A DATA CONTROLLER

In addition to the information provided in the General Privacy Policy, we process the following data as a data controller when you use NordPass Business Services or visit our Website:

- Application diagnostics. This aggregated and anonymized data helps us identify problems related to our app performance and updates. The collected information includes crash error reports and visited web addresses.
- Anonymized app usage statistics. We collect statistical information about the End Users' activity when using NordPass Business Services: (i) the number of items stored, (ii) the date when the item was created, (iii) how the password was created (e.g., imported, autosaved, created manually), (iv) the strength of passwords in percentage (e.g., 85% of your passwords are very strong), (v) the strength of the Master Password, (vi) the percentage of suggested passwords used, and (vii) the number of different folders in NordPass Business Vault, and (viii) information about the usage of autofill feature (e.g., disabling it for certain websites and switching the autofill forms manually). This analytical data gives us information on how our application is being used so that we can improve the NordPass Business users' experience and the app itself.
- Live chat widget. If you contact us via the live chat widget, in addition to processing your contact information, we will process your device information (such as the type of the operating system and browser) and IP address. This information is necessary for our support to determine the user's country, prevent abuse, see if the user is connected to our servers, and help our support to process queries faster.
- Device information. As in the case of when you visit our Website http://www.nordpass.com/business-password-manager, we collect some device information in our application too. Such information is logged automatically and may include your IP address, browser type, operating system version, and similar non-identifying information. We may use this information to monitor, develop, and analyze the use of NordPass Business Services.
- Also, we process your photo if you provide it on a voluntary basis by uploading it on your NordPass Business account. Please note that the photo available on the account will be available to other users of NordPass Business Services with whom you share and/or who share the items with you.

DATA BREACH SCANNER

NordPass Business offers an additional feature — Data Breach Scanner (“Scanner”). This feature enables scanning and monitoring if any of your monitored assets (verified email address(es) and/or credit card(s)) have been involved in any personal data breaches identified by our third-party service provider. Using a third-party provider, the Scanner checks email addresses (which were used by the End Users to join the organization) and credit card numbers (if added) to identify which pieces of data might be exposed. The Scanner continuously monitors and detects breaches daily, even when End User is logged out of NordPass on all devices, eliminating a need for proactive checks for the breaches. By using the Scanner feature, you authorize us to share your hashed email addresses and/or hashed credit card(s) number(s) with our third-party service provider. This enables them to monitor which parts of your data might have been compromised. Should any of your monitored assets have been breached, NordPass will inform you about the breach with an in-app notification and via email. NordPass Business provides the Scanner on an “as-is” basis and does not warrant the completeness or accuracy of the monitoring results. We cannot guarantee that the data or information provided through or from the Scanner will be correct, current, uninterrupted, precise, error-free or up to date. You understand that there might be occasions where your monitored assets have been compromised, but such information is not or does not become available to us or our third-party service provider. You use Scanner entirely at your own risk.

Please note that even when you choose to use the Scanner, NordPass Business has no technical means to access Customer Items stored in the NordPass Business Vault and the Scanner’s search results that are shown on the End Users’ devices. These always remain encrypted and remain available to the End Users with administrative rights (owner and/or admin), as well as End Users having an account.[1]

1

PASSWORD HISTORY

The NordPass Business feature “Password History” allows keeping a record of the last ten (10) password changes made to an item in the Vault, as well as copying and restoring the previous passwords and seeing who made such changes and when (if the item was shared with another user).

In the case of usage of the Password History feature, NordPass Business processes the last ten (10) passwords created on an item, the timestamp of when the event happened, and the email address of the user who changed the password (applicable in cases when the user is granted full rights for item sharing; see more in the section “Item Sharing” below and NordPass Business Whitepaper). We use the aforementioned data to (i) enable the item owner access to password history, (ii) facilitate copying or restoring previous passwords, (iii) inform the item owner if a shared password was overwritten, and identify by whom and when it was done.

EMAIL MASKING

The NordPass Business “Email Masking” feature allows End Users to create a masked email to keep their actual email address private, reducing the receiving of spam emails and helping to protect their data from data brokers. The End User must verify the email address to use this service. Emails received through Email Masking, including the sender and recipient’s email server IP address, sender’s email address, recipient’s email address, and timestamps, are deleted as soon as they are forwarded to the End User’s email address. We use a trusted third-party service provider to manage this service.

Additionally, if you represent a HIPAA-related institution, please note that this feature will not be enabled for you, or it can be disabled upon your request. This ensures adherence to the specific regulatory requirements of such institutions.

ITEM SHARING

NordPass Business End Users may use the “Item Sharing” feature, which enables sharing of Customer Items with other selected users, depending on organization's configuration (Customer Items can be shared with limited or full rights, as it is specified

in the NordPass Business Whitepaper).

By allowing the Item Sharing functionality within an organization, the Customer understands that Customer Items may contain sensitive information, e.g., passwords, private notes, or other confidential information, that, if used improperly or by a compromised user or third party, may cause damage or harm, result in leak or loss of confidential data, and agree to use this functionality at Customer's own risk and discretion. NordPass Business will not and cannot be held accountable for any misuse, loss, harm, or damage caused by improper use of the shared Customer Items by a compromised third-party/user.

Potential risks of sharing Customer Items with other selected users and the assessment of their credibility are solely within the Customer's and End User's own discretion and risk.

DATA CENTER LOCATION

Before commencing NordPass Business services, NordPass Business allows the Customer to select a region between the United States or the European Union where the Customer's and its End Users' data, i.e., Customer Items uploaded to the Vault, both metadata and secret data ("Customer Data") will be located and stored. After selecting a certain region, all Customer Data will be stored in that region, while other data, such as the hashed email address of the End User and which organization this End User belongs to, will always be stored in a data center located at the United States (regardless of the location of the selected data center).

If you plan to use Nord Pass Business via managed service providers ("MSP") please inform MSP about your preferred data center location in advance.

Older versions:

NordPass Business Privacy Notice as updated on November 3, 2022
NordPass Business Privacy Notice as updated on September 25, 2023