NordPass®

NordPass Business Whitepaper

Last updated on 2023/02/01

Version 1.4

Table Of Contents

Table Of Contents

Introduction

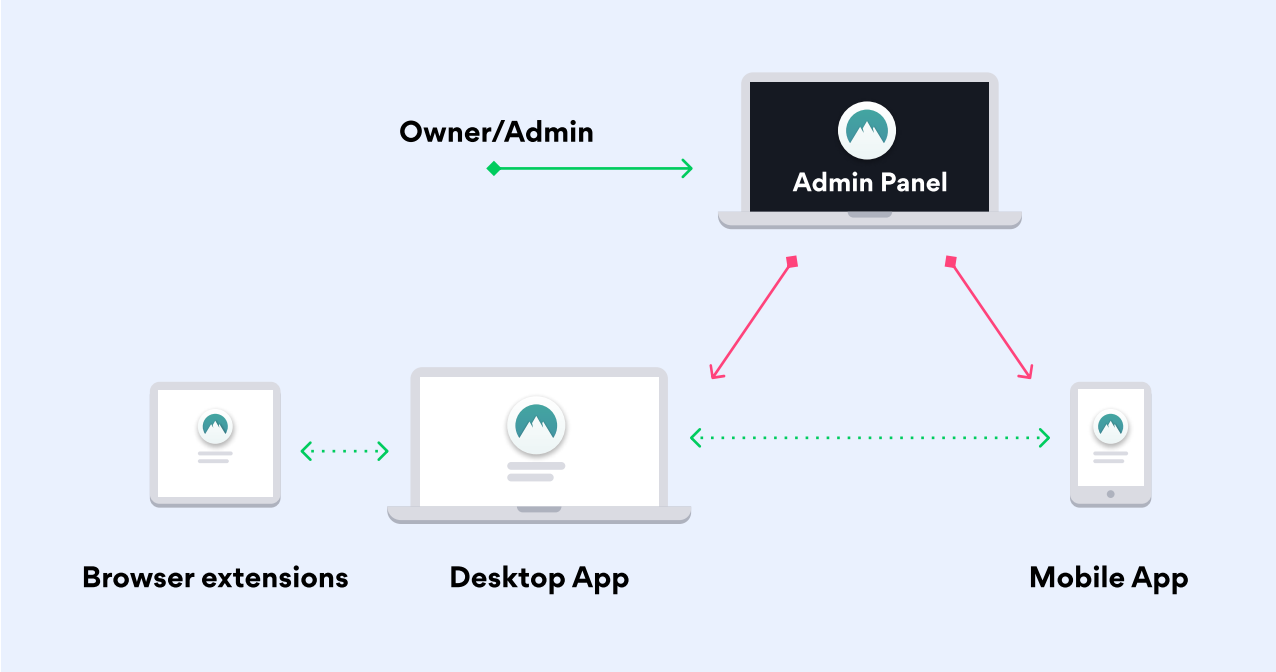
What is NordPass Business?

In the digital age when cyber attacks on companies number in the millions, the NordPass Business password manager was created to address the needs of small and medium-sized enterprises as well as large corporations. It provides your employees with a secure and easy-to-use platform where they can store, access, and share work passwords.

We focus on supplying users with the best tools to address poor password security. That's why NordPass offers additional security tools such as the **Data Breach Scanner** and **Password Health**. They help users to easily detect their data in any known breaches and identify weak, compromised, old, or reused passwords.

The NordPass community is an integral part of the product — it's at the core of what we do. We always gather feedback from our user base and use it to improve NordPass.

The NordPass Business product consists of the Admin Panel (a platform where you can invite and manage your users), NordPass applications (desktop and mobile), and the NordPass browser extension.



Main security principles

NordPass is built upon the following security principles:

- **State-of-the-art encryption algorithms**

Encryption is the foundational part of the entire NordPass security structure. We strive to bring our users a handy, foolproof method of storing their passwords securely at all times. This is made possible with the help of the top-tier elliptic curve encryption library NaCl.

We chose the ChaCha20 family over AES because the performance of the latter heavily relies on the hardware features (such as the AES instruction set for x86 processors), which are rarely available on mobile devices.

- **End-to-end encryption**

NordPass's end-to-end encryption ensures that no sensitive data is exposed at any step of the way. NordPass is built to encrypt data locally and only then move it to the cloud. This means that NordPass employees cannot view or access your items — only you can. And, if your data ends up in the wrong hands, they will see nothing but gibberish.

- **Extra security layers**

To ensure complete protection, we provide users with multiple layers of security. As an organization, you can require all your users to sign in with multi-factor authentication in addition to their Master Passwords. To do so, they can use popular authentication apps or backup codes.

- **Secure item sharing**

NordPass doesn't just store your items but also allows you to share them worry-free. Passwords, credit cards, and secure notes are also end-to-end encrypted and protected from prying eyes.

- **Transparency**

At NordPass, we believe that any claims we make about cybersecurity must be validated. To this end, we've been thoroughly audited by third-party security auditors. This also helps us find new and better ways to ensure our customers' data protection

- **Business authentication**

Business authentication is built on the OAuth 2.0 protocol, which acts as a centralized identity provider and authorization server for NordPass. The implementation of OAuth 2.0 protocols for business authentication is fully compliant with the Internet Standards created and published by the Internet Engineering Task Force (IETF) and is also in line with the best current practices.

How does NordPass work?

Terminology explained

To understand how everything works in NordPass, let's first explain some terminology.

Identity - right now, one user has only one related identity. In the future, one user might have more than one identity, but, in the scope of this chapter, an identity equals a user.

Item - a record containing sensitive data such as a password, credit card number, credentials, etc.

Folder - an item type used as an organizational unit for grouping items.

Group - an item type used as an organizational unit for grouping identities.

Access grant (or relation) - a linking record in our database that has two functions:

1. To identify a relation between an item and identity, folder, or group. This means that, if there is no access grant between an item and identity, the user related to that identity cannot access that item.

2. It has item access Private Key encrypted with the identity's Public Key. In other words, it carries cryptographic information about the relation of one identity and one item required to access the item's content. This ensures that, even if a user gets an item but there is no access grant, he is unable to access the item's content. Also, if a user gets somebody else's access grant, he can't use it either.

Accessing and sharing items

Every identity, item, folder, and group has asymmetric access key pairs. It's more complex than that (read more in the **Encryption** section), but, to simplify things in this chapter, let's assume that there is only one asymmetric key pair.

There's a plethora of identities and items in our database, but only a few of them have access grants (relations). For example, in Figure 1, "Identity 1" has two access grants (relations): "Identity 1" with "Item 2" and "Identity 1" with "Item 6".

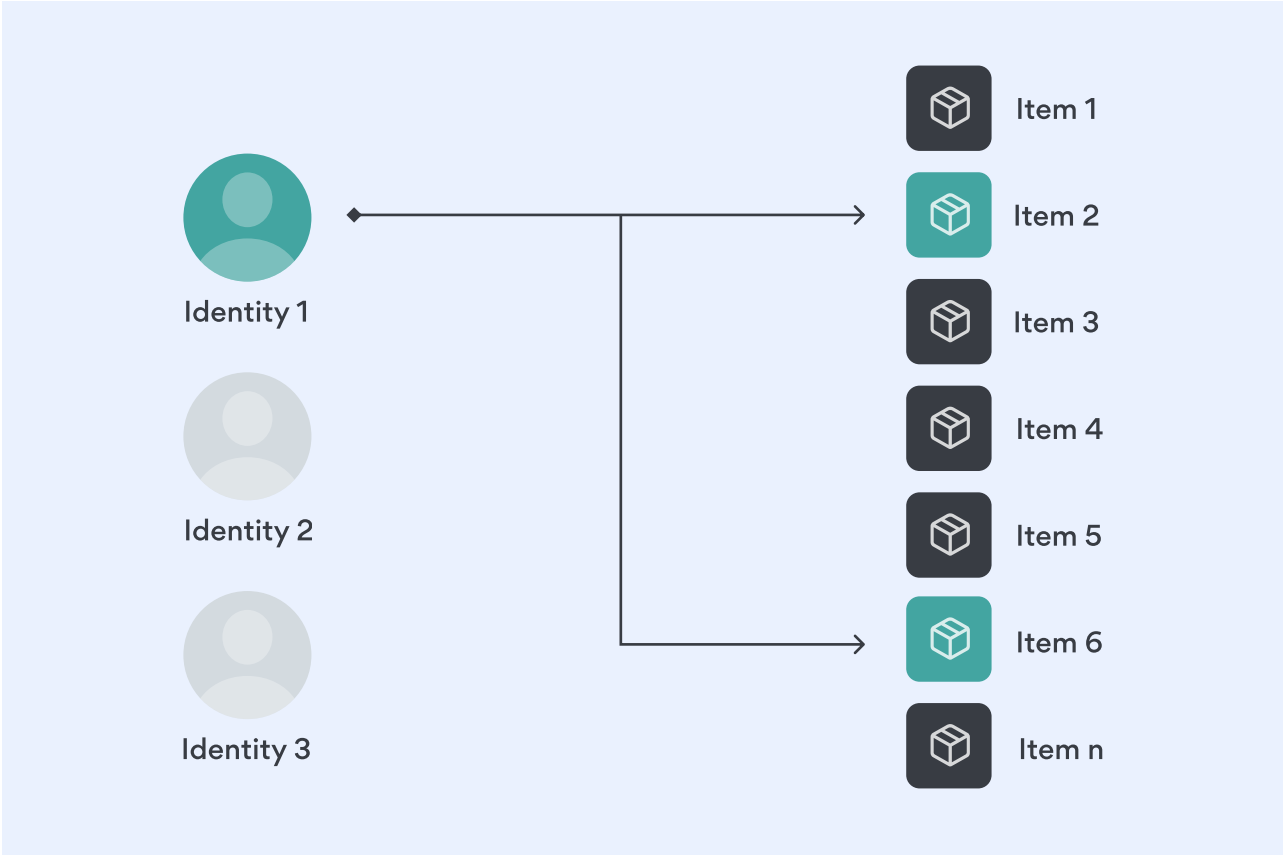


Fig.1 General view

So, when the user related with "Identity 1" logs in, NordPass:

1. Selects access grants (relations) associated with that identity;
2. Selects items associated with these access grants (relations).

So, we end up with a view as in a Figure 2:

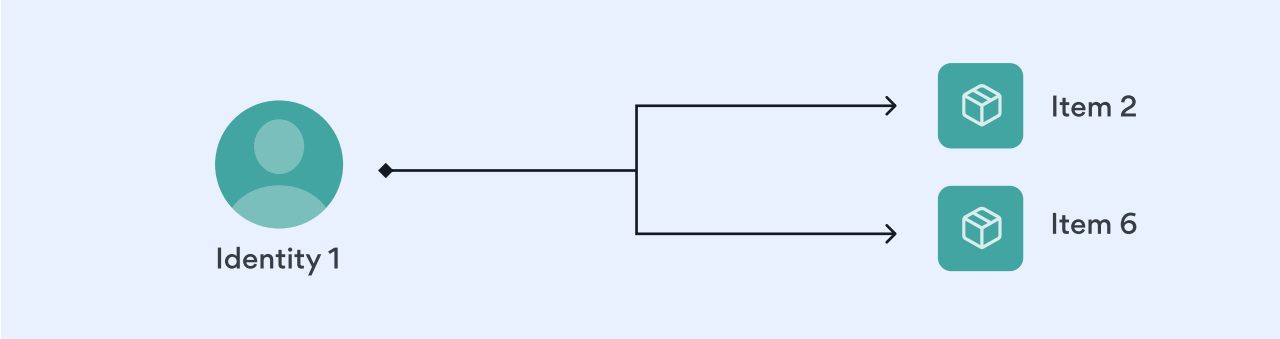


Fig. 2 Identity and related items

As mentioned above, access grant (relation) isn't a simple line — it's a link record (see Figure 3). To create an access grant (relation), the item's Private Key has to be encrypted with the identity's Public Key (red line). To access the item, the identity has to use its Private Key with the access grant (relation) (green line) and get the item's Private Key.

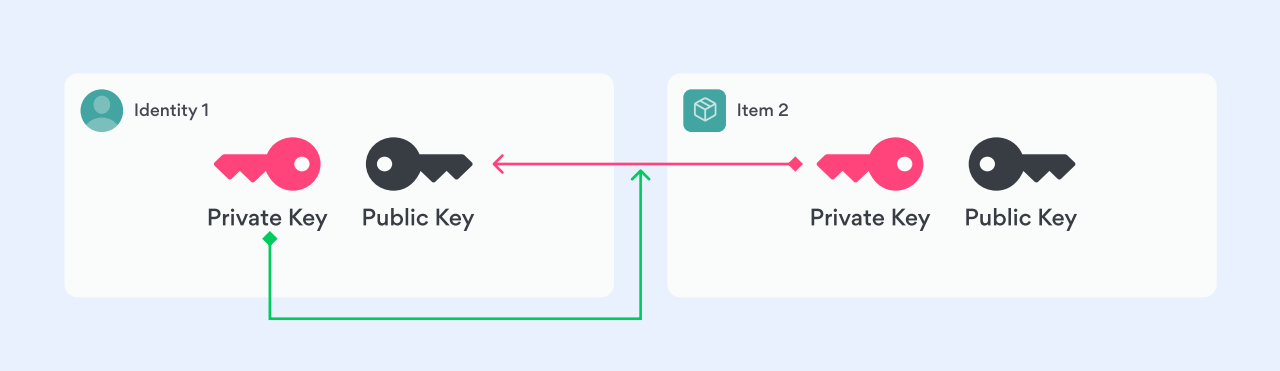


Fig. 3 Access grant (relation)

For "Identity 1" to share "Item 2" with "Identity 2", the following steps must be taken (see Figure 4):

1. Access grant (relation) between "Identity 1" and "Item 2" must exist (red line);
2. "Identity 1" has to use its Private Key on the access grant (relation) (green line);
3. "Identity 1" has to get "Identity 2" Public Key (black line);
4. Encrypt "Item 2" Private Key with "Identity 2" Public Key (black dotted line) and create new access grant (relation) (red dotted line);
5. Only then "Identity 2" can see "Item 2" (Fig. 1 and Fig. 2) and apply its Private Key to that new access grant (relation) to get access to "Item 2" (green dotted line).

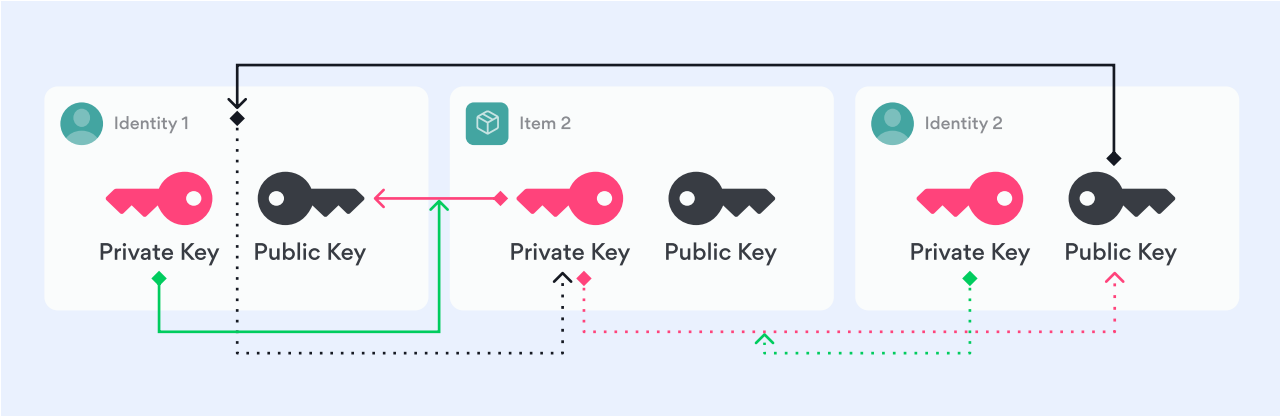


Fig. 4 Sharing an item with another identity

IMPORTANT NOTE. Notice that after "Identity 1" shared "Item 2" with "Identity 2", a new access grant (relation) was created, but only one instance of "Item 2" remains. This means that we neither share a snapshot of the item nor duplicate it. This also means that, if either identity makes any changes to "Item 2", it will instantly affect all the identities (folders, groups) that have access grants (relations) to "Item 2" — they will all be able to access the updated version of the item.

Accessing items via Folders

Now that we have an understanding of access grants (relations) and sharing, let's take a look at a more complex example (see Figure 5). Here, identity is accessing items not directly but via an organizational item type called Folder (Folder has its own key pair).

1. Folder has access grants (relations) with items, or, in other words, each item's Private Key is encrypted with the folder's Public Key (red dotted lines);
2. In order to access the item, the folder's Private Key has to be used on an access grant (relation) (green dotted lines);
3. Identity has an access grant (relation) with the folder (red line);
4. In order to access the folder, identity has to use its Private Key on that access grant (relation) (green line). By getting access to the folder's Private Key, identity inherits its access grants (relations) with items (red dotted lines).

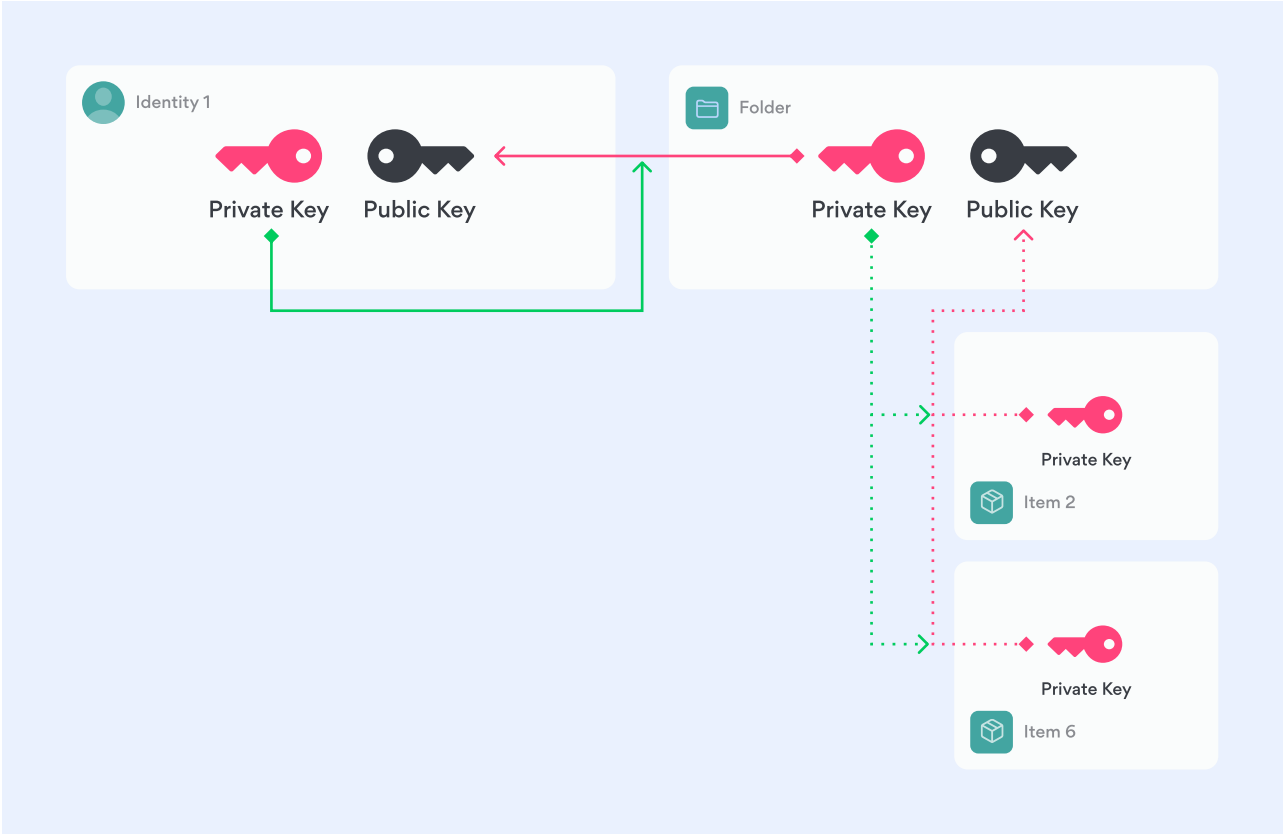


Fig. 5 Accessing items grouped in a folder

Accessing items via Groups

Let's take one step further and group not only items into folders, but identities into Groups, which have their own key pairs (see Figure 6).

1. Folder has access grants (relations) with items (red dotted lines);
2. To access items, the folder's Private Key has to be used on an access grant (relation) (green dotted lines);
3. The Group has access grant (relation) with the folder (red dashed line);
4. To access the folder and inherit access grants (relations) with the items (dotted lines), the group's Private Key has to be used on an access grant (relation) (green dashed line);
5. Identities have access grants (relations) with the group (red lines);
6. To access the group, identity has to use its Private Key on the appropriate access grant (relation) (green line). By getting access to the group's Private Key, identity inherits its access grant (relation) with the folder (dashed line) and items (dotted lines).

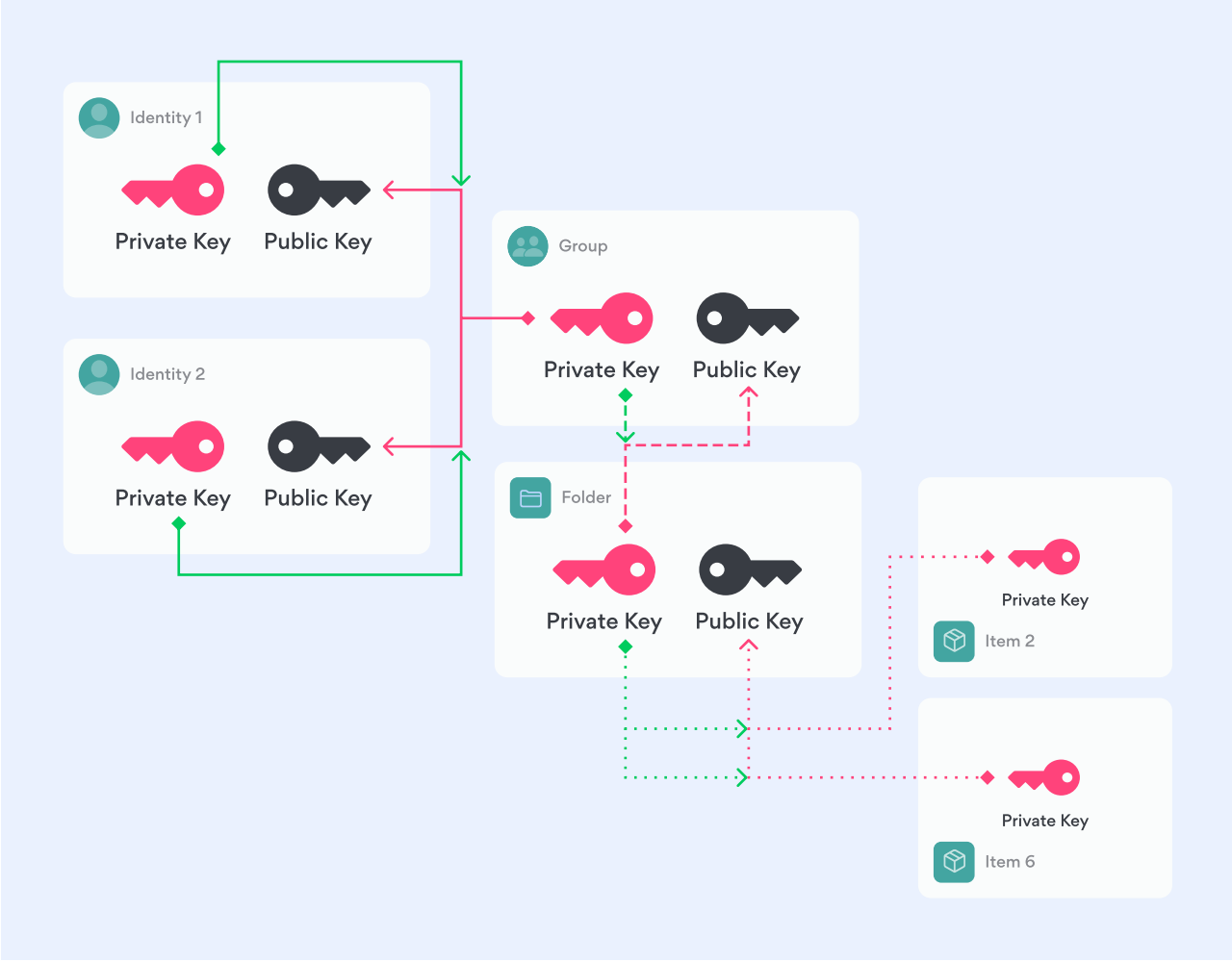


Fig. 6 Accessing items grouped in a folder

NordPass B2B structure

We've covered all the building blocks, and now we can take a look at the actual (although simplified) structure of the NordPass B2B solution:

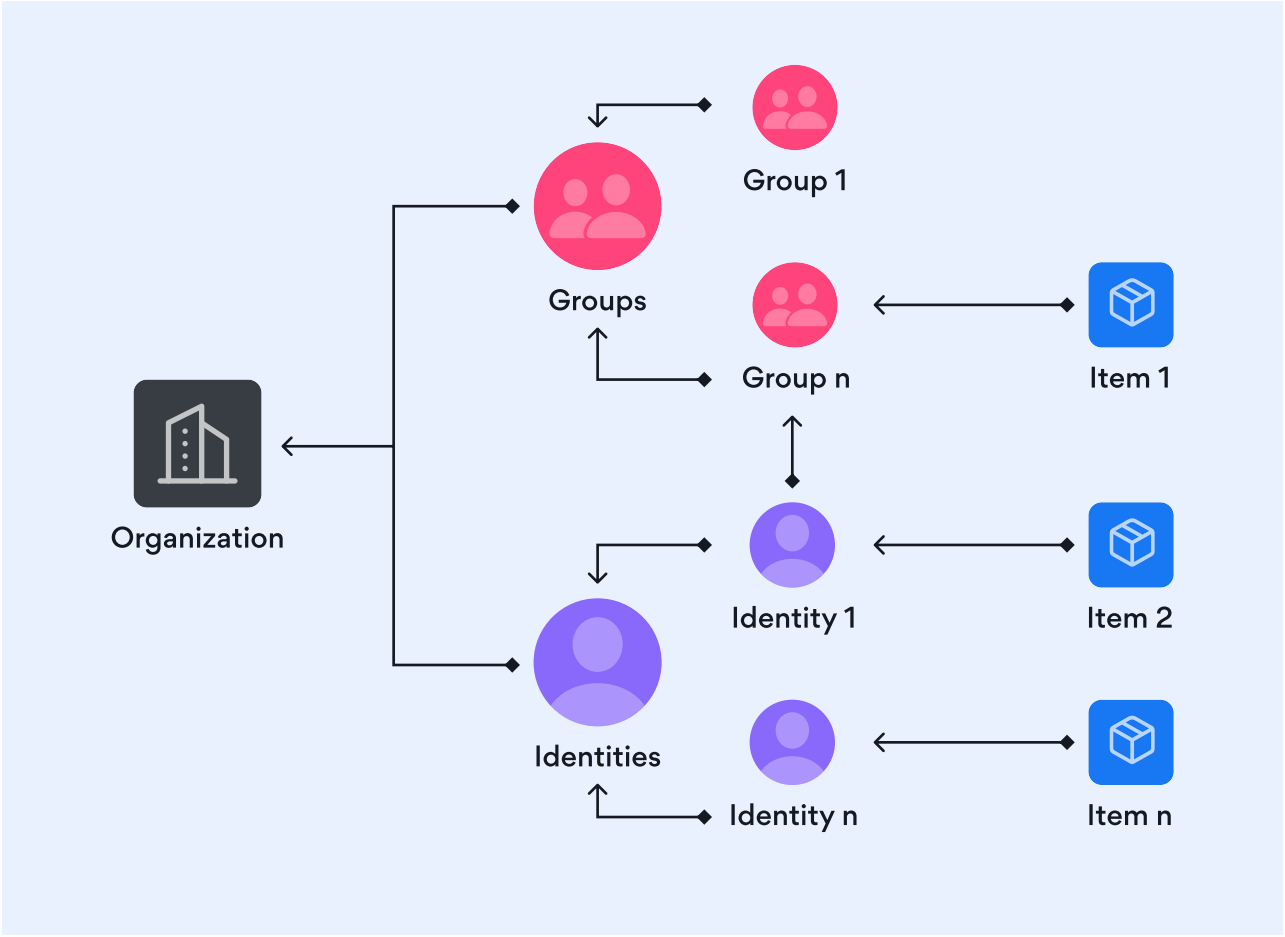


Fig. 7 Simplified architecture of the organization

From Figure 7, we can see that "Identity 1" has direct access grant (relation) with "Item 2", but it also has an access grant (relation) to "Group n", so it inherits access grant (relation) with "Item 1". "Organization" inherits access grants (relations) to all the items, groups, and folders. That is why all items are "owned" by the organization and not the user and why we introduced identity (or user) root folders.

In our B2B solution, when an item is shared with an identity in person (not with a group) instead of using identity Public Key, its root folder Public Key is used. This is how we can ensure that the organization inherits access grants (relations) to all the items of the subordinate identities.

Encryption

Encryption technology explained

In NordPass Business, the organization is the owner of all the data. In other words, if an employee creates an item, the access is instantly granted to that employee, and they can manage that item in the app. But, if the employee leaves the company, their items stay within the organization and can be reassigned to another member. The organization can also recover employees' account without the risk of losing any data.

This is all done using public-key cryptography. For the Master Key derivation, we use the Argon2id function with 16-bytes cryptographic salt.

For secret-key (symmetric) cryptography, we use authenticated encryption algorithm:

- XChaCha20 stream cipher encryption;
- Poly1305 MAC authentication.

For public-key (asymmetric) cryptography, we use authenticated encryption algorithm:

- X25519 key exchange;
- XSalsa20 stream cipher encryption;
- Poly1305 MAC authentication

Each NordPass user has a unique public-key cryptography key pair. Public Key is always stored in plain text form. Private Key, on the other hand, exists in plain text form only on the user's end device for a limited period of time and never leaves it. When we need to store a user's Private Key, it's encrypted with secret-key cryptography (XChaCha20-Poly1305-IETF) on the user's device and only then passed to us.

While the app is unlocked, the unencrypted Private Key is stored in the secure memory accessible only to the NordPass application. When an application is locked, either by the user or automatically after a set period of inactivity, the Private Key is deleted from the secure memory.

For the user's Private Key encryption, the Master Key is used. Master Key is derived from the Master Password together with a 16-bytes-unique-per-user cryptographic salt using the key

derivation function (Argon2id). We ask the user for the Master Password every time we need to decrypt the user's Private Key.

In addition to the encryption principles above, every item (folder, password, credit card, etc.) has two types of data:

- Metadata (title, website address, cardholder name, etc.);
- Secret data (login credentials, credit card number, comments, etc.).

This enables permission granularity: a user can see that an item exists but can’t use it (see credentials) until they are granted the rights to do so.

How items are accessed

Every item can be accessed in two ways:

Direct access flow

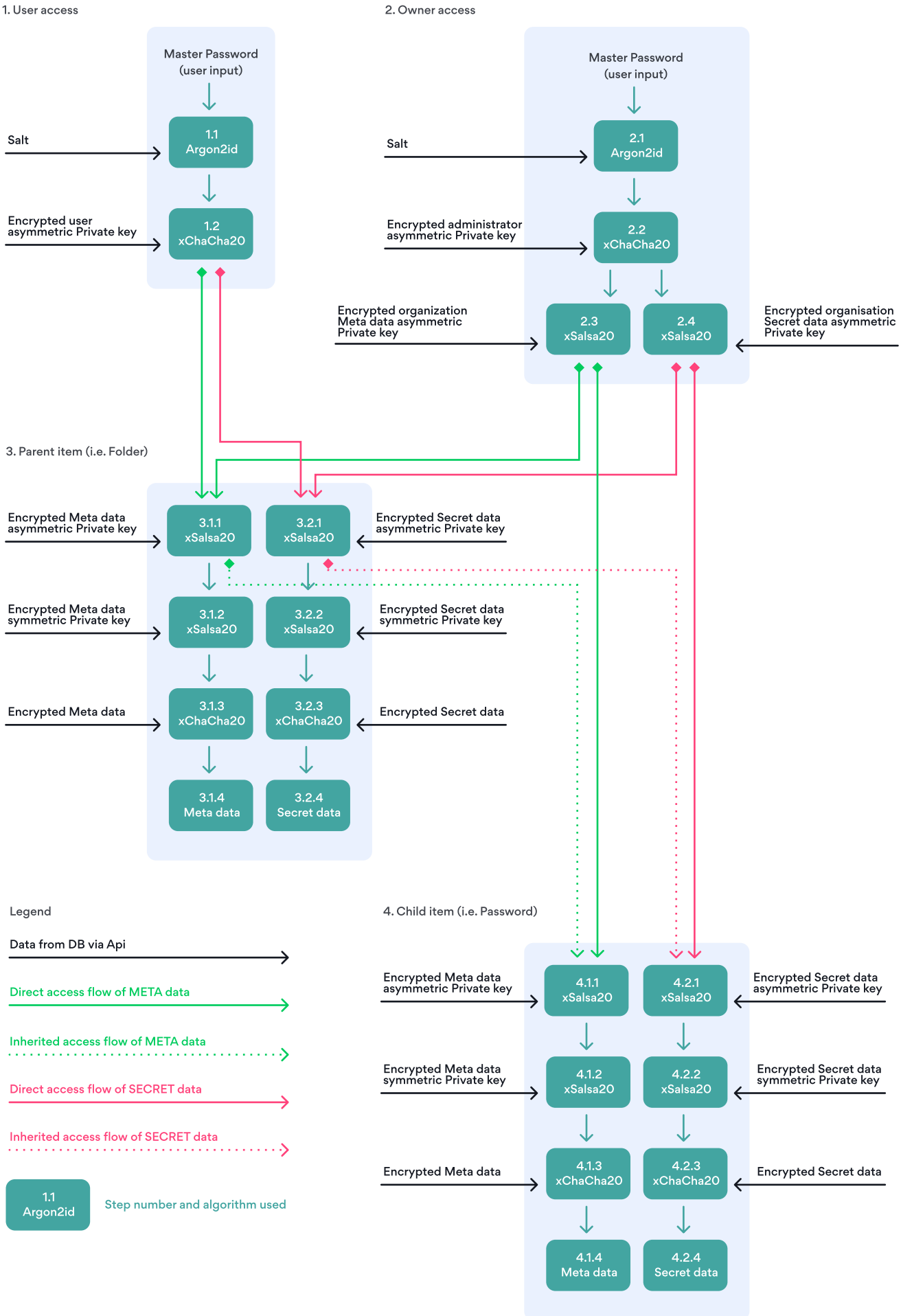
This is a common flow as it is used when an item is shared with a user.

1. The user is asked to input the Master Password, which, together with the unique-per-user cryptographic 16-bytes salt, is used in the key derivation function Argon2id. The result (we call it Master Key) is used as a key to decrypt the user's Private Key;
2. The user's encrypted Private Key is decrypted locally (on their device) with the XChaCha20-Poly1305-IETF algorithm using the Master Key as a decryption key;
3. Since the item has two parts (metadata and secret data), the user's Private Key is used to decrypt the item's metadata private key and secret data private key (or only one of them, depending on the permissions granted to the user);
4. The Private Key of the item's asymmetric key pair (either metadata or secret data private key) is used to decrypt the item's symmetric key using the xSalsa20 algorithm;
5. The symmetric key is used to decrypt either an item's metadata or secret data using the XChaCha20-Poly1305-IETF algorithm.

Organization access flow

As all the items are created on the organization's behalf, every item's asymmetric keys are encrypted with the organization's Public Keys using the xSalsa20 algorithm. This way, the user who has access to the organization keys can access any item as described in the direct access flow. The only difference is that the user has only one asymmetric key pair, and the organization has two separate key pairs — one for the metadata and another for the secret data.

This allows better permission granularity, i.e. access only to the metadata of all the organization's items without permission to read the secret data.


1. User access
Master Password (user input)
Salt
1.1 Argon2id
Encrypted user asymmetric Private key
1.2 xChaCha20
2. Owner access
Master Password (user input)
Salt
2.1 Argon2id
Encrypted administrator asymmetric Private key
2.2 xChaCha20
Encrypted organization Meta data asymmetric Private key
2.3 xSalsa20
2.4 xSalsa20
Encrypted organisation Secret data asymmetric Private key
3. Parent item (i.e. Folder)
Encrypted Meta data asymmetric Private key
3.1.1 xSalsa20
3.2.1 xSalsa20
Encrypted Secret data asymmetric Private key
Encrypted Meta data symmetric Private key
3.1.2 xSalsa20
3.2.2 xSalsa20
Encrypted Secret data symmetric Private key
Encrypted Meta data
3.1.3 xChaCha20
3.2.3 xChaCha20
Encrypted Secret data
3.1.4 Meta data
3.2.4 Secret data
Legend
Data from DB via Api
Direct access flow of META data
Inherited access flow of META data
Direct access flow of SECRET data
Inherited access flow of SECRET data
1.1 Argon2id
Step number and algorithm used
4. Child item (i.e. Password)
Encrypted Meta data asymmetric Private key
4.1.1 xSalsa20
4.2.1 xSalsa20
Encrypted Secret data asymmetric Private key
Encrypted Meta data symmetric Private key
4.1.2 xSalsa20
4.2.2 xSalsa20
Encrypted Secret data symmetric Private key
Encrypted Meta data
4.1.3 xChaCha20
4.2.3 xChaCha20
Encrypted Secret data
4.1.4 Meta data
4.2.4 Secret data

Functionality and features

Roles and Permissions

NordPass Business users are all assigned roles with different permissions. Each member who's joined your organization will have one of the three roles:

Owner is the one who creates a NordPass Business account for an organization and automatically becomes the Owner. This is the primary role with the most privileges within the organization. They can manage members in the Admin Panel and apply company-wide settings.

This role can also grant Owner rights to other members, but this should be done with caution. Owners are the only ones who hold the organization's encryption keys and are responsible for all the items within it. Once someone becomes an Owner, they cannot be demoted, and their profile cannot be edited, deleted, or suspended.

We suggest having at least two Owners per organization. In case one forgets their login details, the other can always recover the account. Otherwise, access to NordPass might be lost.

Admin is a member who was granted access to the Admin Panel. They can invite new members, manage their profiles, suspend or delete them. Admins can also apply company-wide settings but cannot manage Owners or revoke their rights.

User is a person who has access only to the NordPass app. They can be granted Admin rights by other Admins or Owners.

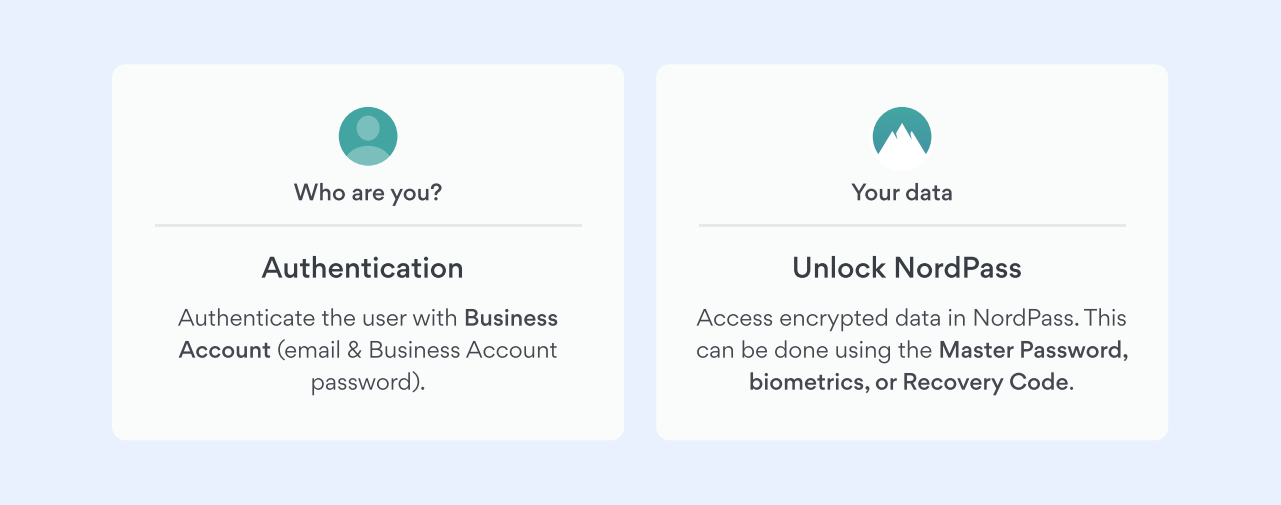
The table below provides a more detailed overview of each role's permissions:

	Owner	Admin	User
Access to the NordPass app	✓	✓	✓
Access to the Admin Panel	✓	✓	✗
Invite and manage members	✓	✓	✗
Grant Admin rights	✓	✓	✗
Grant Owner rights	✓	✗	✗
Delete Owner	✗	✗	✗
Revoke Admin rights	✓	✓	✗
Manage account recoveries	✓	✗	✗
Manage Groups	✓	✓	✗
Apply company-wide settings	✓	✓	✗
Access and manage billing information	✓	✓	✗
Transfer items of a deleted member	✓	✗	✗

User accounts

How to create accounts

1. To start using NordPass Business, **create a Business Account** with your work email and set a password. Signing in to the Business Account is the first step when logging in to the NordPass app or the Admin Panel. It authenticates you as a user.
2. You'll be automatically directed to **create a Master Password**, which acts as a major building block for the cryptographic layer that protects your passwords. The Master Password unlocks the app and decrypts your items for you.



How secure is the Master Password?

The Master Password is as secure as you make it. Therefore, when creating the Master Password, NordPass asks you to meet certain security requirements, such as having a password at least 9 characters long and including numbers or upper-case letters.

It's crucial to remember your Master Password. NordPass uses end-to-end encryption architecture, which means that we don't know your Master Password and have no way of accessing it. We are unable to recover or reset it in case you lose it — only your organization's Owner can.

The Master Password is:

- Always private;
- Used to access and decrypt items locally on the user's device;
- Never transferred over the internet;
- Not known to NordPass employees;
- Only known to you.

What is a Recovery Code?

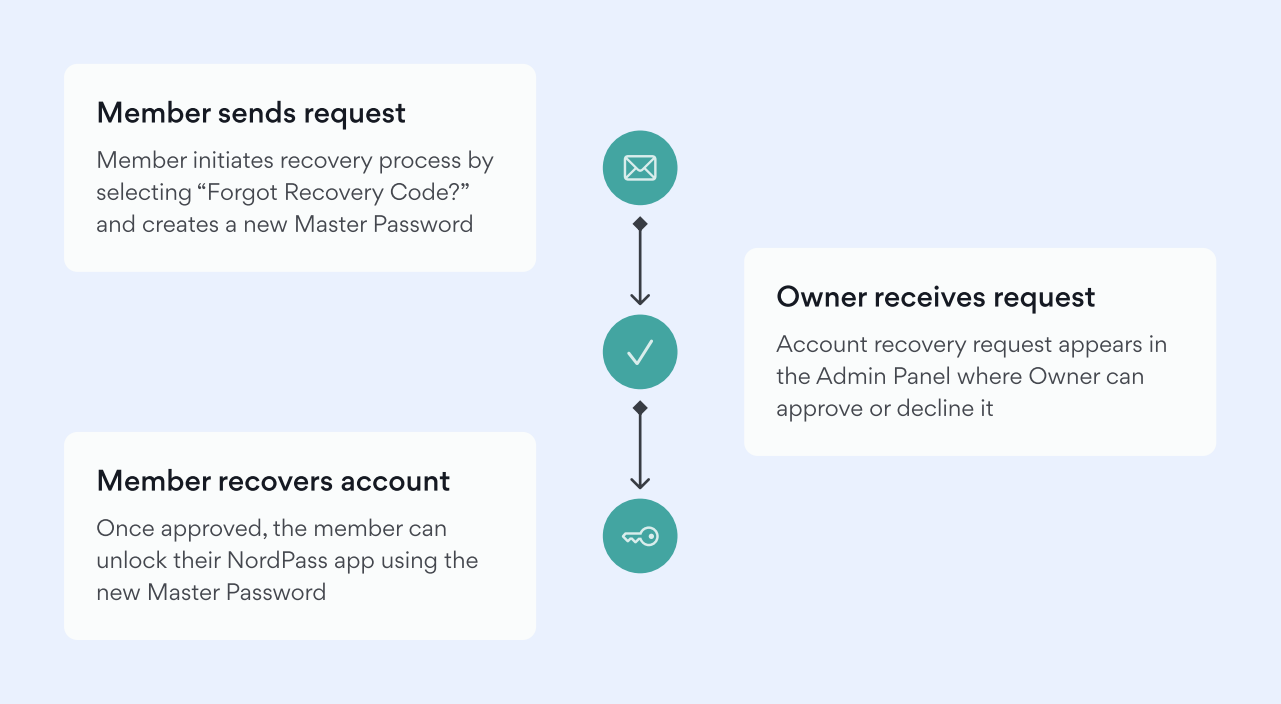
The Recovery Code is generated once the user has created the Master Password. It can be used as an alternative way to access the app in case the user forgets the Master Password.

The Recovery Code is always made of 24 characters that are a mix of upper-case letters and numbers. It's generated using 32 bytes of random data separated by hyphens. The Recovery Code looks like this: VJZX-4RE9-J7XT-94SE-84JX-CU8H.

We understand that memorizing the Recovery Code is close to impossible. Therefore, we strongly recommend downloading it as a PDF file, printing it out, and keeping it somewhere safe. Once you have a physical copy, delete the digital copy from your computer.

Account Recovery Process

The Account Recovery process is only available to B2B users and can be approved only by the Organization Owner. It helps users regain access to their accounts if they lose both their Master Password and the Recovery Code.



How the request is created

Members can initiate the Account Recovery process upon logging in to the NordPass app or Admin Panel. Once on the login page, they need to click Forgot Master Password? and then Forgot Recovery Code?. This will start the Account Recovery process:

1. The new unique-per-user cryptographic salt is generated.
2. The user creates a new Master Password, which, together with the new cryptographic salt, is used to derive the new Master Key.
3. The user’s new Key Pair is generated.
4. The user’s new Private Key is encrypted with the new Master Key.
5. The new Recovery Code is generated, which, together with the new cryptographic salt, is used to derive the new Recovery Key.

6. The user's new Private Key is encrypted with the new Recovery Key.
7. The 4-digit Confirmation Code is generated and encrypted with the organization's Public Key.
8. The user's new Public Key, cryptographic salt, Private Key encrypted with the Master Key, Private Key encrypted with the Recovery Key, and encrypted Confirmation Code are sent to the API, which saves them as a recovery request. It shows up on the Recoveries page in the Admin Panel.

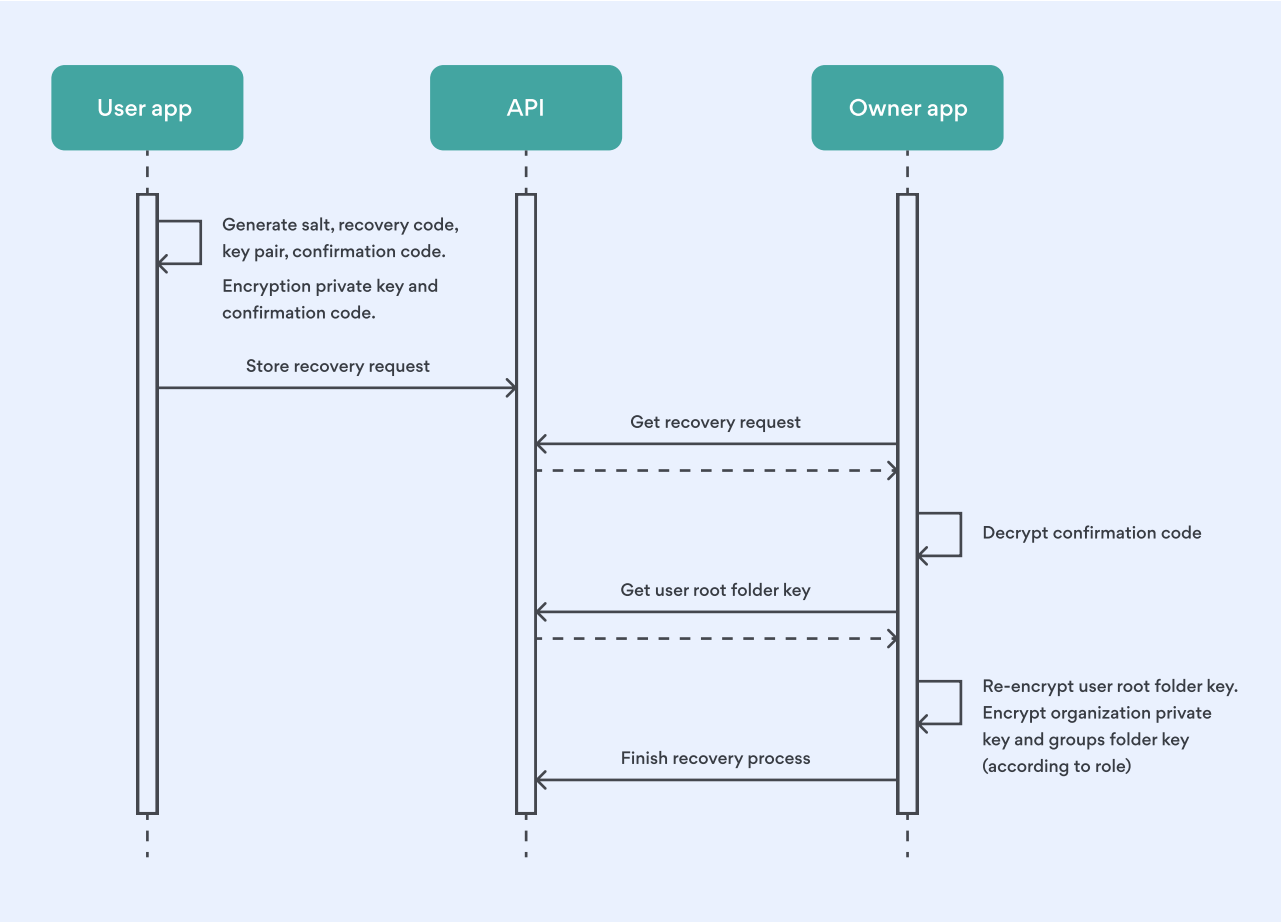
How the request is approved

Only the Organization's Owner(s) can approve requests to recover members' accounts because they are the only ones holding the organization's encryption keys.

Note: We recommend all organizations to have at least two Owners. If one Owner loses their login credentials, the other can recover them. Otherwise, access will be permanently lost.

Here's how the Owner can recover an account:

1. The Owner goes to the Recovery page in the Admin Panel and selects a recovery request.
2. The Confirmation Code decrypted with the organization's Private Key is displayed in plain text.
3. The Owner checks if the Confirmation Code matches with the one provided by the user out-of-band. If it does, the Owner accepts the recovery request.
4. The confirmation of the recovery request initiates these actions:
    a. Decrypt user's root folder metadata and secret data Private Keys with the organization's metadata and secret data Private Keys and encrypt them with the user's new Public Key;
    b. Encrypt organization's metadata and secret data Private Keys with the user's new Public Key (executed optionally if the requesting user's role has to have access to the organization's keys);
    c. Encrypt organization's group folder metadata and secret data Private Keys with the user's new Public Key (executed optionally if the requesting user's role has to have access to the organization's group keys).



What if the request is denied?

If an Owner decides to deny an Account Recovery request, the request will be deleted. Users can then either initiate a new request or try to remember their existing Master Password.

Once the request is initiated, the Owner must approve it within 5 days. Otherwise, the Account Recovery request will expire, and the user will need to submit a new recovery request.

Password Sharing

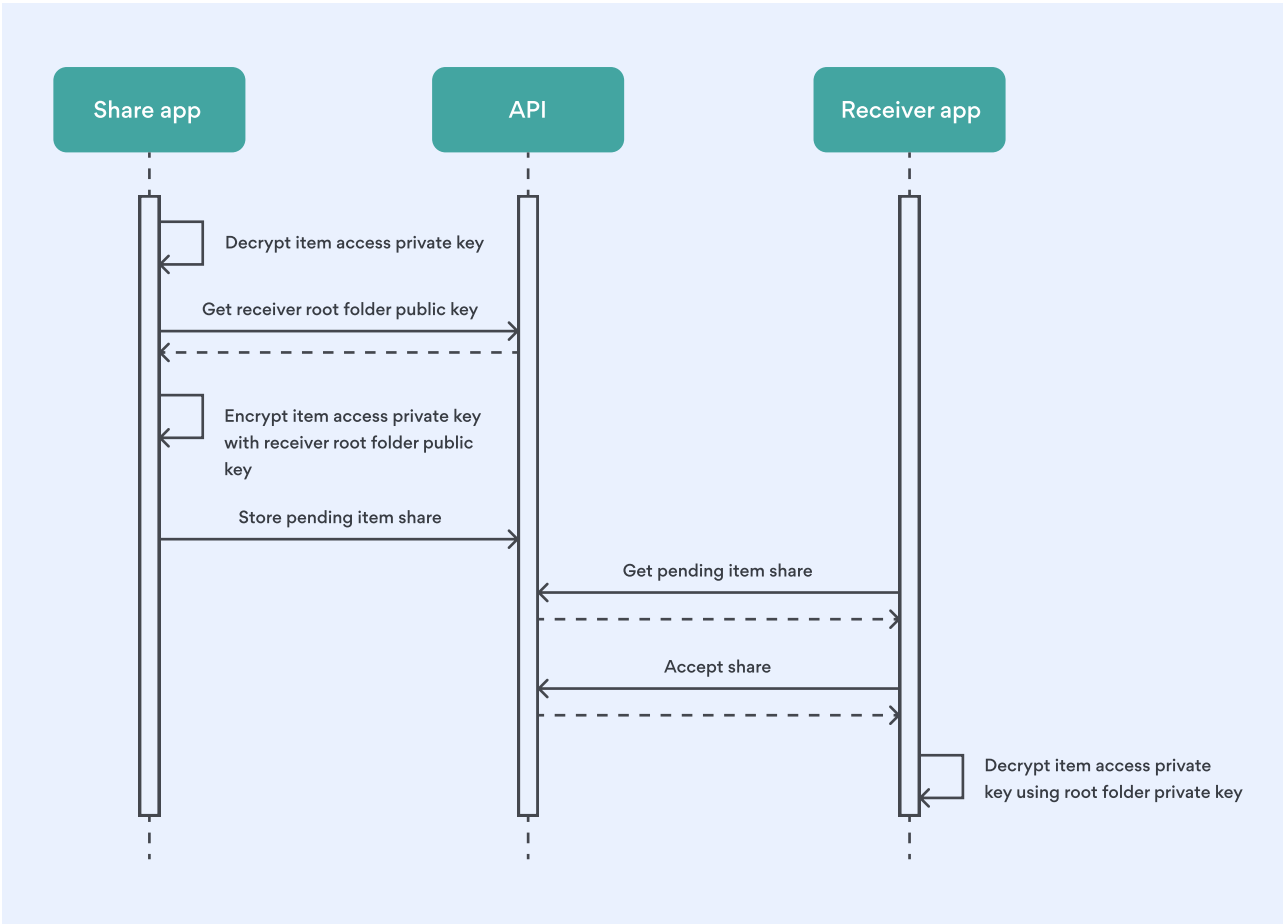
Is it secure?

NordPass allows users to share their items, including passwords, credit card details, secure notes, and personal info.

From a technical perspective, secure item sharing looks like this:

1. The sharer chooses an item and decrypts its access Private Key with their Private Key.
2. The sharer gets the receiver's Root Folder's Public Key from the API.
3. The sharer encrypts the item access Private Key with receiver's root folder Public Key.
4. The receiver gets an email with a pending item shared from the API.
5. If the sharing is accepted, the receiver can decrypt the item access Private Key using his root folder Private Key.

NOTE: If the item is shared with a NordPass B2C account user, the Root Folder steps are skipped as it's only applicable to business users.



It's important to note that we share access to the item — not the data snapshot. This means that, if the user changes any data of that item, it changes for everyone who has access to that item.

Limited rights vs Full rights

When sharing items with others, members can give either full or limited access to that item.

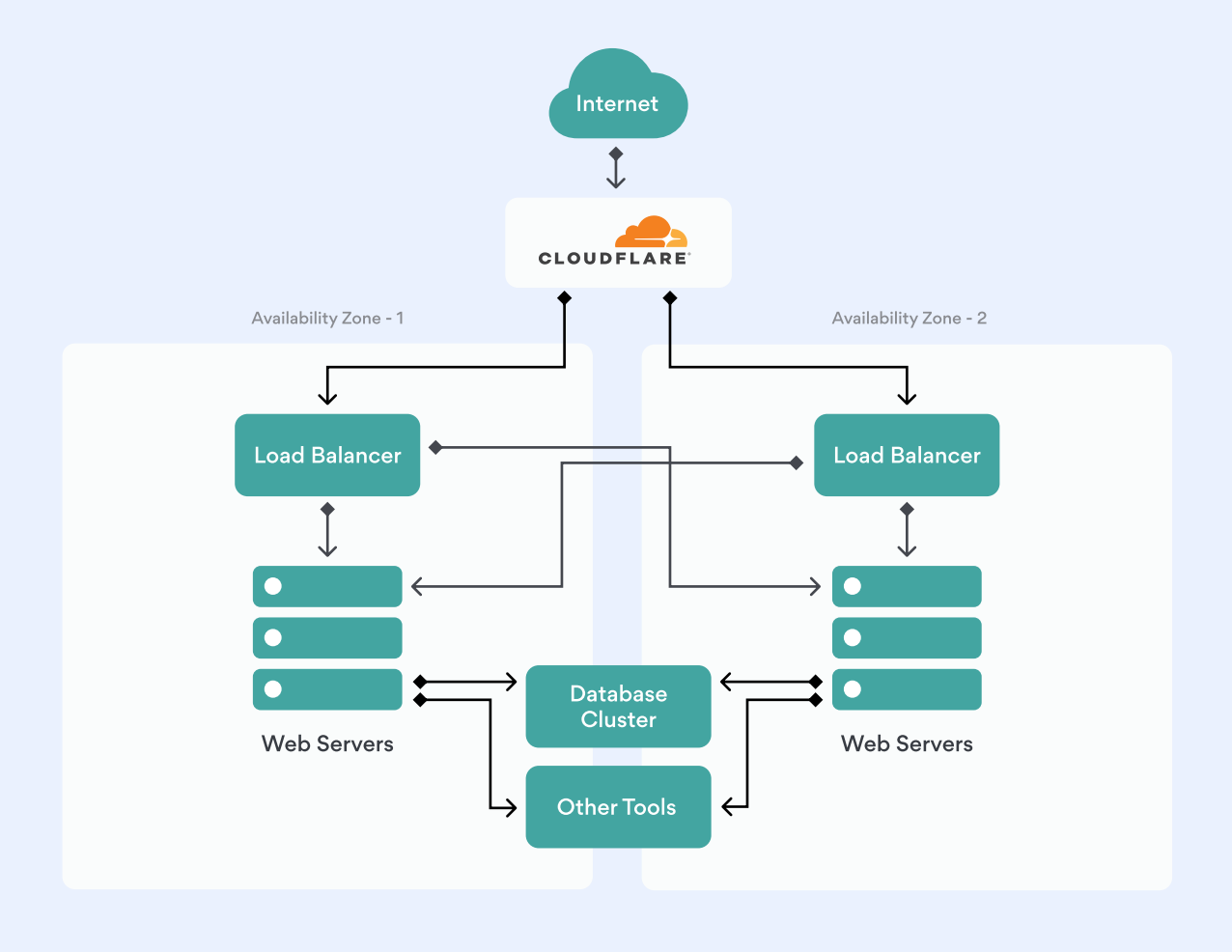
With Full rights, the receiver can access, view, edit, and share the item with others.

With Limited rights, the member can use the item to autofill details when logging in to a specific website, for example. The sensitive information isn't shown in the NordPass app, nor can the receiver change it. However, some websites might display sensitive information when it's autofilled. NordPass is not responsible for and cannot control how sensitive information is displayed outside of the NordPass app.

For a full overview of full and limited rights, please see this article.

Infrastructure

- NordPass uses Amazon Web Services as a cloud provider with its own key management solution for hardware encryption.
- Item storage is processed from the database cluster with active replication. Each cluster member is stored in a different availability zone and meets all the high availability requirements. If one database goes down for any reason, others will seamlessly distribute the load, and our team will be immediately notified.
- Our service is backed by end-to-end encryption architecture, meaning that your data is encrypted and decrypted at the device level. Therefore, the data stored on our servers is always encrypted.
- NordPass is a multi-tenant vault as our infrastructure serves multiple clients.



NOTE: One group or system consists of multiple microservices and groups

Other ways we keep your data safe

External audits

At NordPass, we feel that working with independent third-party auditors is essential. Having an independent team of security experts look into and review our code allows us to improve our service. We believe that building a truly secure product is not a one-time project but an ongoing process. We hope that it also showcases our dedication to transparency and helps us build trust.

How audits happen

We provided the auditors with all the possible information about NordPass, such as access to various materials, documentation, source code, and other data NordPass operates on.

They reviewed our cryptographic premise, the NordPass Business suite software (Desktop app, Android, iOS, browser extensions, Admin Panel, and NordAccount), as well as the background application and its codebase.

The results? No critical issues were identified, which helped NordPass Business to progress from its Beta version.

We will continue to conduct external audits to ensure the highest security standards. For results and more information on future audits, please follow our blog at nordpass.com/blog/.

Internal audits

We have a dedicated Product Security team that continuously performs vulnerability assessments and pentests alongside many other responsibilities. Assessments and pentests are used interchangeably to assess risk posture and identify potential security issues (catalogued in the OWASP Top 10).

This is done as a precautionary measure, and we fix all the security issues as soon as they are identified. However, no matter how big a security issue is, it will never directly affect the user. Even in the unlikely event of NordPass being hacked or the database leaking, none of the information would be accessible to bad actors. NordPass uses end-to-end encryption, and users' data is encrypted locally, which means that any breached data would look like gibberish to intruders.

Logs

App logs are saved on the user's device and are mainly used for troubleshooting. Logs do not contain any data that could be used to identify the user or their device. The user is the only one who can view the logs, which can then be shared with the support team to help them identify any issues and fix them. You can find logs on Windows, macOs, Linux, Android, or iOS devices by following this guide.

Some logs of critical errors are automatically sent to the API, but only if the user has enabled Crash reporting in their Settings. These logs are not tied to any account in any way and cannot be used to identify the user.

Data privacy

Your privacy is important to us. We take all the necessary steps to secure your data, whether it's technical, physical, or administrative.

When providing our services, we are committed to the principles of data privacy laws and make every effort to comply with them, aiming to ensure the lawfulness of processing, data minimization, risk-based approach, and proper security measures.

You can read more about how we protect your privacy in the NordPass Business Privacy policy.

Industry standards and certifications

- **ISO**

The NordPass Business Information Security Management System (ISMS) has been independently audited and certified according to the ISO/IEC 27001:2017 standard, which ensures high efforts in protection of confidential data.

- **SOC 2 Type 1**

NordPass Business has undergone a thorough audit according to the SOC 2 Type 1 procedures. The audit ensures that NordPass Business can securely manage data to protect the interests and privacy of its clients.

- **Cure53**

We take security and transparency seriously. That is why NordPass Business has been subjected and has undergone an extensive security audit performed by Cure53 – an independent German auditor.

- **GDPR**

NordPass makes every effort to comply with GDPR and can help you become GDPR-compliant too. Read this guide to learn how to become GDPR-compliant by protecting the most sensitive information your employees have — their passwords — and protect your customers' data as a result.

- **HIPAA**

If you process sensitive health information, NordPass can help you to get one step closer to being HIPAA-compliant. Read the HIPAA compliance guide to learn how.

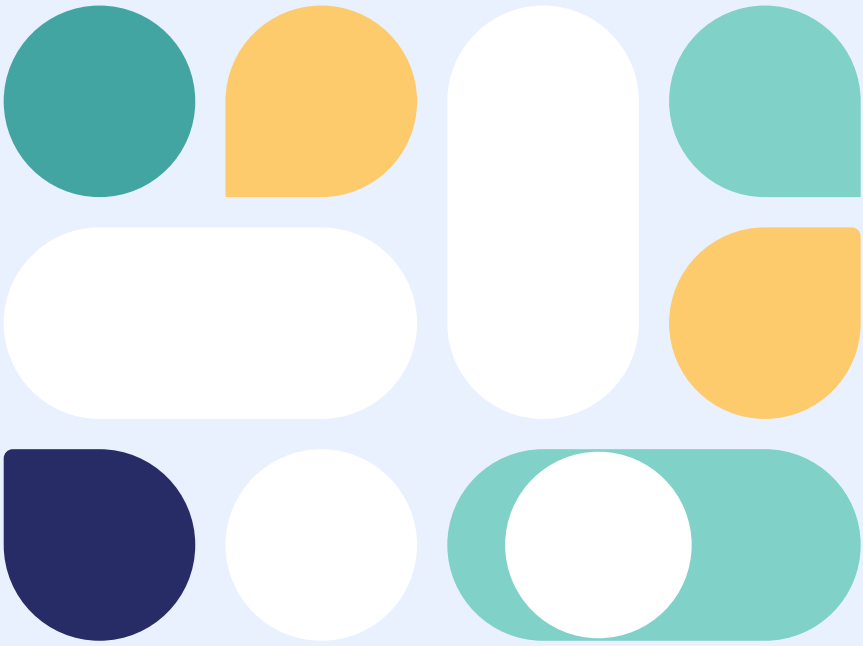
- **California Consumer Privacy Act (CCPA)**

Businesses are required to implement and maintain reasonable security procedures and practices under the CCPA. NordPass is an essential tool that helps its customers to ensure the security of processed personal information and, therefore, can help you with CCPA compliance.

Contact Us

If you have any questions or observations, please contact us.

nordpass@nordsecbusiness.com



Legal disclaimer

This document contains information that is applicable on the day of its issue (as provided above). The document is periodically updated. Nevertheless, as we regularly develop our services and introduce new features to our products, the information provided herein might not correspond to the then-current factual situation. The information is provided for general information purposes only and in good faith. However, we make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information provided in this document.

This document contains privileged and confidential information. It is intended only for the use of the intended recipient(s). If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this document is strictly prohibited