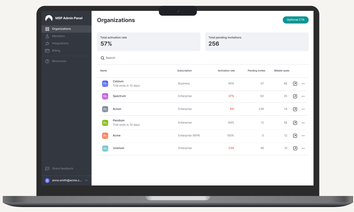
NordPass

How NordPass can help your clients' businesses achieve CIS compliance

simplified

Developed by the Center for Internet Security (CIS), CIS Controls are a collection of prescriptive cybersecurity guidelines. The CIS Controls provide in-depth guidance and a clear path for organizations to improve security infrastructure and mitigate the risks of data breaches and leaks, IP theft, and other cybersecurity threats.

The CIS Controls guidelines also help companies achieve the objectives described by different legal, regulatory, and policy frameworks and meet various compliance standards. Today, being compliant aids organizations in expanding their customer reach and boosting revenue streams.



NordPass is an intuitive business password manager that helps businesses mitigate risks, improve productivity, and comply with strict data security measures. As a product, NordPass can help businesses comply with many of the benchmarks set by the Center for Internet Security's (CIS) Controls. In addition to providing detailed insights to assess your and your customers' digital business security, NordPass offers an array of tools that help stay one step ahead of potential data breaches.

Why should MSPs and their customers use NordPass?

Comply with CIS Controls benchmarks by using NordPass.

3.3 - Configure Data Access Control Lists

Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

NordPass helps businesses stay compliant by hosting passwords and other sensitive data that can be protected by **managing access permissions** for users ranging from limited to full access.

3.11 - Encrypt Sensitive Data at Rest

Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard.

Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

5.2 - Use Unique Passwords

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8 character password for accounts using MFA and a 14-character password for accounts not using MFA.

NordPass excels at facilitating best-practice password implementation for businesses. The product allows businesses to assess their **password uniqueness** and set up a company-wide **Password Policy** to meet security requirements. The **Password Generator** tool helps members quickly and conveniently create passwords that fit the company policy.

NordPass uses **end-to-end encryption** with zero-knowledge architecture. Any passwords or other sensitive data stored in the product are encrypted with **xChaCha20**.

5.4 - Restrict Administrator Privileges to Dedicated Administrator Accounts

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

5.6 - Centralize Account Management

Centralize account management through a directory or identity service.

NordPass can be seamlessly integrated with Okta and Entra ID, facilitating identity and access management capabilities. Additionally, Admins and Owners can monitor Shared Folders and groups where credentials are shared to identify the owners of specific credentials and the members who have access to them. They can also revoke access rights when necessary.

NordPass enables the secure storage and management of all administrator credentials, ensuring that only authorized personnel have access to them. This means that admin credentials can be easily and securely shared between admins only, ensuring that privileged accounts are used strictly for administrative tasks.

6.1 - Establish an Access Granting Process

Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

6.2 - Establish an Access Revoking Process

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

NordPass facilitates **access management** by enabling Admins and Owners to effortlessly provide organization members with the credentials required to log in to specific accounts and platforms. It also allows them to add members to designated groups or Shared Folders, while enabling users to **securely share temporary passwords.**

NordPass can streamline the **process of access removal,** making it easy to quickly revoke a user's access to shared account data.

6.3 - Require MFA for Externally-Exposed Applications

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

6.5 - Require MFA for Administrative Access

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

NordPass includes a **built-in authenticator** that supports setting up MFA for various accounts stored in NordPass, adding an extra layer of security.

In NordPass, an organization can require all its members to **use MFA** when logging in. This ensures that each user goes through an additional verification step beyond entering their password, significantly enhancing account security.

6.7 - Centralize Access Control

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

6.8 - Define and Maintain Role-Based Access Control

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Organization members can use SSO authentication with **Microsoft**, **Google Workspace**, and **Okta** when logging in to NordPass.

8.12 - Collect Service Provider Logs

Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

NordPass allows organizations to assign **different roles** to members for better control over who can access what resources within the organization.

As a service provider, NordPass offers **activity logs** that include a summarized list of actions performed by all members, including vault access, Business Account activity, member invitations, and management, organization setting changes, item access editing, and sharing.

14.3 - Train Workforce Members on Authentication Best Practices

Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

With a **built-in authenticator,** NordPass is designed to help raise awareness and encourage employees to use MFA and secure passwords more effectively, simplifying the implementation of these security measures across their accounts.

Need help getting started?

Visit our Help Center or contact us at partners@nordsec.com