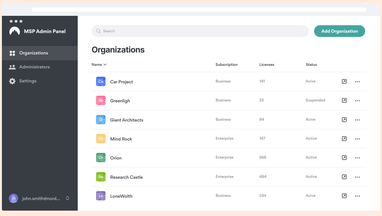
NordPass

How to achieve CIS Compliance with NordPass

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 — the best choice for MSPs



NordPass is an advanced password manager that helps businesses mitigate risks, improve productivity, and meet cyber insurance requirements. 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 security insights to assess your business' digital security, NordPass' array of tools let you stay one step ahead of any potential data breaches.

Why your MSP should 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.

3.6 - Encrypt Data on End-User Devices

Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

NordPass uses end-to-end encryption with zero-knowledge architecture. Any passwords or other sensitive data stored in the product are encrypted with XChaCha20.

3.10 - Encrypt Sensitive Data in Transit

Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

NordPass uses end-to-end encryption with zero-knowledge architecture. Any passwords or other sensitive data stored in the product are encrypted with XChaCha20.

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.

NordPass uses end-to-end encryption with zero-knowledge architecture. Any passwords or other sensitive data stored in the product are encrypted with XChaCha20.

3.14 - Log Sensitive Data Access

Log sensitive data access, including modification and disposal.

NordPass uses end-to-end encryption with zero-knowledge architecture. Any passwords or other sensitive data stored in the product are encrypted with XChaCha20.

4.3 - Configure Automatic Session Locking on Enterprise Assets

Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

Autolock can be enabled in NordPass to lock passwords and other sensitive data hosted in the product after a defined period of inactivity.

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.

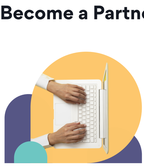
NordPass excels at facilitating best practice password implementation for businesses. The product allows you to assess your business' password uniqueness and set up a company-wide Password Policy to meet security requirements. The Password Generator tool helps members quickly and conveniently create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

17.9 - Establish and Maintain Security Incident Thresholds

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard

NordPass excels at facilitating best practice password implementation for businesses. The product allows you to assess your business' 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 to fit your policy.

Become a Partner



Gain your customers trust by helping them avoid cybersecurity risks with NordPass and take your business to the next level.

Contact us

partners@nordsec.com

nordpass.com