KEEPER
CommSec
Sensible Cyber Security

Data Sheet

Easily Meet ISO 27001 Annex A.9 Requirements With Keeper

ISO 27001 is an international standard for information security that provides a framework and guidelines for establishing, implementing and managing information security management systems. ISO 27001 was designed to help organisations protect critical assets and comply with regulatory requirements necessary for their industry.

As part of achieving ISO 27001 compliance, organisations are required to restrict employees to view only information relevant to their role, reducing the chance of data reaching unauthorised users and risking exposure.

By leveraging Keeper Security's leading cybersecurity solutions, organisations of all sizes can easily and affordably adhere to Annex A.9 of ISO 27001 and strengthen their security posture.

Requirement	Solution
A.9.1.1: Access Control Policy	The access control policy defines the rules and procedures to ensure the security of information assets and enforce least privilege. Keeper provides adherence with Role-Based Access Controls (RBAC) set by administrators to ensure least privilege throughout the organisation. Keeper's Advanced Reporting and Alerts Module (ARAM) seamlessly provides organisations with clear reports on access to privileged assets.
A.9.2.1: User registration and de-registration	Organisations need to ensure there is a formal process governing how users are given access, as well as how access is revoked for company files and services. Keeper's RBAC defines user access policies at the role level and enforces least privilege. Keeper also has Time-Limited Access, allowing users to share records for a set period of time with access being automatically revoked upon expiry. When paired with Keeper Secrets Manager's password rotation, users and administrators can ensure the recipient never has standing access. Decommissioning users within the Keeper platform is simple. Administrators can quickly and easily delete users and transfer the contents of their vault to an appropriate team member, assuring seamless continuance of business operations.
A.9.2.2: User access provisioning	A system, preferably automated, is required to assign and revoke rights throughout the entire organisation. Keeper SSO Connect enables centralised access management, allowing IT teams to monitor and control user access to authorised resources. This approach simplifies access management, improves visibility and ensures compliance with security policies.

Requirement	Solution
A.9.2.3: Management of privileged access rights	Privileged access grants rights to system administrators and those with access to sensitive information. Privileged users are often IT and security administrators, HR professionals, C-level executives or others who need access to privileged systems. ISO 27001 requires a regular review of administrator accounts and a log for all privileged rights. Keeper delivers enterprise-grade password, secrets and privileged connection management in one unified platform. Keeper's solution enables organisations to achieve complete visibility, security, control and reporting across every privileged user on every device.
A.9.2.4: Management of secret authentication information of users	Secret authentication information needs to be highly encrypted and use additional mechanisms to support the security. These systems need to be efficiently managed and remain confidential. Keeper Secrets Manager (KSM) is a fully managed cloud-based, zero-knowledge platform for securing secrets such as API keys, database passwords, access keys, certificates and any type of confidential data. KSM stores all secrets and credentials in the Keeper Vault, with encryption at the record level for the most secure encryption available. Administrators can enforce additional security measures including Multi-Factor Authentication (MFA) and credential rotation to ensure secrets are always secure.
A.9.4.1: Information access restriction	Access control policies must apply to all systems within the company and measures must be set to reflect different levels of access restriction across the organisation. Keeper provides the following for adherence: • Role-based access controls • Granular sharing to enforce rules such as read-only or mandatory shared folder storage of credentials, as well as the ability to revoke sharing access, and limit users to only share or receive credentials internally • Privileged access controls for sensitive information and data
A.9.4.2: Secure log-on procedures	Organisations should apply further methods beyond just passwords to secure log-on procedures. Successful and failed attempts should be recorded. Keeper has several options beyond passwords for log-on methods. Keeper supports a range of MFA solutions, stores and autofills passkeys and supports organisations leveraging Single Sign-on (SSO) solutions to include access to their vaults through their SSO provider, ensuring seamless and secure access. Keeper ARAM empowers teams to support compliance and auditing with more than 200 different event types, including successful and failed log-in attempts, with customised reports, real-time notifications and integration into 3rd party SIEM solutions.

Requirement	Solution
A.9.4.3: Password management solution	Organisations should deploy a password management system to help generate and enforce strong passwords and assist in recovery procedures. Keeper leads the industry in security and compliance certifications and encrypts at the record level, providing the most robust security available in the industry. Every Keeper user has easy access to create passwords and passphrases for all records, ensuring secure passwords are leveraged. BreachWatch by Keeper provides dark web monitoring to alert users and administrators of credentials that have been exposed.
A.9.4.5: Access control to programme source code	Source code is constantly under threat by cyber criminals trying to access company systems. Organisations are required to implement strict access control to protect these systems. Keeper Secrets Manager secures your environment and eliminates secrets sprawl by removing hard-coded credentials from source code, config files and CI/CD systems. Users and administrators should securely store all credentials in their Keeper Vault to eliminate sprawl and provide simple reporting and alerts. Keeper users can manage an unlimited number of secrets, applications and environments.

Keeper is the most secure and user friendly password management solution in the industry.