KEEPER

Gegevensblad

Voldoe met Keeper eenvoudig aan de vereisten voor ISO 27001 bijlage A.9

ISO 27001 is een internationale norm voor informatiebeveiliging die een kader en richtlijnen biedt voor het opzetten, implementeren en beheren van beheersystemen met betrekking tot informatiebeveiliging. ISO 27001 is ontworpen om organisaties te helpen kritieke bedrijfsmiddelen te beschermen en te voldoen aan de wettelijke vereisten die nodig zijn voor hun branche.

Als onderdeel om te kunnen voldoen aan de ISO 27001-norm, zijn organisaties verplicht om beperkingen in te stellen, waarbij werknemers alleen informatie kunnen bekijken die relevant is voor hun functie. Zo wordt de kans kleiner wordt dat gegevens bij onbevoegde gebruikers terechtkomen. Dit zou namelijk het risico op blootstelling van die gegevens vergroten.

Door gebruik te maken van de toonaangevende cyberbeveiligingsoplossingen van Keeper Security, kunnen organisaties van elke omvang eenvoudig en op een betaalbare manier voldoen aan bijlage A.9 van ISO 27001 en zorgen voor een betere beveiliging.

Vereiste	Oplossing
A.9.1.1: Beleid voor toegangscontrole	Het beleid voor toegangscontrole definieert de regels en procedures om de beveiliging van gegevens in de vorm van een bedrijfsmiddel te waarborgen en de minimale privileges af te dwingen. Keeper biedt naleving van Role-Based Access Control (RBAC) die door beheerders is ingesteld om de minimale privileges voor de hele organisatie te waarborgen. De Geavanceerde rapportage- en alarmmodule (ARAM) van Keeper biedt organisaties naadloos heldere rapporten over toegang tot geprivilegieerde bedrijfsmiddelen
A.9.2.1: Registratie en uitschrijving van gebruikers	Organisaties moeten ervoor zorgen dat er een formele procedure in plaats is gesteld voor zowel het verlenen van toegang aan gebruikers toegang, als het intrekken van de toegang tot bedrijfsbestanden en -diensten. De RBAC van Keeper dwingt de minimale privileges af en definieert het beleid voor gebruikerstoegang die afhankelijk is van de functie. Keeper heeft ook een tijdbeperkte toegang, waardoor gebruikers gedurende een vooraf bepaalde tijd bepaalde records kunnen delen. Deze toegang wordt automatisch ingetrokken na afloop van die periode. In combinatie met de wachtwoordrotatie van Keeper Secrets Manager kunnen gebruikers en beheerders ervoor zorgen dat de ontvanger nooit permanente toegang heeft. Het is eenvoudig om de toegang in te trekken en gebruikers te verwijderen binnen het Keeper-platform. Beheerders kunnen gebruikers snel en eenvoudig verwijderen en de inhoud van hun kluis overdragen aan een ander teamlid, waardoor de bedrijfsactiviteiten naadloos worden voortgezet.
A.9.2.2: Inrichting van de gebruikerstoegang	Er is een (bij voorkeur geautomatiseerd) systeem nodig voor het toewijzen en intrekken van rechten in de hele organisatie. Keeper SSO Connect maakt gecentraliseerd toegangsbeheer mogelijk, waardoor IT-teams de gebruikerstoegang tot geautoriseerde bronnen kunnen controleren en bewaken. Deze aanpak vereenvoudigt het toegangsbeheer, verbetert de zichtbaarheid en zorgt voor naleving van het beveiligingsbeleid.
A.9.2.3: Beheer van geprivilegieerde toegangsrechten	Geprivilegieerde toegang verleent rechten aan systeembeheerders en personen met toegang tot gevoelige gegevens. Geprivilegieerde gebruikers zijn vaak IT- en beveiligingsbeheerders, HR-personeel, directieleden of anderen die toegang nodig hebben tot geprivilegieerde systemen. ISO 27001 vereist een regelmatige controle van beheerdersaccounts en een logboek voor alle geprivilegieerde rechten. Keeper biedt het beheer van zakelijke wachtwoorden, geheimen en geprivilegieerde toegang op één uniform platform. Keeper's oplossing stelt organisaties in staat om volledige zichtbaarheid, beveiliging, controle en rapportage te hebben over elke geprivilegieerde gebruiker, op elk apparaat.

Vereiste	Oplossing
A.9.2.4: Beheer van geheime authenticatiegegevens van gebruikers	Geheime authenticatiegegevens moeten sterk versleuteld zijn en extra mechanismen inzetten om de beveiliging te versterken. Deze systemen moeten efficiënt worden beheerd en vertrouwelijk blijven. Keeper Secrets Manager (KSM) is een volledig beheerde cloudgebaseerde, zero-knowledge platform voor het beveiligen van geheimen zoals API-sleutels, databasewachtwoorden, toegangssleutels, certificaten en elk type vertrouwelijke gegevens. KSM slaat alle geheimen en inloggegevens op in de Keeper Vault, met versleuteling van alle records afzonderlijk, om zo de hoogst mogelijke versleuteling te bieden. Beheerders kunnen extra beveiligingsmaatregelen afdwingen, waaronder multifactorauthenticatie (MFA) en rotatie van inloggegevens om ervoor te zorgen dat geheimen altijd veilig zijn.
A.9.4.1: Beperking van de toegang tot gegevens	Het beleid voor toegangscontrole moet gelden voor alle systemen binnen het bedrijf en de maatregelen moeten worden ingesteld op verschillende niveaus van toegangsbeperking binnen de organisatie. Keeper biedt het volgende voor naleving: • Functiegebaseerde toegangscontroles • Gedetailleerd delen om regels af te dwingen, zoals het opslaan van inloggegevens voor alleen-lezen of verplichte gedeelde mappen, evenals de mogelijkheid om de gedeelde toegang in te trekken en gebruikers te beperken om alleen inloggegevens intern te delen of te ontvangen • Geprivilegieerde toegangscontroles voor gevoelige gegevens en overige informatie
A.9.4.2: Veilige inlogprocedures	Organisaties moeten meer methoden toepassen dan alleen wachtwoorden om inlogprocedures te beveiligen. Succesvolle en mislukte pogingen moeten worden geregistreerd. Keeper heeft verschillende opties naast wachtwoorden voor inlogmethoden. Keeper ondersteunt een reeks MFA-oplossingen, slaat passkeys op en vult ze automatisch in en ondersteunt organisaties die Single Sign-on (SSO)-oplossingen gebruiken om toegang te krijgen tot hun kluizen via hun SSO-provider, waardoor een naadloze en veilige toegang wordt gegarandeerd. Keeper ARAM stelt teams in staat om naleving en audits te ondersteunen met meer dan 200 verschillende soorten evenementen, waaronder succesvolle en mislukte inlogpogingen, met aangepaste rapporten, realtime meldingen en integratie in SIEM-oplossingen van derden.
A.9.4.3: Oplossing voor wachtwoordbeheer	Organisaties moeten een systeem voor wachtwoordbeheer implementeren om sterke wachtwoorden te genereren en ondersteuning te bieden om herstelprocedures af te dwingen. Keeper is toonaangevend in de sector op het gebied van beveiligings- en nalevingscertificeringen en versleutelt alle records afzonderlijk, waardoor de hoogst mogelijke beveiliging kan worden geboden in de branche. Elke Keeper-gebruiker heeft eenvoudige toegang om wachtwoorden en wachtwoorden aan te maken voor alle records, zodat er kan worden gegarandeerd dat gebruikers veilige wachtwoorden gebruiken. BreachWatch van Keeper biedt dark web-monitoring om gebruikers en beheerders te waarschuwen voor inloggegevens die zijn blootgesteld.
A.9.4.5: Toegangscontrole tot de broncode van het programma	Broncodes wordt voortdurend bedreigd door cybercriminelen die toegang proberen te krijgen tot bedrijfssystemen. Organisaties zijn verplicht om een strikte toegangscontrole te implementeren om deze systemen te beschermen. Keeper Secrets Manager beveiligt uw omgeving en elimineert het verspreiden van geheimen door hard-coded inloggegevens te verwijderen uit de broncode, configuratiebestanden en CI/CD-systemen. Gebruikers en beheerders moeten alle inloggegevens veilig opslaan in hun Keeper Vault om sprawl te voorkomen en eenvoudige meldingen en waarschuwingen te verstrekken. Keeper-gebruikers kunnen een onbeperkt aantal geheimen, applicaties en omgevingen beheren.