visits

PasswordGuard

Powered by KEEPER

A password manager is a must-have for any organisation.

Mitigate against risk and impact of data breaches

Create random, high-strength passwords for your websites/applications and store them in a secure vault.

Increase data security controls for your applications and data

Auditing, reporting, alerting and policies all help to strengthen your security posture and protect what matters most.

A private vault for every employee

Everyone gets a private vault to store and manage their passwords, files and private client data. Store credit cards, ID and other sensitive data.

Shared folders for your teams and projects

Securely create, share and manage both individual records and encrypted folders across teams or individual users.

Secure file storage

Protect sensitive documents and files, maintaining the same security controls as passwords.

Version control and record history

Access a full history of records, view previous versions, see what's changed and recover records at any time.

Password security audit score and reporting

Visibility into your password security with robust reporting and auditing tools to enforce internal controls and maintain compliance standards.

visits

PasswordGuard

Powered by KEEPER

Keeper protects your business with market-leading security.

Private master password

Only the user has knowledge of and access to their Master Password and key that is used to encrypt and decrypt their information.

Multi-factor authentication

Keeper supports MFA, biometric login and Keeper DNA which uses the Apple Watch or Android Wear device to confirm your identity.

Strongest encryption

Keeper protects your information with AES 256-bit encryption and PBKDF2, widely accepted as the strongest encryption available.

Secure & reliable cloud vault

Keeper utilises Amazon AWS in multiple geographic locations to host and operate the Keeper Vault. Data at rest and in transit is fully isolated.

Deep-level encryption

User data is encrypted and decrypted at the device level not on Keeper's servers or in the cloud.

Keeper has the longest standing SOC 2 Type 2, ISO 27001 and TRUSTe certification in the industry. Keeper's ISMS will ensure that strict security controls are in place to protect customer data and ensure secure operation of the products and services.

SOC 1 / SSAE 16 / ISAE3402 (SAS70)

SOC 2

SOC 3

ISO 27001

GDPR Compliant

HIPAA Compliant

For more information on the Keeper security architecture, including accreditations, please visit: https://www.keepersecurity.com/security.html

VISITS

PasswordGuard

Powered by KEEPER

Editions & Pricing

	Business	Business Plus	Enterprise Plus
Encrypted vault for every user	✓	✓	✓
Shared team folders	✓	✓	✓
Access from web, desktop and mobile	✓	✓	✓
Password strength and re-use reporting	✓	✓	✓
Multi-factor authentication	✓	✓	✓
Security policy management and role-based access controls	✓	✓	✓
FREE personal plan for each staff member[1]	✓	✓	✓
Secure file storage	100GB	1TB	1TB
Audits all activity	✓	✓	✓
Dark web breach monitoring for stored passwords		✓	✓
Advanced reporting and alerting module (ARAM)[2]		✓	✓
Single Sign-On / Active Directory integration			✓
Ability to automate staff provisioning and permission changes based on groups			✓

NOTE: VISITS bills **monthly**. There is no need to purchase an annual plan.

[1] If the staff member leaves, their plan reverts to the limited free tier. They can then choose to upgrade their plan to a paid version.

[2] Alerts are configured to send to nominated champions ('owners of the system')

PasswordGuard

Powered by KEEPER

VISITS Support Package

Our support includes the following features:

- **Assist your staff with using Keeper**
  We'll help individuals with questions and issues when using the Vault.[1]
- **Deployment of Keeper software**
  If we manage your computer fleet, we'll install and manage the Keeper client and browser plugins.
- **Training content on our hubl portal**
  Access tips and information on how to use Keeper, managing passwords and other cybersecurity content.
- **User account management**
  We manage users and teams on your behalf.

Ad hoc services

Policy changes

We can adjust security policies and hierarchy as required.
Additional fees apply.

[1] We can assist with using the Keeper application only. We do not have any access to your data and therefore cannot access or change records.

visits

PasswordGuard

Powered by KEEPER

Standard implementation services

Our standard implementation of Keeper Password Manager ensures that you maximise the solution from the first day of use.

It is vital that all your staff are involved and see the value/importance of using a password manager.

The standard scope includes:

- **Planning session**
  Discuss the necessary steps for your business to successfully adopt the Keeper Password Manager.
- **Webinar training**
  We train both champions (the people who 'own' the system) and staff with a structured webinar.
- **Single sign-on / Active Directory integration (Enterprise only)**
  Your existing SSO solution or AD is integrated into Keeper for user authentication and provisioning.
- **Standard configuration**
  We deploy a standard security framework and hierarchy for a balance between security and convenience.
- **Reporting & Alerts**
  Configure notifications to your champions when important events occur
- **Templates**
  Several document and communication templates are provided to you to help drive adoption and governance.

Optional implementation services

Readiness assessment

We work with your business stakeholders and staff to analyse and document how you currently store passwords and other secrets (such as codes, credit cards and highly sensitive documents).

This service complements our implementation to provide an end-to-end integration of Keeper into your business.

Implementation for IT Teams

A lean project for IT teams who wish to implement and manage the solution themselves.

We provide the necessary training and assistance to empower your IT team to deploy and manage Keeper.

PasswordGuard

Powered by KEEPER

Frequently asked questions

How secure is Keeper?

Keeper uses a multitude of industry leading security frameworks and architectures to protect the application and the Vault. We suggest you read through Keeper's security overview by visiting https://www.keepersecurity.com/security.html.

Does Keeper and/or VISITS have access to my organisation's data?

No. Only your account has access to your records. Only through sharing are others allowed to access records you own.

The combination of your master password, two-factor authentication and secret question/answer protects your account from being accessed by others, including by administrators, VISITS and Keeper Security.

VISITS can only perform user, team and policy changes to your tenant.

What happens when data is deleted?

Upon deletion, records are moved to a recycle bin where they can be restored at any time.

After a period of time (determined by policy), they can be purged from Keeper and are then deleted permanently. Permanently deleted items cannot be recovered.