TOSHIBA

Password Security

> Protect your business from password-related data breaches and cyber threats

> Zero-knowledge platform that scales to meet the size and requirements of your organisation

> Generate strong, random passwords and automatically fill them for users

> Mitigate risk by storing high-strength passwords in a secure vault

Password manager for protecting your business.
Keeper Business Password Manager* is the leading cyber security platform protecting millions of people and thousands of businesses globally, by preventing password-related data breaches and cyber threats.

Implementing secure business passwords across your organisation will improve productivity, by saving employees time, frustration and eliminate the need for them to reset, reuse and remember passwords.

Keeper also enforces compliance standards by supporting role-based controls, 2FA, auditing, event reporting and industry compliance with HIPAA, DPA, FINRA, GDPR and more.

KEEPER®

TOGETHER INFORMATION

*Delivered in conjunction with Keeper Security and Brigantia.

KEEPER®

Cyber security starts with password security

Individuals and businesses often deal with the password issue by using shortcuts.
For example, they choose simple passwords that are easy to guess, they use the same password for every online account, or they write those passwords on sticky notes stuck to the side of their monitor. Such methods may seem like an easy way to avoid the work of creating and using secure passwords, but they make it easy for cyber criminals to do their damage. People need a far more secure and convenient way to protect their online accounts and other online assets.

Save employees time, frustration and eliminate the need for them to reuse and remember passwords. Keeper will generate strong, random passwords and automatically fill them for users. The Keeper vault, with a responsive and intuitive user interface (UI), is available to employees from any device and location. Everything Keeper does is geared towards quick user adoption and security

Key benefits:

- An encrypted vault for every user, with folder and sub-folder functionality
- The ability to created shared team folders
- Allows access from unlimited devices
- A strong policy engine with enforcement
- Built-in, continuous security audit
- Advanced activity reporting and an alerts module
- Two-Factor Authentication (SMS, TOTP, smartwatch, DUO, RSA and FIDO U2F)
- Single Sign-On (SAML 2.0) authentication
- Active Directory and LDAP sync
- SCIM and Azure AD provisioning
- Email auto-provisioning and ability for command-line provisioning
- Developer APIs for password rotation and backend integration
- 1TB Secure Storage

Key features include:

BreachWatch® by Keeper | Scans employees' Keeper vaults for passwords that have been exposed on the dark web from a public data breach and notifies the user to take action. It also informs the administrator whether that employee has resolved the exposed password or ignored it.

Security Audit Score and Reporting | Provides password security visibility with robust reporting and auditing tools to enforce internal controls and maintain compliance standards.

Admin Console | Distributes, manages and monitors across the entire organisation and enforces password security, 2FA and other data security policies.

Safeguard your business with Password Security
Contact our Managed IT Services team to take the next step.

Toshiba Tec UK Imaging Systems Ltd.

T 020 7735 9992 | **E** managed.itservices@toshibatec.co.uk | **W** www.toshibatec.co.uk

Toshiba Tec UK deliver these services in conjunction with Keeper Security and Brigantia.
www.brigantia.com | www.keepersecurity.com