Magoo & Associates LLC
"Your technology solution provider"

WHY YOUR ORGANIZATION NEEDS A CENTRALIZED PASSWORD MANAGER

Weak or compromised passwords cause about 80% of successful data breaches, yet many organizations still don't mandate that their employees use a password manager, resulting in a lack of consistency, visibility, and centralized administration.

Here are 6 reasons why organizations need to centralize their entire organization under a single business password management solution such as Keeper.

Obtain Complete Visibility into Employee Password Practices

If password management isn't centralized, IT administrators have no visibility into employee password practices. Visibility has always been an issue, but it's even more important now that so many employees are working remotely.

Keeper's zero-knowledge password management and security platform provides administrators with complete visibility into employee password practices through one centralized console, whether employees are working on-site, remotely, or a combination of both.

Ability to Standardize and Enforce Password Policies

Standardizing under one centralized password management platform allows organizations to standardize and enforce password security policies across the organization, such as strong, unique passwords and using multi-factor authentication (2FA) on every site that supports it.

Using Keeper's admin console and policy enforcement tools, IT administrators can ensure that all employees are adhering to organizational password policies.

Ability to Implement Role-based Access Control

Every employee should have only as much system access as they need to perform their jobs, and no more. In addition to helping prevent insider attacks, this helps organizations limit their exposure if an employee account is compromised.

Keeper enables organizations to implement role-based access control (RBAC) and monitor accounts for anomalous activity that could indicate misuse or compromise.

Secure Password Sharing for Teams

Without a business password manager, employees who need to share passwords will use insecure and inefficient sharing methods, such as email, text messaging, or writing the passwords down.

Keeper allows organizations to create secure shared folders for individual departments, project teams, or any other group.

Simplified Onboarding/Offboarding for New and Departing Employees

When all employees are using the same password manager, onboarding of new hires is a snap, even when part or all of the team is working remotely. Using Keeper, IT administrators can get new employees set up and ready to go in only a few minutes.

Former employees who are still in possession of working passwords are a huge cyber risk. When employees leave the company, all of their system access should be terminated immediately. In addition to giving IT administrators the ability to immediately revoke access for former employees, Keeper allows organizations to opt to mask current employees' passwords across the platform.

Ability to Monitor the Dark Web for Compromised Passwords

Cybercriminals frequently attack Software as a Service (SaaS) developers and other vendors with the goal of stealing credentials belonging to their clients' employees. Because it can take a breached organization months to detect a breach, the victims of these third-party breaches are typically the last ones to know they've been compromised.

Keeper **BreachWatch**™ scans Dark Web forums and notifies organizations in real-time if any of their employee passwords have been put up for sale. BreachWatch seamlessly integrates with the Keeper password management platform, enabling IT administrators to force password resets right away.

Talk to your Account Manager about how you can expand Keeper's top-rated cyber protection to the rest of your organization.

Not a Magoo customer yet? Speak with an Account Manager to discover how Magoo can protect your business through a layered approach to cyber security.