KEEPER

Keeper Cyber Essentials

Easily Meet Cyber Essentials Requirements with Keeper

Cyber Essentials is a UK government-backed cybersecurity certification providing a baseline for organisations to guard against online threats, which covers essential cybersecurity measures. Cyber Essentials Plus is an advanced certification with a more rigorous assessment, including hands-on verification, to ensure effective defence. Both certifications demonstrate a commitment to cybersecurity best practices and enhancing overall resilience.

By leveraging Keeper Security's leading cybersecurity solutions, organisations of all sizes can easily and affordably streamline their compliance process and improve their overall security posture.

Requirement	Solution
Protection against brute force password guessing	Organisations are required to adhere to several regulations to protect against brute force attacks, including locking accounts after a set amount of unsuccessful attempts and limiting the number of guesses allowed in a specified time period. Keeper provides the ultimate protection against these types of attacks by requiring Two-Factor Authentication (2FA) in advance of users entering their master password. This level of authentication ensures that only the authorised user can access a Keeper Vault.
Set a minimum password length of at least 8 characters	Cyber Essentials requires organisations to set a minimum password length of at least 8 characters. By default, Keeper requires a 12 character length for master passwords. Keeper Administrators have the ability to set minimum password complexities combining password length and types of characters required.
Do not set a maximum password length	Cyber Essentials mandates that organisations cannot set a maximum password length. Keeper's Password Generator supports password creation up to 100 characters.
Change passwords promptly when compromise is known or suspected	Passwords need to be changed quickly when there is knowledge or even suspicion that they could be breached. Organisations face serious consequences when user passwords are breached or stolen, and sold on the dark web. BreachWatch is a powerful dark web monitoring tool that can be added on to Keeper Password Manager. BreachWatch constantly scans Keeper Vaults for passwords that have been exposed on the dark web and immediately alerts users to take action and protect themselves and their organisations.

Requirement	Solution
Avoid choosing obvious and common passwords	Avoiding easy-to-guess passwords heightens an organisation's security posture. Furthermore, randomising passwords and enforcing complexity, while not required, also significantly increases security. Keeper recommends organisations require the use of a password generator to mitigate the risks associated with users choosing obvious passwords. Leveraging Keeper's Password Generator helps organisations achieve compliance with the following Cyber Essentials requirements: • Avoid choosing obvious passwords, such as those based on easily discoverable information like the name of a favourite pet. • Not to choose common passwords.
Do not reuse passwords	Adherence to Cyber Essentials requires administrators to deploy a password policy that requires users to not use the same password on multiple accounts. Keeper streamlines this policy by providing each user with a Security Audit tab in their Keeper Vault. Security Audit provides information about password strength and notifies users and administrators of password reuse. To preserve zero-knowledge, the summary of each Security Audit score is encrypted with the Enterprise Public Key, then stored encrypted in the Keeper Cloud.
Define where and how to store passwords securely	Organisations are required to outline where and how users should store passwords and references a sealed envelope in a secure cupboard. This is a dated and insecure method of securing passwords. Keeper recommends all passwords are stored in a password manager. Users need to only memorise their master password, simplifying password usage and securing organisations.