Donation Policy
(How do we spend your donations?)

This policy will be reviewed on an ongoing basis, at least once a year. Time to Help UK will amend this policy, following consultation, where appropriate.

Date of last review: 16/03/2023

[Registered Charity Number: 1160467 | Company Number: 08659663]

Overview

Employees at "Time to Help UK" are given access to various IT resources, including computers and other hardware devices, data storage systems, and other accounts in the course of carrying out their duties.

Passwords are a crucial part of our cyber security strategy and are fundamental to protecting the business and, therefore, our employees' livelihood.
All employees who have access to those resources are responsible for choosing strong passwords and protecting their login credentials.

The purpose of this policy is to make sure all "Time to Help UK" resources and data receive adequate password protection. We cannot overstate the importance of following a secure password policy and therefore have provided this document for your guidance. The policy covers all employees responsible for one or more accounts or access to any resource that requires a password.

Password Creation

- All passwords should be sufficiently **complex** and challenging for anyone to guess. **Employees should choose passwords that are at least** twelve characters long and contain a combination of upper- and lower-case letters, numbers, punctuation marks and other special characters.
- In addition to meeting those requirements, employees should also use common sense when choosing passwords. **They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1", and "Pa$$w0rd" are equally bad from a security perspective**.
- A password should be **unique**, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to selecting a strong password that is still easy to remember is: Pick a phrase, take its initials, replace some of those letters with numbers and other characters, and mix up the capitalisation. For example, "This may be one way to remember" can become "TmB0WTr!".
- Employees must choose **unique** passwords for all their company accounts and may not use a password they are already using for a personal account.
- It will be necessary to change passwords at specific frequencies in some cases. This requirement will be enforced using software when possible.
- If the security of a password is in doubt– for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.

- Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

Important!:

- Never use personal information such as your name, birthday, user name, or email address. This type of information is often publicly available, making it easier for someone to guess your password.
- Use a longer password. Your password should be at least twelve characters long, although it should be even longer for extra security.
- Don't use the same password for each account. If someone discovers your password for one account, all of your other accounts will be vulnerable.
- Include numbers, symbols, and both uppercase and lowercase letters.
- Avoid using words that can be found in the dictionary. For example, swimming1 would be a weak password.

Use Multi-Factor Authentication (MFA) For Important Accounts

One of the most effective ways of providing additional protection to a password-protected account is to use MFA. Accounts that have been set up to use MFA require a second factor, which is something that you (and only you) can access. This could be a code that's sent to you by text message or created by an app, so even if an attacker discovers a password, they won't be able to access the associated account without compromising the other factor.

MFA is best used where there may be an additional risk (such as logging into an account on a new device, internet-facing systems, or priority accounts). Refer to the NCSC's guidance on Multi-factor authentication for online services for more detailed information.

Protecting Passwords

- Passwords must be secret; employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their unique password.

- Employees may never share their passwords with anyone internal or external to the business, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and additional sensitive information. All employees will receive training on how to recognise these attacks.

Protect Passwords In Transit

Passwords can be intercepted when in transit. To protect them, you should ensure that all corporate web apps requiring authentication use HTTPS. A common type of attack involves stealing a security token to gain access to another device or server. 'Pass the hash' is an example of this, where a stolen hash is used to authenticate the attacker. For more information, refer to the NCSC guidance on preventing lateral movement.

Storing Passwords

- Employees must refrain from writing passwords down and keeping them at their workstations.
- Employees are encouraged to use password managers but should discuss with the SLT or IT support to agree on the suitability of the chosen application and best use practices.

Review interval	Next review due by	Next review start
1 year	January 2023	January 2023
2 year	March 2024	January 2024

Version history

Version	Date	Approved by	Notes
1.0	2022	Board	(First Draft)

End of Policy