holibob

Password Management - Policy

Version: 3

29 October 2024

Table of Contents

1 Introduction

This document provides guidance on the use of passwords and Personal Identification Numbers (PINs) within Holibob.

The document helps you protect our IT systems by telling you about choosing and using passwords and PINs.

Whenever you encounter the word "system" here, it applies to:

- **Hardware** - such as laptops, PCs, servers, mobile devices, and any IT equipment.
- **Software** - such as the Operating System, or applications installed on hardware, or mobile device applications (apps).
- Services - such as remote databases or cloud-based tools like Teams, OneDrive, SharePoint etc.

This guidance is for all users. It also includes more detail for system administrators or developers.

Note: Except where stated, the guidance in this article applies to both passwords and PINs.

2 General best practices

You shall not share your password or account details with **anyone**, unless you have documented approval to do so from an employee of The Company with a level of Director or higher.

If a system or another person provides you with a password, change it before doing any work on the system that it grants access to.

Examples of 'single-use' passwords include:

- the account you use on a work-provided laptop.
- A shared account for accessing a data analytics service.
- All vendor-supplied accounts such as Teams, OneDrive, Spendesk, Ticketing systems, and Monitoring systems.

You shall change a password whenever:

- There has been a security incident involving your account or password. For example, someone guessed your password, or you used it on another account.
- There was a security incident with the service that you access using the password. For example, if someone broke into the system that provides the service you use.
- Your line manager or other authorised person tells you to do so.

When required to change a password, **you shall** do so as soon as possible.

If you don't change the password soon enough, you might be locked out of your account automatically.

2.1 Best password practices for everyone

The Company password guidance follows NCSC guidance[1]. The NCSC recommends a simpler approach to passwords.

Some systems might have specific additional requirements or variations. Check your team Intranet or ask your Line Manager for more information.

Follow the CyberAware advice[2] to generate your passwords.

Always use a separate and unique password for each account or service.

It is essential that you never use the same password for access to different systems and that you never use a password within The Company's systems that you also use for any personal system.

This is critical to all of our security and prevents a situation where a single system is compromised by a bad-actor who is then able to gain details of your email/username and password and attempt to access other systems with the same.

2.1.1 The basic rules for passwords

The most important points to remember are that passwords should be:

1 https://www.ncsc.gov.uk/guidance/using-passwords-protect-your-data
2 https://www.cyberaware.gov.uk/passwords

- At least 8 characters long.
- No more than 128 characters long.
- Not obvious.
- Not a dictionary word. A combination of dictionary words might be suitable, such as "`CorrectHorseBatteryStaple`".
- Unique for each account or service.

2.1.2 The basic rules for PIN numbers

Some devices, especially mobile devices, only support numerical passwords, or Personal Identification Numbers (PINs).

If the device supports passwords, then passwords **should** be used rather than PINs.

If the device supports only PINs, you **should**:

- Always use a separate and unique PIN for each account or service.
- Ensure the PIN is at least 4 characters long.
- Avoid using obvious PINs, such as `1234`.
- Avoid using repeating digits in the PIN, for example, `0000` or `9999`.

2.2 App-based password protection for files

Some applications - including Microsoft Office tools such as Word, Excel, and PowerPoint - provide mechanisms for protecting files. A password controls whether someone can open, or edit, a file.

While these app-based password protection mechanisms are better than nothing, there are three good reasons for avoiding them if possible.

- You depend on the application to provide and maintain strong password protection. If the password implementation fails, or has a weakness, you might not know about it. This means that you might think your information is protected, when in fact it is at risk.
- It is tempting to use a standard password for protecting a file within the app, so that other people can share and work with the file. Changing the password becomes "inconvenient". The result is that many versions of the data file are all protected with the same password. Also, if anyone has ever been given the password to access the file, they will always be able to access the file.

- If you forget the app-based password, there might not be a recovery process available to you.

For these reasons, The Company advice is that you **should not use password tools within an app** to protect data files that are processed by the app.

For example, you should not use the password protection options within Microsoft Word, Excel, or PowerPoint.

To protect information within files

- Store the data files in a shared but secure area company repository such as a OneDrive/SharePoint storage facility.
- Use separate encryption tools to protect data files, separate from the app that works with the data files.

Of these two options, storing data files in a shared but secure area is strongly preferred. The reason is that you can add, modify, or revoke access permissions to the storage area easily.

If you have no choice and have to use app-based password protection, ensure that the same password is not used indefinitely for a data file. You **should** use a different password for:

- Each major version of a data file, for example version 2.x is different to version 3.x.
- Any data file where the password is more than three months old.

Note: This advice is a specific exception to the general guidance, that you do not normally need to change passwords.

2.3 Password expiry

You don't have to change a password because it is old. The reason is that the time-expiry of passwords is a outdated and ineffective practice.

Some current or legacy systems don't allow passwords that follow The Company's guidance. For example, some mobile devices, laptop hard drive encryption tools, or older computers might not be able to support a mix of character types. For such systems, choose passwords that are as close as possible to the guidance.

2.4 Password managers

As passwords become more complex, and you need to look after more of them, it becomes increasingly necessary to use a password manager.

The Company provides access to the BitWarden password manager and will share passwords with you through this tool alone.

You still need to remember one password. This is the password that gets you into the manager application. Once you have access, the application works like a simple database, storing all the passwords associated with your various accounts and services.

Bitwarden also includes the following features:

- A Password generator.
- Storage of Time-based One-Time Passwords (TOTP) a common form of two-factor authentication (2FA).
- Storage of other secure information such as credit and debit card details, access keys and encryption keys
- Automatically fill in username and password fields for you when during login.
- Mobile, Desktop and Browser plugins

The BitWarden password manager database is stored in the cloud so that you can use it anywhere. The database is encrypted, so only you can open it. That's why your single password key is so important. Without it, you can never get access to the password database again.

Using a password manager for all your accounts and service details is recommended.

2.5 System administrators or developers

All engineers and systems employees are required to ensure that systems support the password requirements.

Systems **must be developed to support** the ability to issue, change, reset, and revoke passwords using well-defined and fully-described processes. The

2.6 Service Accounts

System and application authentication must always use service accounts.

Use certificates for service account authentication whenever possible. Follow guidelines for issuing and securing the certificates. If you can't use certificates, passwords are an acceptable alternative.

Service account passwords shall:

- Be system generated.
- Be at least 15 characters long but generally 36 character UUID
- Be no more than 128 characters long.
- Be complex, including upper-case and lower-case letters, digits, punctuation, and special characters except where a UUID is used
- Be kept secure, by using hashes or encryption.
- Not be stored in the clear in any systems or applications.
- Not be used by standard or administrative users for any purpose.

2.7 Default passwords

Change all default passwords when a new, modified, or replacement system arrives. Complete the changes before making the system available for any work.

When preparing devices or services for first use, system developers or system administrators must configure the default password on the device or service so that it can be used once only.

The "first use" of a password must force the user to change the password before the device or service can be used.

2.8 Multi-factor Authentication

Multi-factor Authentication (MFA) provides extra security for login and access controls. MFA is also referred to as Two-Factor Authentication or 2FA.

MFA shall be implemented and enabled on all systems where it is supported.

When performing a privileged action, such as installing or reconfiguring a system, or changing critical or sensitive details, it is important that the user is correctly and reliably authenticated. This is best done by using MFA. For example, before deleting a database configuration, MFA should have been completed successfully during the authentication process, to confirm that the user is indeed who they claim to be, and that they are indeed authorised to perform that privileged task.

Use a Time-based One-Time Password Algorithm (TOTP), or hardware and software tokens, as the preferred MFA mechanisms.

The company issues BitWarden cloud service should be used to store all TOTP codes and generate the MFA response.

If possible, avoid using SMS or email messages containing one-time login codes. If TOTP applications, or hardware- or software-based tokens, are not available to you, then SMS MFA or email MFA is still better than no MFA.

2.9 Password storage

Never store, display or print passwords in the clear. If you need to store them, do so by using the company issues BitWarden password manager.

2.10 Password access attempts

Typically, If a password is ever entered incorrectly, a count starts. After at most 10 (ten) consecutive failed attempts at using the correct password, access to the account or system is likely to be blocked.

A successful use of the password resets the count to zero again.

2.11 Password reset

If a password lock occurs, a reset is necessary. This requires action by the system administrator which can be requested via the support team.

The process should be like issuing the password for the first time. Other account details are not changed during the reset. This helps avoid losing any work.

2.12 Blocking bad passwords

You should not try and use obvious passwords. Attempts to do so will be blocked.

Developers and administrators should configure systems to check for and block obvious passwords embedded within a password. For example, `MySecretPassword` is not a good password!

2.13 Distributing passwords to users

There are times when a system needs to send a password to a user. An example is when granting access to a service for the first time. To send a password to a user, the mechanism used **must** be secure.

The most secure way to share a password with any user is via the Company issues BitWarden password manager which includes the ability to share a secret with anyone. There is no requirement that the recipient also have access to BitWarden. The process works by sending an email to the intended recipient with a link to recover the secret. This link will generally work only once..

Passwords created for a user and shared in this way should always be single-use.

> Sharing passwords over email is prohibited. Failing to adhere to this policy may result in disciplinary action.

2.14 Identity Providers and Single Sign-On

The Company generally seeks to secure access to all systems using our Enterprise Identity Provider (IDP) Microsoft Entrata.

The company also enables access to all of our Partner-facing systems using a variety of IDPs as may be appropriate to the requirements of the Partner.

Where this has been enabled you will be able to gain access to systems using the single email address and password that you use to access our Microsoft products such as Teams.

This helps reduce the need to design, create, deploy and manage yet another solution.

SSO integration in existing IdP solutions improves the user experience as you may only need to login to a single system to be magically granted access to all other systems supported by the same IDP.

2.15 Account management

This guidance on passwords is separate from the guidance on account management. You should still follow the rules and processes for managing accounts. In particular, while you don't need to change passwords after a period of time, you should still expire accounts promptly.

Examples would be when accounts are no longer required, or have fallen out of use.