

Password Manager Recovery Kit

Name:

Date verified:

***FILL BY HAND, NOT ON A COMPUTER**

Password manager details	
Name (e.g. Bitwarden)	URL (e.g. vault.bitwarden.com)
Email address	Username (only if separate from email)
Password*	
Secret Key (1Password only)*	

Password manager multifactor authentication	
Authenticator app (e.g. Ente Auth)	App details
	TOTP Secret Key*
Hardware key (e.g. YubiKey)	Device identifier (e.g. serial number)
Other (specify)	Notes
Backup/recovery codes*	

A copy of this sheet is stored with a trusted contact.

Name:

Phone number:

Password Manager Recovery Kit

INSTRUCTIONS

Purpose

This one-page Recovery Kit has everything you need to access your password manager. From there, you can access your online accounts and devices. It is the keys to your digital kingdom.

Use the Recovery Kit if you forget your password manager login details, or cannot use multifactor authentication methods. Give a paper copy to a trusted contact so they can access your accounts and devices in an emergency. They can also store these details in their own password manager.

The Recovery Kit contains highly sensitive information. For security, **FILL THE STARRED * FIELDS BY HAND, NOT ON A COMPUTER**. Store a paper copy with other vital documents (i.e. birth certificate, passport), ideally in a fireproof safe.

Line instructions

- Name: Full name
- Date updated: Verify details before entering into the Recovery Kit. Update if details change (e.g. new password)

Password manager details

- Name: password manager service (e.g. Bitwarden, 1Password, KeePassXC, Dashlane)
- URL: password manager web address. Takes you directly to your passwords. Note that URLs change frequently
- Password: **PRINT BY HAND**. Use a passphrase for easier entry and memorization
- Secret Key: **PRINT BY HAND**. Required for services like 1Password

Password manager multifactor authentication (MFA)

- Authenticator app: generates temporary one-time passwords (TOTP)
 - App details: e.g. Ente Auth, Aegis Authenticator
 - TOTP Secret Key: **PRINT BY HAND**. A string of letters and numbers that syncs the authenticator app with the online account. Use to set up authenticator app
- Hardware key: A physical device that authenticates your identity to an online account
 - Device identifier: name, serial number
- Other: Don't use one-time passwords sent by email or text. These are less secure than an app or hardware key
- Backup/recovery codes: **PRINT BY HAND**. Single-use codes generated by the password manager when you set up MFA. Use if you cannot access other methods