# VaultDrop

## User Guide

*Encrypt it. Decrypt it. Shred it.*

Korerium LLC

www.korerium.com

# Table of Contents

This guide covers everything VaultDrop does and how to get the most out of it. Use the sections below to find what you need.


| | |
|---|---|
| What is VaultDrop | 2 |
| How VaultDrop Works | 2 |
| System Requirements | 3 |
| Getting Started | 4 |
| The Encrypt Screen | 4 |
| The Decrypt Screen | 5 |
| The Shred Screen | 6 |
| Auto-Lock | 7 |
| Settings | 8 |
| License Activation | 9 |
| Understanding the .vdrop Format | 10 |
| Privacy Statement | 10 |

# What is VaultDrop

VaultDrop is a native macOS privacy tool that encrypts your files, securely decrypts them when needed, and permanently shreds files you no longer want to keep. Whether you are protecting sensitive documents before sending them, storing confidential files locally, or disposing of files you need gone for good, VaultDrop handles all three tasks in one focused application.

VaultDrop works entirely on your Mac. No account is required, no data is uploaded anywhere, and your files never leave your device. It is a one-time purchase with no subscription.

## Who is VaultDrop for?

- Individuals who need to send sensitive documents and want strong encryption before sharing.
- Professionals handling client files, contracts, or confidential records who need reliable at-rest protection.
- Anyone who wants to permanently delete files beyond recovery, not just move them to the Trash.
- Privacy-conscious users who want full control over their data without cloud dependency.

# How VaultDrop Works

VaultDrop uses three independent pipelines, each accessed from the sidebar: Encrypt, Decrypt, and Shred.

## Encryption Pipeline

VaultDrop encrypts files using AES-256-GCM, a symmetric authenticated encryption algorithm trusted by governments and security professionals worldwide. Each encryption operation derives a unique key using PBKDF2-SHA256 with 100,000 rounds and a randomly generated salt. This means the same passphrase produces a different key for every file you encrypt. The encrypted output is saved as a .vdrop container. The

original filename is encrypted inside the ciphertext so that the container file itself reveals nothing about what it holds.

### Decryption Pipeline

To decrypt a .vdrop file, drop it onto the Decrypt screen and enter the passphrase used to encrypt it. VaultDrop derives the same key, authenticates the ciphertext, and writes the decrypted file alongside the container. If the passphrase is incorrect or the file has been tampered with, decryption will fail and VaultDrop will tell you why.

### Shred Pipeline

VaultDrop shreds files using the DoD 5220.22-M standard: seven overwrite passes with alternating patterns before the file is deleted. This makes the original file content unrecoverable by standard forensic tools. Shredding is permanent and cannot be undone.

### Shred on Encrypt

When the Shred on Encrypt toggle is enabled in Settings, VaultDrop automatically shreds the original file after a successful encryption. This is the recommended workflow when your goal is to replace a plaintext file with its encrypted version and leave no recoverable copy behind.

## System Requirements

| Requirement | Minimum |
|---|---|
| macOS | macOS 26 or later |
| Architecture | Apple Silicon (M1 or later) |
| Storage | 15 MB for the application |
| Memory | 4 GB RAM recommended for large batches |
| Internet | Not required for use |

# Getting Started

On first launch VaultDrop presents a brief welcome screen that walks you through the three core functions: Encrypt, Decrypt, and Shred. After completing the welcome screen you will not see it again unless you reopen it from the Help menu.

## License Activation

VaultDrop includes a five-use trial so you can verify it works with your files before activating. A trial use counter appears at the top of the window while in trial mode. To activate, open Settings, scroll to the License card, enter your name, email address, and license key, then click Activate License.

## First Run Checklist

- Open VaultDrop from your Applications folder.
- Complete the welcome screen.
- Drag a file onto the drop zone or click to browse.
- Enter a strong passphrase and confirm it.
- Click Encrypt File.
- Use the folder icon to locate the .vdrop container.

# The Encrypt Screen

The Encrypt screen is where you protect files. It is divided into three zones: the sidebar on the left, the drop zone in the center, and the passphrase panel below it.

## Sidebar

The sidebar shows the app name, navigation links for Encrypt, Decrypt, and Shred, a session stats block showing files processed in the current session, and the version number in the footer.

## Drop Zone

The drop zone is the large target area at the top of the Encrypt screen. Drag any file onto it or click to browse. VaultDrop accepts any file type. You can drop one file at a time for encryption.

### Passphrase Panel

After dropping a file, the passphrase panel appears below the drop zone. Enter your passphrase in the first field and confirm it in the second. VaultDrop does not enforce a minimum passphrase length, but a strong passphrase is essential -- the security of the encrypted file depends entirely on it.

### Output Location

By default, the .vdrop container is saved in the same folder as the original file. You can change the output location in Settings.

### Shred on Encrypt

If Shred on Encrypt is enabled in Settings, VaultDrop will shred the original file immediately after a successful encryption. A confirmation sheet appears before shredding begins so you have a final opportunity to cancel. Once shredding starts it cannot be undone.

### Encrypt Button

Click Encrypt File to begin. VaultDrop derives the encryption key, encrypts the file, writes the .vdrop container, and shows a success state with the output path. A folder icon lets you open the container location in Finder.

## The Decrypt Screen

The Decrypt screen reverses the encryption process. Drop a .vdrop file onto the drop zone, enter the passphrase, and VaultDrop writes the decrypted file to disk.

### Sidebar

The sidebar shows the app name, navigation links for Encrypt, Decrypt, and Shred, a session stats block showing files processed in the current session, and the version number in the footer.

### Drop Zone

The Decrypt drop zone accepts .vdrop files only. If you drop a file with a different extension, VaultDrop will display an error. Drag your .vdrop container here or click to browse..

### Passphrase Entry

Enter the passphrase used to encrypt the file. VaultDrop uses the salt stored inside the .vdrop container to derive the decryption key. The passphrase is never stored anywhere.

### Output

The decrypted file is saved alongside the .vdrop container with the original filename restored. If a file with that name already exists at the destination, VaultDrop appends a number to avoid overwriting it.

### Retry on Failed Decrypt

If the passphrase is incorrect or the file fails authentication, VaultDrop displays an error with the reason. The passphrase field clears so you can try again without removing and re-dropping the file.

### Decrypt Button

Click Decrypt File to begin. VaultDrop derives the decryption key, authenticates the ciphertext, and writes the decrypted file to disk. A folder icon lets you open the output location in Finder.

## The Shred Screen

The Shred screen permanently destroys files. Once a file has been shredded it cannot be recovered, including with forensic tools. Use this when you need to be certain a file is gone.

### Drop Zone

Drag one or more files onto the Shred drop zone. VaultDrop shows each file as a card in the queue with its name and size.

### Confirmation

Before shredding begins, VaultDrop shows a confirmation sheet listing the files that will be destroyed. Review the list carefully. This is the last opportunity to remove a file before it is permanently gone. Click Shred to proceed or Cancel to return to the queue.

### Shred Progress

Each file passes through seven overwrite passes following the DoD 5220.22-M standard. Progress is shown per-file. VaultDrop processes shred operations sequentially to ensure each pass completes before moving to the next file.

### Shred Standards

| Standard | Description |
|---|---|
| DoD 5220.22-M | 7-pass overwrite with alternating bit patterns. Default for all shred operations. |
| Pass Count | Seven total passes per file before deletion. |
| Recovery | File content is unrecoverable by standard forensic tools after completion. |

# Auto-Lock

• Open Settings and find the Auto-Lock section. Choose from four timeout options:

• 1 minute

• 5 minutes

• 15 minutes

• 30 minutes

You can also disable Auto-Lock entirely if you prefer to manage locking manually. To lock VaultDrop immediately, use the lock icon in the sidebar footer or press the keyboard shortcut shown in the menu bar.

# Settings

Open Settings from the sidebar or by pressing Command-Comma. Settings are organized into four sections: Preferences, License, About, and Danger.

## Preferences

Preferences contains controls for output location, Shred on Encrypt, and Auto-Lock timeout.

- Output Location: Click to choose a custom folder for all encrypted containers. By default VaultDrop saves .vdrop files alongside the original. Click Reset to restore the default behavior.
- Shred on Encrypt: Toggle this on to automatically shred the original file after a successful encryption.
- Auto-Lock: Set the inactivity timeout or disable it.

## License

The License section shows your current activation status and lets you enter a license key for a new activation. It also shows the name associated with the current license and allows you to edit the display name.

## About

The About section shows the current VaultDrop version, build number, and links to korerium.com and support.

## Danger

The Danger section contains irreversible actions. Currently this includes Reset All Settings, which clears your preferences and license activation. Use with caution.

# License Activation

VaultDrop includes a five-use trial. After five uses you will need to activate a license to continue encrypting, decrypting, and shredding files.

## How to Activate

• Open Settings from the sidebar.

• Scroll to the License section.

• Enter your first and last name.

• Enter the email address you used to purchase VaultDrop.

• Enter your license key exactly as it was delivered, including the dashes.

• Click Activate License.

Activation is verified entirely offline using a cryptographic key derived from your email address. No internet connection is required.

## License Key Format

License keys are 35 characters in the format:

XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX

## Support

If you have trouble activating, contact support@korerium.com with your order confirmation and the email address used to purchase.

# Understanding the .vdrop Format

Every file encrypted by VaultDrop is saved as a .vdrop container. The format is designed to be self-contained, tamper-evident, and opaque.

| Component | Description |
|---|---|
| Magic Bytes | VDRP -- four-byte identifier at the start of every .vdrop file. |
| Version | Format version number for forward compatibility |
| Salt | Unique random salt used for key derivation. Stored in plaintext inside the container. |
| Ciphertext | AES-256-GCM encrypted payload including the original filename and file contents |
| Auth Tag | GCM authentication tag. Decryption fails if the file has been modified. |

## What the Container Reveals

The .vdrop container reveals nothing about the file inside. The original filename is encrypted within the ciphertext. An observer seeing only the container file knows it is a VaultDrop file by the VDRP magic bytes, but cannot determine the original filename, file type, or contents without the correct passphrase.

# Privacy Statement

VaultDrop is a local-first application. It does not collect, transmit, or store any data about you, your files, or your usage.

## What VaultDrop Does Not Do

- Does not connect to the internet for processing or license validation.
- Does not send usage analytics or telemetry.
- Does not upload your files, passphrases, or metadata to any server.
- Does not require an account, email address, or login for normal use.
- Does not store your passphrase at any point during or after encryption.

• Does not retain any information about which files you have processed.

## What VaultDrop Stores Locally

VaultDrop stores your preferences, including output folder, Shred on Encrypt toggle, and Auto-Lock timeout, in your Mac's standard preferences system (NSUserDefaults). This data never leaves your Mac. You can reset it at any time in Settings > Danger > Reset All Settings, or by running the following command in Terminal:

```
defaults delete com.korerium.VaultDrop
```

## License Verification

License key validation is performed entirely offline using HMAC-SHA256 cryptography. Your email address and license key are never transmitted to Korerium or any third party. Validation happens on your Mac using a locally computed cryptographic signature.

## Contact

Questions about VaultDrop's privacy practices can be directed to support@korerium.com