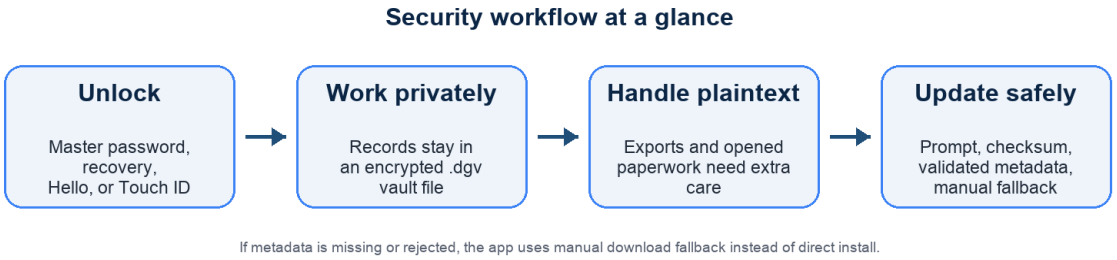
Security Workflow

Plain-English guide for users and testers



User-facing security path: vault unlock, private work, export caution, and guarded updates.

This guide explains the security workflow in plain language. It is written for owners and testers who need to understand what the app protects, what the app asks the user to confirm, and what happens during app updates.

The Short Version

Digital Gun Vault protects inventory data by keeping records inside an encrypted `.dgv` vault file. The app is local-first: the website and update system do not receive firearm records, serial numbers, images, paperwork, passwords, recovery passwords, or vault contents.

The app has four security checkpoints that matter most to users:

1. Unlock the vault with the master password, recovery password, Windows Hello, or Touch ID.
2. Work with inventory records while remembering that anything visible on the screen can be seen by someone with access to the device.
3. Treat exports and opened paperwork copies as sensitive plaintext.
4. Accept app updates only through the in-app update prompt or an official release/download page.

What Stays Encrypted

The `.dgv` vault stores firearms, accessories, locations, images, notes, and paperwork in an encrypted container. A wrong password or tampered vault should fail closed, meaning the app should not parse or show partial inventory data.

Digital Gun Vault does not intentionally log:

- Master passwords.
- Recovery passwords.
- Vault keys.
- Decrypted vault JSON.
- Plaintext inventory records.

Passwords, Recovery, And Convenience Unlock

The master password is the normal way to open a vault. The recovery password is the portable backup method. Store the recovery password offline and separate from the vault file.

Windows Hello and Touch ID are convenience unlocks. They help reopen a vault on the same trusted device after the vault was already opened with the master password or recovery password. They are not a replacement for the master password or recovery password.

If the vault file changes outside the app, convenience unlock material is invalidated and the app asks for the password again.

Attachments And Paperwork

Attachments are stored inside the encrypted vault after they are added. Before a file enters the vault, the app restricts attachments to supported file types and size limits.

Allowed examples:

- Firearm images: common image formats such as JPG, PNG, HEIC, BMP, and GIF.
- NFA paperwork: PDF plus approved image formats.

Rejected examples:

- Executables.
- Scripts.
- Links and shortcuts.
- Archives.
- Macro-capable document formats.
- Files whose content does not match their extension.
- Oversized files.

When the user clicks Open on attached paperwork, the app writes a randomly named temporary local copy so the operating system can open it in the normal viewer. The app tracks those copies and attempts to delete them when the app closes, locks, switches vaults, or performs periodic cleanup. External PDF/image viewers may keep their own recent-file lists or caches, so the local device profile should still be treated as sensitive.

Exports

Excel and PDF exports are plaintext. They are not encrypted by Digital Gun Vault after export. The app requires recent password confirmation before plaintext export after the reauthentication window has elapsed.

Recommended user workflow:

1. Export only when needed.
2. Save exports to an encrypted or otherwise trusted location.
3. Delete exports when they are no longer needed.
4. Do not keep plaintext exports beside the vault file unless that location is protected.

App Updates

The installed app checks the public Digital Gun Vault website for update metadata. The website worker overlays platform-specific update fragments from the Azure update host when those fragments are available.

The app can offer an automatic update only when the manifest includes a direct installable package for the current platform and a SHA-256 checksum. If direct update metadata is missing or rejected, the app falls back to a manual download or release page.

Current update protections:

- The public manifest endpoint is served with no-store caching.
- The website worker validates Azure update fragments before overlaying them.
- Wrong-platform, malformed, non-HTTPS, outside-host, or incomplete direct

artifact entries are ignored.

- The desktop app verifies the downloaded package checksum before replacement.
- Release-channel publishing is routed through a protected GitHub environment.
- Azure update storage uses blob versioning, at least 30-day soft delete, and a

documented delete-protection lock path.

> Important current limitation: release hardening is still in progress for signed update metadata and platform package signing. Until that work is complete, checksum verification helps catch download corruption or mismatch, but signed metadata and signed/notarized packages remain the production release blocker.

Build Channels

Digital Gun Vault uses three user-facing release lanes:

Channel	Who should use it	Purpose
Nightly	Owner/internal validation	Fast checks for the newest changes.
Beta	Limited testers	Candidate builds after nightly checks pass.
Release	Public users	Stable builds after validation and approval.

Promotion follows this path:

```
main -> nightly -> beta -> release
```

The app should not jump directly from untested code to public release. Each lane gives the project a chance to test, verify, and stop a bad update before it reaches a wider audience.

If Something Looks Wrong

Stop and report it if:

- The app update prompt shows an unexpected channel.
- The version or build number does not match the expected test build.
- The app falls back to a browser download when an automatic update was

expected.

- A downloaded app fails checksum verification.
- A vault asks for a password after convenience unlock was expected.
- Attachments or exports appear in an unexpected location.

For sensitive issues, do not attach a real vault file, screenshots with serial numbers, recovery passwords, or paperwork. Use the synthetic sample vault for repro steps whenever possible.

What Users Control

Users remain responsible for:

- Choosing a strong master password.
- Storing the recovery password safely.
- Locking the vault before stepping away.
- Securing the device account.
- Treating exports and opened paperwork as sensitive plaintext.
- Keeping backups of the encrypted vault and recovery material separately.

Digital Gun Vault provides encryption, guarded update checks, attachment limits, and workflow prompts. It cannot protect data that is copied out of the vault into plaintext files or viewed on a compromised device.