3-Minute File Defense Plan

This guide gives you fast, actionable steps to lock down any file in under 3 minutes. Use it for sensitive drafts, project files, personal records, anything you don't want scanned, copied, or leaked.

STEP 1: Encrypt the File (with Picocrypt)

1. Download Picocrypt from https://github.com/Picocrypt/Picocrypt
2. Open it, drag your file into the window.
3. Click "Create" and then "Generate" a password, then click Encrypt. **(SAVE THE PASSWORD!!!)**
4. Save the encrypted `.pcv` file somewhere safe.

Your file is now encrypted. No install required. Fully local.

STEP 2: Make a Local Backup (Air-Gapped)

1. Plug in a clean USB drive.
2. Copy the encrypted `.pcv` file to this USB.
3. Store it somewhere safe (drawer, safe, keychain, etc).

This step protects against device failure, ransomware, or theft.

STEP 3: Verify File Integrity (Optional but Strong)

1. On Linux/macOS: run `shasum -a 256 yourfile.pcv`
   On Windows: use PowerShell -> `Get-FileHash yourfile.pcv -Algorithm SHA256`
2. Save the resulting hash to a `.txt` file or print it out.

Use this hash to confirm your file hasn't been tampered with.

Done. Your file is now private, backed up, and integrity checked.

Not perfect. Just yours.
-GHOST