

FLUX WIKI

STARTER KIT — SECURITY & SANITIZATION

WHAT NEVER SHIPS — SECRETS, PERSONAL PATHS, REAL CATALOG DATA, AWS KEYS — AND HOW THE KIT IS SANITIZED.

flux.dantesisofo.com/wiki/starter-kit-security/

FLUX_WIKI_v2.0

JUNE 2026

FLUX DOCUMENTATION SYSTEM Layer 11 – STARTER KIT | starter-kit-security
flux.dantesisofo.com/wiki/starter-kit-security/

STARTER KIT – SECURITY & SANITIZATION

The packaging rule is simple: **the kit ships the *machinery*, never the *identity*, *secrets*, or *data***. This page is the checklist that gates any release.

1. NEVER SHIP (SECRETS)

- `.env` – portal password, SMTP credentials, AI API key. Ships only as `.env.example` with empty/placeholder values.
- `~/.aws/credentials` **and** `config` – cloud access keys. These live outside the project folder; they must never be copied into the repo or a zip.
- Any pasted access key, secret, session token, or API key in code, notebooks, or commit history.

Because a starter kit is built as a **fresh repo / clean folder** (not a copy of the working tree), there is no git history to leak old secrets from. Start clean.

2. NEVER SHIP (PERSONAL IDENTITY / INFRA)

Replace these with config variables (`.env`) or generic placeholders:

Real value (do not embed)	Ships as
your S3 bucket name	FLUX_BUCKET (placeholder)
your CloudFront distribution ID	FLUX_CF_DIST (placeholder)
your public domain	FLUX_BASE_URL (placeholder)
your AWS region	FLUX_REGION
your author/photographer name	FLUX_AUTHOR = Your Name
your IAM user name	n/a (student uses their own)
absolute home paths (<code>/Users/<you>/...</code>)	relative paths / <code>\$HOME</code>

These identifiers are sprinkled across the working code; sanitization means **externalizing all of them into one config** so the student sets their own.

3. NEVER SHIP (PERSONAL DATA)

- Your real photographic archive (original JPEGs, derivatives, exports).
- The real **catalog JSON** (your walks, GPS tracks, addresses, drafts).
- Local working folders: drafts, pending runs, repair/reset backups.
- Deployed personal site content (your published pages, hub, dispatches, wiki).

Ship instead a tiny **sample walk** (CC0 / public-domain geotagged photos, or a generator that stamps sample EXIF+GPS) and an **empty catalog seed**. See **TEMPLATE KIT PLAN**.

4. PRIVACY OF GEOTAGS

Geotagged photos contain precise locations. Two things to teach students:

- **Derivatives strip EXIF** – the published web images do not carry GPS; only the route polyline (which the author chose to publish) is exposed.
 - The author controls what's published. Encourage care with home/private locations; the system makes route publication an explicit step, not automatic.
-

5. SANITIZATION CHECKLIST (RELEASE GATE)

Before any kit leaves your machine:

- [] No `.env`, no `~/.aws/*`, no keys/tokens anywhere in the tree.
 - [] grep the kit for your bucket, distribution ID, domain, name, and home path → **zero hits** outside `.env.example` placeholders.
 - [] Catalog is the empty seed; no real drafts/pending-runs/backups.
 - [] Only sample media present (and it's licensed for redistribution).
 - [] `.gitignore` blocks `.env`, drafts, pending runs, data JSON (except the seed), media, caches.
 - [] Fresh repo/zip – no history from the working tree.
 - [] A second person can run it with only their own credentials and the docs.
-

Next: **TEMPLATE KIT PLAN** for exactly what code is included vs excluded.

FLUX_WIKI_v2.0 – flux.dantesisofo.com/wiki/starter-kit-security/