

A PRE-FLIGHT LIST FOR SOFTWARE DELIVERY INTO DISCONNECTED ENVIRONMENTS — FREE TO USE WITH ATTRIBUTION

# Deliver like the network is never coming back.

The generic, unclassified pre-flight we run before any disconnected delivery. Engineering practice only — site-specific procedures always belong to the site, and nothing here overrides a customer's own security process.

## §1 • BUILD — DETERMINISTIC OR IT DIDN'T HAPPEN

- ☐ Build is reproducible: same inputs produce byte-identical artifacts on a second, independent machine.
- ☐ Every dependency is pinned by version *and* content hash — no floating tags, no "latest."
- ☐ A software inventory (SBOM) is generated at build time and shipped with the bundle.
- ☐ Artifacts are signed at build; the verification key travels separately from the bundle.
- ☐ The build machine's toolchain versions are recorded in the manifest.

## §3 • TRANSFER EVIDENCE — BOTH SIDES CAN PROVE IT

- ☐ A manifest lists every file with its size and content hash; the manifest itself is signed.
- ☐ Hashes are verified on the receiving side before anything is installed, and the verification result is recorded.
- ☐ The transfer follows the customer's approved process — the checklist defers to it, never replaces it.
- ☐ Chain of custody is written down: who prepared, who carried, who received, when.
- ☐ A copy of the manifest stays on the originating side for later audit comparison.

## THE ONE-QUESTION AUDIT

**Pick any installed file and ask: which bundle did this come from, and what hash did it arrive with?** If the answer takes more than a minute, the process needs work. Same discipline as our published Evidence Ledger ([federal.ai/evidence-ledger](https://federal.ai/evidence-ledger)) and the Cleared FDE Standard §2.1 ([federal.ai/standard](https://federal.ai/standard)).

## §2 • PACKAGE — ASSUME NOTHING ON THE FAR SIDE

- ☐ The bundle carries everything: dependencies, container images, model weights, license files, documentation.
- ☐ Zero install-time network calls — verified by installing on a machine with networking disabled.
- ☐ Installer is idempotent: running it twice is safe, and a failed run can be re-run cleanly.
- ☐ Configuration is externalized and documented; site-specific values have clearly marked placeholders.
- ☐ Bundle size, media format, and file-count limits are confirmed against the receiving process beforehand.

## §4 • INSTALL & ACCEPT — LEAVE IT OPERABLE, NOT JUST INSTALLED

- ☐ A smoke test proves core function with no external dependencies, and its expected output is documented in advance.
- ☐ Evaluation cases run on-site against the installed system — measured, not demonstrated.
- ☐ Rollback is rehearsed: the previous state can be restored from on-site materials alone.
- ☐ Operators run the acceptance test themselves; delivery is done when they say it is, in writing.
- ☐ Update path is documented for the *next* bundle — including how the system behaves between updates.