



FedShredder

Data Handling Summary

FedShredder

Pack version: 1.0.0 · Generated: 2026-05-29

Executive summary

FedShredder delivers a **verified, source-linked requirements baseline** used by capture teams before drafting begins.

This document describes the **Pilot Sprint** handling model for solicitation materials and the constraints that keep the workflow reviewable and auditable.

Data flow (Pilot Sprint)

```

flowchart LR
    subgraph Customer
        U[Capture manager]
    end
    subgraph Intake
        I[Secure intake email / agreed channel]
    end
    subgraph Processing
        B[FastAPI backend]
        G[Gemini API]
    end
    subgraph Deliverables
        M[Compliance matrix .xlsx]
        V[Volume outline]
    end
    U --> I
    I --> B
    B --> G
    G --> M
    G --> V
    M --> U
    V --> U
  
```

1. Customer executes **Mutual NDA** and **Pilot Data Addendum**.
2. Solicitation PDFs transmitted via agreed secure channel (not the public marketing site).
3. Operator ingests files; text extracted locally (`IngestionProcessor`).
4. Structured extraction via **Gemini API** (multi-pass compliance pipeline).
5. Deliverables returned to Customer; retention clock starts for 30-day purge window.

Scope constraints (Pilot Sprint)

- Train foundation models on Customer Pilot Data
- Publish Customer solicitations or matrices on fedshredder.com without consent
- Accept classified materials on the standard Pilot path
- Process CUI-marked or export-controlled material unless explicitly agreed in writing under a separate handling plan
- Replace customer proposal review, color-team process, or final submission authority

Review checkpoints and auditability

FedShredder is designed to produce a baseline your team can defend during internal reviews.

Each matrix row is treated as an auditable unit with a verifiable coordinate:

- Source document
- Source section / reference (when present)
- Source page
- Source excerpt
- Review status (Auto-confirmed, Formatting review, or Human review)

Rows that cannot be reconciled programmatically are **not hidden**. They are explicitly flagged for operator QA and customer review.

Verification

Download [security-pack-manifest.json](https://fedshredder.com/security/security-pack-manifest.json) and run checksum verification (see `manifest verifyCommand`). Cross-reference `security-pack-verification-report.json` in `/security/developer/` for claim-to-code mapping.

Enterprise intake: `/contact?intent=enterprise`

Human QA required on all final deliverables. FedShredder establishes a verified, source-linked requirements baseline before drafting begins.