**PRD-35 — Media Governance and Malware Hygiene for Product Docs**

**Intent**

Protect your catalog from risky files: enforce allowed types, deep malware scans, forbidden content patterns, and retention/lifecycle on product-scoped media.

**Preconditions**

• Scanner (AV + sandbox), MIME/type detector, content rules engine, retention matrix.

**Steps**

• Allowlist & Sniff: only permitted MIME types; sniff header to prevent spoofing.

• Deep Scan: run sandbox for risky types (Office/PDF/archives); store scan report hash.

• Forbidden Patterns: detect disallowed content (secrets, PII) with rule engine; quarantine on hit; open exception.

• Retention & TTL: apply retention by doc type (e.g., MSDS 10y, marketing 3y); schedule purge with signed Purge Receipt.

• Lineage: link media to product version/PCV/lot; show hash and origin in Proof Bundles.

• User UX: preview safely (image/PDF viewer); download banners show hash + scan date.

**Edge cases**

• Password-protected archives → require supplier to re-submit or capture password with policy gate.

• Very large files → chunked upload + background scan; block use until cleared.

**Done when**

• 100% product media complies with allowlist, scans clean, and is governed by retention with notarized purges.