

COMPLIANCE WORKING RECORD

Backup integrity validator

Fictional sample. Requires tailoring and responsible review.

Document control

Field	Value
Document type	Backup integrity validator
Document reference	FICTIONAL-REVIEW-1
Jurisdiction	United States
Version	fictional-v1
Status	Mechanical review prepared
Prepared by	Fictional records owner
Prepared on	October 8, 2026
Rule pack	2026-10-08.evidence-control.1
Generated	October 9, 2026

Purpose and boundary

Validate actual local evidence-workspace backup structure, exact source hashes and supported recovery completeness before restoring it.

Inspect supported evidence-control backup ZIPs without restoring them. Bound compressed and expanded bytes, require exact declared entries, validate tool/version/input/history structure and rehash every original file. Unsupported backups remain unsupported, never reported recoverable.

Customer facts, source bytes, file metadata, approvals and declared dates stay in this browser. Mechanical findings do not authenticate provenance, approval authority, source correctness, legal applicability, redaction completeness or unrecorded events. No remote source is fetched, file is deleted or external provider is called.

Declared review scope

Fictional evidence population. Replace every fact before use.

Review findings

2 source-linked findings. Indexed 1, Recoverable structure 1.

Formal report findings display at most 100 rows and 1000 characters per field. Complete accepted inputs and findings remain in Excel and JSON.

Kind	ID	Result	Finding
Exact local file	f1	Indexed	Exact original bytes retained. Provenance remains customer-declared.
Backup recovery	f1	Recoverable structure	Supported 40-evidence-manifest-builder. 2 exact source files and 1 retained events verified. Restore was not performed.

Selected exact attachments

ID	Filename	Bytes	SHA-256
f1	fictional-evidence-backup.zip	1050	589dee3bbe40cbeedf313842ef303d4b9d8bdb3589a5636c1ec52c7a780371d4

Unresolved items and limits

- Customer statements, authority and source correctness remain unverified.

Limitations

- Customer facts, source bytes, file metadata, approvals and declared dates stay in this browser. Mechanical findings do not authenticate provenance, approval authority, source correctness, legal applicability, redaction completeness or unrecorded events. No remote source is fetched, file is deleted or external provider is called.

Official sources

Source	Provision	Date	Link
National Institute of Standards and Technology: Secure Hash Standard	SHA-256 file and event digests detect changes relative to retained digests. They do not authenticate source facts, approval authority, event timing, a rewritten log or legal requirements.	October 8, 2026	https://csrc.nist.gov/pubs/fips/180-4/upd1/final