AETERNA – INTEGRITY AUDIT REPORT

Cryptographic Integrity & Audit Assurance Report

Executive Summary

This report documents the deterministic integrity verification performed by **Aeterna** on **2026-02-02T03:24:42.112841Z**.

Aeterna evaluated the complete sequence of recorded operational events using cryptographically chained audit records.

VERDICT: PASS

No evidence of post-ingest modification, record tampering, record deletion, or chain discontinuity was detected within the evaluated scope at the time of verification.

System Identification

Instance ID	6f15bfea-2e24-4ecc-99bc-a6d5bbd17091
Customer	Client
License Type	Standard
Declared Scope	final

Verification Details

A total of **1** sequentially chained audit records were verified, forming a continuous integrity chain from session initiation through session closure.

The verification process is deterministic: any alteration, removal, or insertion of records after ingestion would irreversibly break the chain and be immediately detectable.

Scope Monitoring and Control

During operation, Aeterna continuously monitored execution activity against the declared operational scope.

No scope violations, unauthorized execution paths, or integrity anomalies were detected during the monitored period.

Technical Assurance

Aeterna implements cryptographically chained audit records using **SHA3-512 hashing**, combined with **HMAC-based digital signature generation at ingestion time**.

Each record's integrity depends on the immutability of all preceding records. Any post-ingest modification invalidates all subsequent records and compromises the audit chain in a deterministic and non-repudiable manner.

This report attests exclusively to **data integrity over time**. It does not assert the correctness, legality, or semantic validity of the underlying data itself.

Deliverable Evidence Record

Deliverable Hash	6721441d721e423fcff4c923cd01cf486aa9e23a188e1245b80f77a2bc189c9cb8a787bfc15fdebf68f67233be1be0c8f542e49c2ccb7d5f43f5c77c6651b6ce
Hash Algorithm	SHA3-512
Declared By	Client
Purpose	final

Evidence Integrity Statement

This document constitutes a **deterministic integrity artifact** derived exclusively from cryptographically verifiable audit records.

Any modification to the underlying records after the reported verification timestamp is cryptographically detectable and invalidates both the audit chain and this report.

Instance Binding

This report is cryptographically bound to a specific Aeterna execution instance. The following fingerprint uniquely identifies the audited system instance at the time of verification:

Instance Fingerprint	002cf8fb-461d-4301-86e1-4903e5b80025

Sealed Deliverable

Deliverable Hash (SHA3-512)	6721441d721e423fcff4c923cd01cf486aa9e23a188e1245b80f77a2bc189c9cb8a787bfc15fdebf68f67233be1be0c8f542e49c2ccb7d5f43f5c77c6651b6ce
Declared By	Client
Purpose	final

Cryptographic Attestation & Non-Repudiation

Report Hash (SHA3-512)
3bb439cc15d39485509e31af7eafea320270787300592059ec964aaef94643765d38c8adcbcc02d8ce8f03c2ca9787abb5e8f84db609a12339d3fb0de7fd27f8

Digital Signature (HMAC – Aeterna)
6c45e69723cc9de466b88fd0e1fb6650d19fb6de0b2143dd3069fa1b8a4794697b36efba13e7bcc5b3dccba8e655ca2eccbde6805b02d6c2283959e1645aa052

*Report generated by **Aeterna***
2026-02-02T03:24:57.287534 UTC

Confidential – Generated for internal audit, compliance, and executive review