

AETERNA – INTEGRITY AUDIT REPORT

Cryptographic Integrity & Audit Assurance Report

Executive Summary

This report documents the deterministic integrity verification performed by **Aeterna** on **2026-01-29T03:59:38.638191Z**.

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	6723f45b-b28d-41cb-95b5-03c5fde13e88
Customer	Client
License Type	Standard
Declared Scope	glso342

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	3ef731cc3e7dea741d05fc88001a83de4744863d6e7e08e74848598661d8d3
Hash Algorithm	SHA3-512
Declared By	
Purpose	glso342

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	56a9f35d-0fb6-4729-aa93-341f7c324e7e
----------------------	--------------------------------------

Sealed Deliverable

Deliverable Hash (SHA3-512)	3ef731cc3e7dea741d05fc88001a83de4744863d6e7e08e74848598
Declared By	Client
Purpose	glso342

Cryptographic Attestation & Non-Repudiation

Report Hash (SHA3-512)

f8db6411208cd8a7eb9f7e78419379aea504115663bd3905e3850b5541f3f95e6d73127efca262aa3069a847d67de0e65d2031967ed64715245e4241800cdff9

Digital Signature (HMAC - Aeterna)

5d6377a4283a714ceb8eaf78db419ecf5128c942098fcf3d9f00a1e94f94cd8b94bb02c105877e0ffee5d03cec2d457628e3879a00b22e65a2cafac7b4f43073

*Report generated by Aeterna
2026-01-29T04:00:02.269967 UTC*

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