

Evidence Readiness Pack

Executive & Operational Specification

Purpose

The Evidence Readiness Pack defines the enterprise's ability to produce complete, reliable, and defensible evidence within 24 hours of a material security incident, regulatory inquiry, or legal hold. It converts logging, monitoring, and investigation capability into an executive-governed control.

Board-Level Assertion

The organization asserts that for Tier-1 incidents it can identify what occurred, when it occurred, who was affected, and what decisions were taken, supported by preserved, time-synchronized, and chain-of-custody protected evidence.

Evidence Readiness Objectives

- Produce Tier-1 incident evidence within 24 hours
- Maintain ≥ 180 -day retention for Tier-1 sources
- Preserve integrity and chain-of-custody
- Correlate cyber and physical evidence
- Support regulator, law enforcement, and litigation needs

Operational Evidence Requirements

Tier-1 Evidence Sources (Mandatory)

• Identity logs (authentication, MFA, token issuance) • Endpoint and server logs • Network flow and firewall logs • Cloud control plane logs • Application and API logs • Email and messaging security logs • Physical access logs (badge, CCTV indices)

Logging Standards

All Tier-1 logs must be time-synchronized, tamper-evident, centrally searchable, and retained for the approved duration. Log formats must include actor, action, target, outcome, and timestamp.

Chain-of-Custody Requirements

Evidence must be collected, transferred, and stored in a manner that preserves integrity and provenance. Access must be restricted and logged. Hashing or immutability controls are required for Tier-1 artifacts.

Legal Hold & Preservation

Legal hold triggers must be predefined. Upon trigger, evidence retention is frozen, deletion is suspended, and custodians are notified. Counsel approval is required for release or destruction.

24-Hour Evidence Readiness Checklist

Capability	Requirement
Log Availability	Queryable within 24 hours
Time Synchronization	Verified across systems
Retention	≥180 days for Tier-1
Integrity Protection	Hashing / immutability enabled
Chain-of-Custody	Documented and enforced
Physical Correlation	Badge/CCTV linkage
Export Capability	Forensic-grade output

Failure to meet any checklist item constitutes an evidence readiness gap requiring executive visibility and remediation tracking.

Acknowledgement and Attestation

By signing below, the undersigned acknowledge review of this Evidence Readiness Pack and attest that the controls, processes, and obligations described herein are implemented and maintained. Signatures attest to accountability and oversight, not delegation.

Role	Name	Signature	Date
Board Chair			
Audit / Risk Committee Chair			
Chief Information Security Officer (CISO)			
Chief Information Officer (CIO)			
General Counsel			