# DigiEmu Core Security Model v1.0

Status: Normative Supporting Framework – Enterprise Edition
Scope: Security Controls & Integrity Protection
Date: 2026-02-17

## 1. Purpose

This document defines the security model governing DigiEmu Core implementations. It establishes mandatory controls protecting snapshot integrity, immutability enforcement, and tenant isolation.

## 2. Security Objectives

Implementations MUST ensure:
• Snapshot integrity protection
• Hash integrity validation
• Immutable entity enforcement
• Tenant boundary isolation
• Controlled access to core services.

## 3. Threat Surface Overview

Primary threat vectors include:
• Unauthorized data mutation
• Snapshot tampering
• Cross-tenant data leakage
• Hash manipulation
• Infrastructure compromise.

## 4. Immutability Enforcement Controls

Committed ContentVersion and Snapshot entities MUST be protected by database-level constraints or equivalent mechanisms preventing retroactive modification.

## 5. Hash Integrity Protection

Snapshot hashes MUST be generated via SHA-256 over canonical payloads. Any recomputation mismatch SHALL be treated as integrity violation.

## 6. Access Control Requirements

Access to core APIs MUST be authenticated and authorized. Administrative privileges MUST be restricted and auditable.

## 7. Environment Isolation

Production, staging, and development environments SHALL be separated. Sensitive snapshot data MUST NOT be exposed outside controlled zones.

## 8. Operational Monitoring

Systems SHOULD implement continuous integrity monitoring, including periodic snapshot verification and anomaly detection.

## 9. Incident Response Alignment

Security incidents affecting snapshot integrity MUST trigger formal incident response procedures aligned with enterprise standards.

## 10. Governance & Version Alignment

Security controls SHALL remain aligned with the DigiEmu Versioning & Stability Policy. Breaking security model changes require formal review and version increment.