Data-at-Rest and Data-in-Transit Encryption Standard

Document ID: IE-DES-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: IT & Engineering - Security

1. Goal

To protect all NexaCore and client data from unauthorized access through the mandatory application of cryptographic controls.

2. Data-in-Transit (DIT)

- **Mandatory Protocol:** All communication entering or leaving NexaCore's perimeter, and all internal service-to-service communication, must be encrypted using **TLS 1.2 or higher**.
- **Cipher Suites:** Only strong cipher suites (e.g., AES-256 with GCM) are permitted. Weak ciphers (e.g., RC4, 3DES) are strictly prohibited.
- **Client Connections:** The SaaS platform API gateway must enforce HTTPS for all client connections.

3. Data-at-Rest (DAR)

- **Storage Requirement:** All data stored in persistence layers (databases, object storage, block storage, and backups) must be encrypted at rest.
- **Managed Keys:** Encryption keys must be managed by the Cloud Provider's Key Management Service (KMS) or a NexaCore-controlled Hardware Security Module (HSM). Direct, unencrypted storage of cryptographic keys is prohibited.
- **Specific Data:** Highly sensitive data (e.g., client authentication secrets, specific P-2 data) must utilize **application-level encryption**, adding a layer of protection beyond standard disk encryption.

4. Key Management

- **Rotation:** Cryptographic keys used for production services must be automatically rotated on a schedule no longer than **90 days**.
- **Access Control:** Access to KMS/HSM is restricted via IAM and JIT principles, limited only to authorized engineers for deployment purposes.