Encryption and Key Management Policy

Version: 1.0
Last Updated: October 2025
Approved By: Chief Technology Officer (CTO)

1. Purpose

This policy establishes Orbitel.ai's framework for using encryption to protect sensitive data and for securely managing cryptographic keys throughout their lifecycle.
It supports compliance with ISO 27001 A.10, GDPR Article 32, and the DPDP Act 2023.

2. Scope

Covers all forms of data handled by Orbitel.ai:

- Data at rest in databases, object storage, backups, and logs.
- Data in transit between users, services, and systems.
- Encryption keys used for applications, APIs, and infrastructure services.

3. Governance and Responsibilities

- **CTO:** Approves encryption standards and key management systems.
- **Security Team:** Implements and monitors cryptographic controls.
- **Engineering Teams:** Ensure proper encryption integration in applications.

4. Policy Statements and Controls

a. Encryption Standards

- All sensitive data at rest is encrypted using AES-256 or stronger.

- Data in transit is protected using TLS 1.2 or higher.
- Asymmetric encryption uses RSA 2048 bits or Elliptic Curve Cryptography (ECC P-256 or better).

b. Key Management

- Keys are generated, stored, and rotated using cloud-native Key Management Systems (KMS) with hardware security modules (HSMs).
- Access to keys is restricted to authorized personnel via RBAC and MFA.
- Keys are rotated automatically every 12 months or immediately after compromise suspicion.
- Encryption keys are never stored in application code or repositories.

c. Data Handling

- Temporary files and cache data are encrypted and deleted on session termination.
- Encryption is validated during code review and security testing.

d. Key Recovery and Backup

- Key backup copies are encrypted and stored separately from production keys.
- Key recovery procedures are documented and tested annually.

e. Cryptographic Agility
Orbitel regularly reviews cryptographic standards to phase out deprecated algorithms and implement quantum-resilient approaches when available.

5. Compliance and Continuous Improvement

Orbitel's encryption controls are audited annually as part of ISO 27001 certification and SOC 2 assessments.
Findings from audits and incident reviews inform ongoing improvements to key management practices.