Information Security Policy

Version: 1.0
Last Updated: October 2025
Approved By: Chief Information Security Officer (CISO)
Next Review Date: October 2026

1. Purpose

Orbitel.ai is committed to ensuring the confidentiality, integrity, and availability of all information assets under its management. The purpose of this Information Security Policy is to define the high-level framework, principles, and governance mechanisms that protect Orbitel's digital ecosystem and customer trust.

This policy establishes Orbitel's approach to information security based on internationally recognized standards, including **ISO/IEC 27001:2022**, **NIST Cybersecurity Framework (CSF)**, **GDPR**, and the **Digital Personal Data Protection Act (DPDP), India 2023**.

2. Scope

This policy applies to:

- All **Orbitel Labs Pvt. Ltd.** employees, contractors, and third-party vendors with access to company information systems.
- All **information assets**, whether physical or digital, including AI training data, SaaS platforms, source code, and documentation.
- All systems owned, leased, or operated by Orbitel, including **cloud infrastructure, end-user devices, and hosted environments**.

It also extends to **Orbitel's customers' data** processed through its AI and voice-based products and services.

3. Governance and Accountability

Orbitel's Information Security Management System (ISMS) is centrally governed by the **Chief Information Security Officer (CISO)** and monitored through the **Information**

Security Committee, which includes representatives from Engineering, Legal, Compliance, and Operations.

Roles and responsibilities include:

- **CISO:** Defines, implements, and maintains the ISMS and approves all major policy changes.
- **Department Heads:** Ensure team-level compliance and risk management.
- **Security Team:** Conducts threat analysis, monitoring, and incident response.
- **Employees and Contractors:** Must comply with all security controls, complete annual training, and promptly report security events.

4. Core Security Principles

Orbitel's ISMS is founded on the **CIA Triad**:

- **Confidentiality:** Information is accessible only to authorized individuals.
- **Integrity:** Data is accurate, complete, and protected from unauthorized modification.
- **Availability:** Systems and services are resilient and accessible when required.

Orbitel's architecture incorporates **defense-in-depth** and **zero-trust principles** across its infrastructure.

5. Security Controls and Practices

Orbitel implements multiple layers of technical, administrative, and physical controls:

a. Data Protection and Encryption

- All customer and internal data are encrypted **in transit using TLS 1.2+** and **at rest using AES-256**.
- Encryption keys are managed securely under the **Encryption and Key Management Policy**.
- Sensitive data (such as PII, business communications, or API credentials) is anonymized or tokenized where possible.

b. Access Controls

- All access follows the **least privilege principle**.
- Role-based access control (RBAC) is enforced through identity management tools.
- Multi-factor authentication (MFA) is mandatory for all privileged and administrative accounts.

c. Secure Software Development

- Orbitel integrates **security-by-design** and **privacy-by-design** principles into its SDLC.
- All code changes are peer-reviewed, scanned using SAST/DAST tools, and tested before deployment.
- Production and development environments are segregated.

d. Physical and Environmental Security

- Offices and data centers use biometric or badge-based access control.
- Visitors are registered and escorted in secure zones.
- Backup power, redundant connectivity, and fire suppression systems are in place.

e. Monitoring and Auditing

- Orbitel uses centralized logging and continuous monitoring for anomaly detection.
- Security logs are retained per the **Data Retention Policy** and reviewed periodically.
- Independent audits and vulnerability assessments are performed regularly.

f. Third-Party Security

- Vendors and subprocessors undergo due diligence and sign data protection agreements.
- Cloud providers must be compliant with ISO 27001, SOC 2, and other recognized standards.

6. Awareness and Training

All Orbitel employees and contractors complete mandatory **information security and data privacy training** at onboarding and annually thereafter.
Refresher sessions are conducted following major incidents, policy changes, or new threats.

7. Compliance and Continuous Improvement

Orbitel continuously reviews and enhances its ISMS based on:

- Internal audits and management reviews.
- Changes in business processes, technology, or legal frameworks.
- Lessons learned from incidents or customer feedback.

Any policy non-compliance is treated as a disciplinary matter and may result in access suspension or corrective action.

8. Review Cycle

This policy is reviewed annually by the CISO and updated as needed to reflect changes in laws, standards, and operational requirements.