Backup and Restoration Policy

Version: 1.0
Last Updated: October 2025
Approved By: Chief Technology Officer (CTO)**
Next Review Date: October 2026

1. Purpose

The purpose of this policy is to ensure that Orbitel.ai maintains reliable, tested, and secure backup and restoration procedures that protect data availability and integrity during system failures, cyber incidents, or disasters.
This policy supports Orbitel's Business Continuity and Disaster Recovery (BCP/DR) strategy.

2. Scope

Applies to all:

- Databases, application data, configuration files, and code repositories.
- Cloud-hosted systems, customer environments, and critical business records.
- Backup storage media and services managed directly or through authorized vendors.

3. Governance and Responsibilities

- **CTO:** Owns and approves backup standards and recovery procedures.
- **Infrastructure and DevOps Teams:** Implement automated backup systems and test restorations.
- **Information Security Team:** Monitors backup encryption and access controls.

4. Policy Statements and Controls

a. Backup Frequency and Coverage

- **Critical systems** (production databases, configurations, and logs) are backed up daily.
- **Non-critical systems** follow weekly or bi-weekly schedules.
- Backups are automated, logged, and monitored for successful completion.

b. Encryption and Storage Security

- All backups are encrypted using AES-256 before transfer or storage.
- Backup data is stored in geographically redundant, access-controlled environments.
- Access to backups is restricted to authorized personnel only via role-based controls and MFA.

c. Data Retention and Rotation

- Backups are retained for a minimum of 30 days, with retention periods defined by system criticality.
- Old backups are securely deleted following Orbitel's Data Retention and Deletion Policy.

d. Testing and Verification

- Restoration tests are conducted quarterly to validate backup integrity and recovery timelines.
- Tests are documented with recovery time and data accuracy metrics.

e. Restoration and Recovery

- In the event of data loss, the latest verified backup is restored in coordination with the Incident Response Team.
- Recovery procedures follow predefined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

5. Compliance and Continuous Improvement

Orbitel's backup procedures comply with ISO 27001 A.12.3 and ISO 22301 standards.
Backup and restoration processes are reviewed annually and following any significant system upgrade or security incident.