Business Continuity and Disaster Recovery (BCP/DR) Policy

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

1. Purpose

The purpose of this policy is to define Orbitel.ai's strategy for maintaining operational continuity and minimizing disruption in the event of natural disasters, cyber incidents, or major system failures.

Orbitel's BCP/DR framework ensures resilience, timely recovery, and the protection of critical business functions.

2. Scope

Applies to:

- All Orbitel business operations, cloud platforms, and customer-facing services.
- Core functions such as product delivery, customer support, and data hosting.

3. Governance and Responsibilities

- **CTO:** Oversees the BCP/DR framework and approves major revisions.
- **Business Continuity Manager:** Coordinates BCP planning, testing, and documentation.
- **Operations and Infrastructure Teams:** Maintain redundant systems and backup processes.
- **All Employees:** Must understand their role during a declared continuity event.

4. Policy Statements and Controls

a. Business Impact Analysis (BIA)

- Critical functions and dependencies are identified and ranked by Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- Risks such as cyberattacks, data center outages, and third-party failures are assessed annually.

b. Data Backups

- Backups are encrypted, geographically redundant, and performed daily.
- Backup integrity is verified through monthly restoration drills.

c. Disaster Recovery Readiness

- Orbitel maintains failover environments in multiple cloud regions to support rapid recovery.
- DR plans include detailed step-by-step restoration procedures for systems, databases, and network configurations.

d. Continuity Planning

- Alternate communication channels and collaboration tools are available for employees during outages.
- Third-party dependencies are reviewed for resilience and response capabilities.

e. Testing and Review

- Tabletop and live failover tests are conducted bi-annually.
- Lessons learned are documented and integrated into the next BCP revision.

5. Communication and Escalation

During a disruption, the Incident Response Team activates the BCP protocol, notifies stakeholders, and provides status updates until services are restored.

6. Compliance and Continuous Improvement

Orbitel's BCP/DR framework aligns with ISO 22301 and ISO 27031 standards.
Results of recovery tests and impact analyses are reviewed annually by the CTO and reported to the executive team.