Access and Identity Management Policy

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

1. Purpose

This policy defines Orbitel.ai's approach to managing user identities, authentication, and authorization mechanisms to protect access to corporate and customer data.

Its goal is to ensure that:

- Access is restricted to authorized personnel only.
- Authentication mechanisms are secure and monitored.
- Accounts are managed throughout their lifecycle to prevent misuse or unauthorized access.

2. Scope

This policy applies to:

- All Orbitel employees, contractors, and third parties with logical or physical access to Orbitel's networks, cloud platforms, and applications.
- Identity and access controls across all corporate, development, and production environments.

3. Roles and Responsibilities

- **Security Team:** Administers access control systems, monitors logs, and enforces policy compliance.
- **Department Managers:** Approve or revoke access for their teams based on job functions.

- **Human Resources:** Coordinates account provisioning and deactivation during onboarding and offboarding.

- **All Users:** Must safeguard their credentials and immediately report any suspected compromise.

4. Policy Statements and Controls

a. Identity Lifecycle Management

- Access requests must be documented, reviewed, and approved by the responsible manager.

- User accounts are uniquely identifiable and tied to verified identities.

- Accounts are automatically disabled upon termination or inactivity beyond a defined threshold.

b. Authentication Requirements

- All Orbitel systems enforce **multi-factor authentication (MFA)** for privileged access.

- Passwords follow minimum complexity and rotation standards consistent with NIST SP 800-63B.

- Service accounts use certificates or keys instead of passwords where feasible.

c. Authorization and Least Privilege

- Role-based access control (RBAC) is applied consistently across systems.

- Privileged users have separate administrative accounts for sensitive operations.

- Access rights are reviewed quarterly by department heads and the Security Team.

d. Session Management and Logging

- Sessions automatically time out after defined periods of inactivity.

- All access events, logins, and administrative actions are logged, monitored, and retained for investigation.

e. Third-Party and Vendor Access

- Third-party access is granted only under formal contracts and NDAs.
- Access is time-limited, purpose-specific, and monitored.
- Vendors must comply with Orbitel’s security standards.

5. Monitoring and Enforcement

- Automated tools detect anomalous login patterns and privilege escalations.
- Any unauthorized or suspicious access is immediately escalated to the Security Team for review.
- Violations may result in suspension, investigation, or termination of access privileges.

6. Compliance and Review

This policy supports Orbitel’s compliance with ISO/IEC 27001:2022, DPDP 2023, and GDPR.
It is reviewed annually or following any significant change in system architecture, vendor landscape, or compliance requirements.