Security Overview

TalentOS — Confidential · June 2026

TalentOS is built with security as a first-class concern. This one-pager summarises our key security controls, practices, and compliance posture.

Infrastructure & Hosting

TalentOS is hosted on AWS with multi-region redundancy. All infrastructure is provisioned via Infrastructure-as-Code (Terraform) and audited continuously. We maintain a 99.9% uptime SLA.

Data Encryption

All data is encrypted at rest (AES-256) and in transit (TLS 1.2+). Encryption keys are managed via AWS KMS with automatic rotation. Database backups are encrypted and retained for 30 days.

Access Control

Access follows the principle of least privilege. Employee access is managed via SSO with MFA enforced. Customer data is isolated per tenant with row-level security enforced at the database layer.

Vulnerability Management

Continuous SAST/DAST scanning via SonarQube and Trivy. Dependencies are audited weekly. Critical vulnerabilities are patched within 24 hours; high severity within 7 days.

Incident Response

We maintain a documented incident response plan with defined SLAs. Security incidents are escalated within 1 hour. Affected customers are notified within 72 hours per GDPR requirements.

Compliance

TalentOS operates in compliance with GDPR and CCPA. We conduct annual third-party security audits and maintain a formal data retention and deletion policy.

Security Contact

Report vulnerabilities or security concerns to security@talentos.io. We operate a responsible disclosure program and aim to respond within 48 hours.