

Information Security Risk Management

How Workplacer identifies, assesses, treats, and monitors information security risk.

1. OVERVIEW

Workplacer operates a continuous information security risk management process. Risk is managed as an ongoing cycle — identification, assessment and prioritization, treatment, and monitoring — embedded in day-to-day engineering rather than treated as a periodic exercise. The process is operational today. Workplacer is not currently certified against ISO 27001 or SOC 2 (Section 5).

2. PROCESS

Phase	Activities
Identify	Automated dependency scanning (GitHub Dependabot) with daily security-advisory monitoring; automated architecture and security audits against internal rules (tenant isolation, background-job safety, data-handling); founder and AI-assisted code review on every change; and periodic security self-assessment.
Assess & prioritize	Findings are triaged by severity and exploitability. Remediation is driven by defined service levels (below). Where a risk is accepted rather than immediately remediated, the acceptance is recorded with an expiry date so it is re-reviewed rather than silently retained.
Treat	Remediation through code fixes, dependency upgrades, and configuration changes. Every change is verified in CI (TypeScript strict typing, linting, automated unit and end-to-end tests) and reviewed before it reaches production.
Monitor	Daily security-posture review across production error tracking (Sentry), the immutable application audit log, and dependency advisories; real-time anomaly surfacing in production; rate limiting on cost- and abuse-sensitive endpoints.

3. REMEDIATION SERVICE LEVELS

Severity	Target time to remediate
Critical	Within 7 days of confirmation
High	Within 14 days of confirmation
Medium / Low	Prioritized and scheduled into the normal release cycle

4. SUPPORTING CONTROLS

- **Secure development lifecycle** — branch-and-review model; no change reaches production without review and passing CI gates.
- **Access & isolation** — role-based access control, per-tenant data isolation enforced at the query layer, encryption in transit (TLS 1.3) and at rest (AES-256).
- **Secrets management** — credentials held in per-environment secret storage; never committed to source control; never logged.
- **Audit logging** — immutable audit trail across data-changing operations, retained per the data retention schedule.
- **Incident response** — defined breach-notification process with a 72-hour notification commitment aligned to GDPR Article 33, followed by a root-cause report.

5. MATURITY AND ROADMAP

The risk management process described above is operational and continuous. Workplacer is not currently certified against ISO 27001 or SOC 2. We align our controls with the principles of these frameworks and will pursue formal certification and independent penetration testing as the business scales. Customer-led security reviews are welcomed under NDA.

This document summarizes Workplacer's information security risk management process for due-diligence purposes. It should be read alongside our Data Processing Agreement, Data Retention Schedule, and Backup & Disaster Recovery documentation.