

Threat & Vulnerability Management Policy

How Workplacer identifies, classifies, remediates, and monitors security threats and vulnerabilities.

1. PURPOSE & SCOPE

This policy defines how Workplacer manages threats and vulnerabilities across the systems that build, run, and store data for the Workplacer platform — application code, dependencies, cloud infrastructure, and the data layer. It applies to all newly developed and existing functionality that could interact with customer data.

2. RESPONSIBILITY

Overall accountability for threat and vulnerability management sits with engineering leadership (currently the founder). Day-to-day identification and remediation are embedded in the development process and supported by automated tooling. This is a continuous process, not a periodic exercise.

3. VULNERABILITY IDENTIFICATION

- **Dependency scanning** — automated scanning of third-party dependencies (GitHub Dependabot), with security advisories monitored daily.
- **Static analysis** — TypeScript strict-mode type checking and linting enforced on every change before merge.
- **Security review** — human and AI-assisted review of code changes for security regressions.
- **Automated architecture audits** — internal checks enforce data-safety rules on every change, including multi-tenant isolation, safe background-job handling, and centralized data/prompt handling.
- **Periodic assessment** — recurring security assessment of the codebase (threat modelling and vulnerability review).

4. SEVERITY CLASSIFICATION & REMEDIATION SLAS

Identified vulnerabilities are triaged by severity and exploitability, and remediated within the following target timeframes:

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

Where a vulnerability is accepted rather than immediately remediated, the acceptance is recorded with an expiry date so it is re-reviewed rather than silently retained.

5. REMEDIATION & VERIFICATION

Remediation is delivered through code fixes, dependency upgrades, and configuration changes. Every change is verified in continuous integration (strict typing, linting, automated unit and end-to-end tests) and reviewed before deployment. Deployments are zero-downtime with instant rollback available.

6. THREAT MONITORING

- **Runtime monitoring** — real-time error and anomaly surfacing in production via Sentry.
- **Audit logging** — immutable audit trail across data-changing operations.
- **Rate limiting** — applied to abuse- and cost-sensitive endpoints to mitigate automated abuse.
- **Preventive controls** — enforced multi-tenant isolation, least-privilege role-based access, and encryption in transit (TLS 1.3) and at rest (AES-256).

7. MATURITY & REVIEW

This policy and the controls it describes are operational and continuous. Workplacer is not yet independently validated by an external penetration test or formal certification (ISO 27001 / SOC 2); commissioning an independent penetration test and formal attestation is planned as the business scales. This policy is reviewed at least annually and when significant changes to the platform or its architecture occur.

This policy should be read alongside our Information Security Risk Management summary, Software Development Lifecycle controls, and Business Continuity & Disaster Recovery Plan.