

Access Control Policy

How Workplacer controls who can access systems and customer data, and on what basis.

1. PURPOSE & SCOPE

This policy defines how access to the Workplacer platform, its data, and its supporting infrastructure is granted, enforced, reviewed, and revoked. It applies to application users, administrators, and the personnel who operate the production environment.

2. PRINCIPLES

- **Least privilege** — individuals are granted only the access necessary for their role.
- **Role-based access control (RBAC)** — access is assigned through defined roles rather than ad hoc permissions.
- **Multi-tenant isolation** — every data access is scoped to the owning company; cross-tenant access is not permitted and is enforced at the data-access layer, not the user interface.

3. IDENTITY & AUTHENTICATION

- Application access requires an authenticated, session-based login. Sessions expire after 7 days.
- Administrative and infrastructure accounts (hosting, database, source control) require multi-factor authentication.
- Credentials and secrets are stored in per-environment secret storage, never committed to source control and never logged.

4. AUTHORIZATION MODEL

Within each company, access is governed by membership tiers (Owner, Admin, Member, Viewer) and a granular capability model. Permissions are further scoped by company, site, and project. Authorization is enforced server-side on every request, so a user can only read or change data their role and scope permit.

5. PRODUCTION & INFRASTRUCTURE ACCESS

Access to production infrastructure (hosting, database, secrets) is limited to essential personnel (currently the founder) on a least-privilege basis, through managed provider consoles protected by multi-factor authentication. Changes reach production only through a reviewed pipeline with automated checks, not ad hoc modification.

6. PROVISIONING & DEPROVISIONING

- Access is provisioned per individual, aligned to role.

- When a person leaves or a contract ends, their access is revoked immediately: application accounts and memberships are removed (which invalidates active sessions), infrastructure access is removed through the provider consoles, and any shared secrets they could have known are rotated.

7. MONITORING & REVIEW

Data-changing operations are recorded in an immutable audit log. Access is reviewed when roles change and at least annually. This policy is reviewed at least annually and on significant change. Formalised, granular access roles and periodic access certification will be expanded as the team grows.

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