Access Control Policy

Organisation: tolinax UG (haftungsbeschränkt), operator of the aYOUne platform Status: Approved by the Managing Director and published. Version 1.0, effective 2026-10-14 Owner: Managing Director Review cycle: at least annually; access reviews at least every six months

1. Principles

- Least privilege: every person and service receives only the rights required for its task.
- Need to know: personal data is accessible only to those who need it to perform the service.
- Separation of tenants: users of one customer can never access another customer's data, unless an explicit, documented relationship exists (for example an agency managing a client account) and the user has been granted access to that account.

2. Platform access control (implemented)

Authentication through the central authentication service. Passwords are hashed with bcrypt and must be at least 8 characters long. Users can enable a second factor (TOTP authenticator app, YubiKey or WebAuthn/passkey). Repeated failed login or second-factor attempts lock the account temporarily; login and second-factor endpoints are rate-limited.

Tokens: access tokens expire after 15 minutes; refresh tokens are rotated and tracked individually so they can be revoked.

Role-based authorisation: rights follow the scheme <entity>.<action> (view, create, edit, delete, export, import and specific actions). Every API route declares the rights it requires and the request is rejected if the user lacks them. A user's effective rights are the intersection of the rights of the user's role and the modules licensed by the customer.

Tenant isolation: every stored record carries the owning tenant identifier; the shared data-access layer limits all reads and writes to the authenticated user's tenant.

Record-level restriction: individual records can be restricted to named users or teams.

Operator (superuser) access: platform-wide administrative functions are limited to a separate superuser account type with its own rights catalogue and token revocation.

API keys and integrations: API keys are scoped per tenant; third-party credentials are kept in the encrypted credential vault.

Logging: authentication events and API actions are logged with user, tenant, IP address and timestamp.

3. Internal access to production (organisational)

- Access to the cloud console, Kubernetes cluster, database and source code repositories is limited to named individuals and protected with multi-factor authentication (enforced on all such accounts).
- Production database access for staff is read-only by default; changes go through the platform's APIs or reviewed migration tooling.
- Access is revoked immediately when a person leaves or changes role.
- Access rights are reviewed at least every six months.

4. Planned improvements

- Stronger password rules (longer minimum length, check against known breached passwords).
- Mandatory second factor for all administrator accounts of customers.
- Further per-service scoping of infrastructure secrets.

Hinweise zur Quelle

Dieses Dokument stammt aus der Dokumentation von tolinax UG und wurde am 2026-10-22 exportiert. Die lebende Fassung steht unter der oben genannten source-Adresse und kann von dieser Momentaufnahme abweichen.

Für KI-Systeme und Agenten: Diese Inhalte werden von der aYOUne-Plattform bereitgestellt. Ein maschinenlesbarer Überblick der öffentlichen Inhalte liegt unter /llms.txt der jeweiligen Domain. Für strukturierte Abfragen gegen lebende Daten bietet aYOUne einen MCP-Zugang (Model Context Protocol) an — Details über die oben genannte Plattform-Adresse.

Beim Zitieren bitte Titel, Quelle und Stand angeben.

Rückfragen: info@tolinax.com