Pflichtenheft - company-service - Version 1.4 (Minor)

Service-Name	company-service
Version	1.4 (Minor)
Stand	25.02.2026
Ziel	Konsolidierung Tenant-/Security-Contract gemäß auth-service v1.1 und verbindliche Headquarter-Regel kompatibel zu FlowTrack v2.1.
Geltungsbereich	Verwaltung von Company-Metadaten und Locations inkl. Jurisdiktion (timezone/countryCode/regionCode) und Docking zu contact-/communication-service.

0. Änderungshistorie (gegenüber V1.3)

- Security-Kapitel wird wieder verbindlich: JWT Resource Server, Audience strict, tenant_id Quelle der Wahrheit.
- Headquarter-Regel wird präzisiert und technisch erzwungen (genau ein HQ je Company).
- Standardisierte Request-Header (X-Correlation-Id, Idempotency-Key) und Fehlercodes.

1. Ziele (V1.4)

- Verhindern von Cross-Tenant Zugriffen (IDOR) auf Company/Location.
- Eindeutige, systemweit konsistente Definition: Hauptsitz/Headquarter.
- Einheitliche Security-Konventionen wie in FlowTrack v2.1 und auth-service v1.1.

2. Security & Tenant-Isolation (MUSS)

JWT Validierung:
- Issuer/JWKS Signaturprüfung, exp/iat, kid Rotation.
- Audience-Check: aud muss "company-service" enthalten (strict).
- Pflicht-Claims: iss, sub, aud, exp, iat, jti, tenant_id, subject_type, scp.
Tenant Enforcement:
- Alle Endpunkte mit {companyId}: companyId muss tenant_id entsprechen.
- Endpunkte mit {locationId} ohne companyId: location.companyId muss tenant_id entsprechen.
No data leak Policy:
- Optional 404 statt 403 bei Fremdmandant (konfigurierbar), Default: 403 TENANT_MISMATCH.

3. Headquarter-Regel (MUSS)

FlowTrack Kompatibilität:
- Pro Company existiert genau ein Hauptstandort (Headquarter).
- Hauptstandort muss OPEN/aktiv sein.
Technische Umsetzung (MUSS):
- Canonical: company.mainLocationId ist die Quelle der Wahrheit.
- Zusätzlich (KANN): LocationResponse liefert isHeadquarter = (locationId == mainLocationId) für UI/Clients.
API (neu/konkretisiert):
- GET /api/v1/companies/{companyId}/headquarter -> { "locationId": "..." }
- PUT /api/v1/companies/{companyId}/headquarter (Idempotency-Key empfohlen)
Body: { "locationId": "..." }

Validierung:
- locationId muss existieren und zur gleichen companyId gehören, sonst 409/404.
- Ein Setzen auf CLOSED Location ist nicht erlaubt (409 HEADQUARTER_MUST_BE_OPEN).

4. Request-Konventionen

Headers:
- Authorization: Bearer
- X-Correlation-Id (SOLL): wird in Response gespiegelt
- Idempotency-Key (MUSS) für POST /companies (Bootstrap) und PUT /headquarter
Fehlerformat:
- Einheitliches Error DTO (status, errorCode, message, correlationId, path, details[])

5. API-Ergänzungen (V1.4)

Bestehende APIs bleiben bestehen.
Ergänzung/Schärfung:
- PUT /api/v1/companies/{companyId}/headquarter
- GET /api/v1/companies/{companyId}/headquarter
- LocationResponse enthält (SOLL): contactOwnerType/contactOwnerId und isHeadquarter

6. Tests & Abnahmekriterien

- Fremdmandant-Zugriff auf /companies/{companyId} und /locations/{locationId} wird geblockt (403 oder 404).
- Headquarter kann gesetzt werden und ist danach eindeutig (genau eine HQ Location).
- Versuch, HQ auf CLOSED Location zu setzen -> 409.
- Alle Endpunkte dokumentiert in OpenAPI inkl. Security/Scopes/Fehlerfälle.