CS-DOC-0003 · GXP-DESK DOCUMENTATION

Roles and Permissions.

FIT-only redaction. Effective 2026-06-04.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0003	v1.0	2026-06-04	Customer Success

Public — Documentation · Review cycle: On change

01 — DOCUMENT CONTROL

Control block and metadata anchor.

The control block identifies the document, its current revision, the regulated process it supports, and the people accountable for its lifecycle. Every value below is the source of truth for any downstream record, audit trail entry, or signature block.

DOCUMENT ID	CS-DOC-0003
TITLE	Roles and Permissions
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-06-04
REVIEW CYCLE	On change
DOCUMENT OWNER	Customer Success
CLASSIFICATION	Public — Documentation
RELATED RECORDS	—
SUPERSEDES	— (initial release)

02 — APPROVALS

Sign-off table, ready for ink or e-signature.

The signatures below confirm review and authorisation of this document. Approvals must be recorded in chronological order. If the document is signed electronically, the e-signature record on the GxP-Desk platform supersedes any handwritten entry on this page and carries the same legal weight under 21 CFR Part 11 and EU GMP Annex 11.

Role	Name	Function	Date	Signature
Author		Validation Lead		
Reviewer		Quality Assurance		
Reviewer		Process / System Owner		
Approver		Head of Quality		
Approver		Regulatory Affairs		

03 — CONTENTS

What's in this document.

01 — Document Control 2

02 — Approvals 3

03 — Contents 4

01 — What this version covers 5

02 — What this version does NOT cover (roadmap topics) 6

03 — How permissions work 7

04 — Permission patterns in this implementation 8

05 — Separation of Duties (SoD) — Hard-Wired Enforcement 10

06 — User flags for admin access 11

07 — Permission Troubleshooting 12

08 — Code references 13

Revision History 14

Glossary & Abbreviations 15

01 — WHAT THIS VERSION COVERS

What this version covers.

This documentation addresses the permission model of GxP-Desk:

- The 3-level permission concept (Account/Tenant/Change)
- The role structure with permissions and the isCustom flag
- Hard-wired Separation of Duties (SoD) enforcement
- TenantUserAssignment with roleId for tenant-scoped assignments
- The isSystemAdmin and isAccountAdmin flags on User

02 — WHAT THIS VERSION DOES NOT COVER (ROADMAP TOPICS)

What this version does NOT cover (roadmap topics).

The following concepts from the original spec are not, or only partially, implemented:

- **Complete built-in-roles taxonomy with concrete names** — The Role model exists, but a defined list of named built-in roles (Account Owner, Account Admin, Tenant Owner, QA Approver, etc.) is not enforced in code. (Roadmap: see `/gap-implementation-plans/PLAN-04-*.md`)
- **Custom roles must inherit from built-in + narrowing only** — The isCustom flag exists on Role, but no validator enforces the inheritance or narrowing-only rule.
- **Permission-resolution algorithm "lowest-grant-wins"** — No implemented resolver logic that cascades inheritance and overrides across all four levels.
- **Delegation with a time limit** — Not implemented.
- **Account-Admin/Tenant-Admin/System-Admin bypass logic** — The flags exist, but the bypass mechanisms are not systematically documented.

03 — HOW PERMISSIONS WORK

How permissions work.

GxP-Desk enforces every authorization decision against a single, deterministic question:

> **NOTE**
> "At the lowest level where a value was granted to this user — what does that value say?"

The answer is the user's effective permission. There are no implicit assignments, no overlap rules, and no priority ordering to remember — only the 4-level hierarchy (Account → Tenant → System → Change) and the rule that the lowest explicit assignment wins.

The three components of every assignment

Component	What it specifies	Examples
Subject	The individual user being granted access	`jane.doe@acme.com` (email as the unique user ID)
Role	The named bundle of capabilities	Tenant Owner, QA Approver, System Author, Read-Only Auditor, Custom Role
Scope	The hierarchy node on which the role applies	Account, a tenant, a system, a single change

Effective permission = the lowest explicit assignment:

If Jane has **QA Approver** at the tenant level and **Read-Only** on a specific system, her effective permission on that system is **Read-Only**. The platform always narrows on the way down, never broadens. There is no configuration setting to reverse this — intentionally.

Permission patterns in this implementation.

The 3-level model

GxP-Desk implements permission guards at three levels:

Level	Guard function	Purpose
Account level	`requireAccountPermission()`	Account admin, user management, tenant lifecycle
Tenant level	`requireTenantPermission()`	Tenant-specific operations, system registration, change management
Change level	`requireChangePermission()`	Change-specific operations, deliverable approval

System Admin and Account Admin bypass:

Users with `isSystemAdmin = true` or `isAccountAdmin = true` bypass all permission checks at their respective level.

Role model

The `Role` model in Prisma has:

```
model Role {
  id             String
  name           String
  isCustom       Boolean @default(false)  // true wenn customer-authored
  permissions    String[]                 // Array von capability strings
  accountId      String
  account        Account
  // ...
}
```

The `permissions` are modeled as a string array. No resolver logic is implemented for inheritance or narrowing validation.

TenantUserAssignment

The M2M relationship between user and tenant carries an optional `roleId`:

```
model TenantUserAssignment {
  id        String
  userId    String
  tenantId  String
  roleId    String?    // optional tenant-scoped role override
  isDefault Boolean    // default tenant on login
  // ...
}
```

This allows a user to be assigned a specific role at the tenant level.

05 — SEPARATION OF DUTIES (SOD) — HARD-WIRED ENFORCEMENT

Separation of Duties (SoD) — Hard-Wired Enforcement.

GxP-Desk enforces SoD at the change level. The enforcement point is in the signature and approval flows:

SoD rule	Status in code	Enforced in
Author ≠ Reviewer	Implemented	`app/actions/signatures.ts:35`
Author ≠ Approver	Implemented	`app/actions/signatures.ts:44`
Reviewer ≠ Approver	Configurable (disabled by default)	Policy engine (planned)

Why SoD is hard-wired:

Every published warning letter concerning computerized systems contains at least one deviation of the form: *"the same person approved their own work"*. Hard-wiring SoD removes the most common Annex 11 / Part 11 deviation category before the inspection begins.

06 — USER FLAGS FOR ADMIN ACCESS

User flags for admin access.

The `User` model carries two admin flags:

```
model User {
  id              String
  email           String @unique
  isSystemAdmin   Boolean @default(false)  // Gesamtplattform-Admin
  isAccountAdmin  Boolean @default(false)  // Account-Level Admin (NEW)
  // ...
}
```

- **isSystemAdmin** — Bypasses all permission checks. Access to every account, every tenant, every system.
- **isAccountAdmin** — Bypasses permission checks at the account level. Access to account settings, user management, and tenant creation within the account.

07 — PERMISSION TROUBLESHOOTING

Permission Troubleshooting.

Symptom	Likely Cause	Resolution
A user cannot see a tenant they expect	No tenant-scoped role assigned; an account-level role alone does not grant tenant visibility	Assign a tenant role (Read-Only is the smallest)
A user can read but not write	The effective permission is the lower of two assignments	Check for system-level assignments narrower than the tenant level
The approval button is grayed out	The user is the author or reviewer of the same record (SoD)	Reassign the author/reviewer; the platform will not relax SoD
A custom role is not available	The role is not yet QA-approved or has been retired	The Account Compliance Lead must approve it, or the role must be revived

08 — CODE REFERENCES

Code references.

Prisma models

- `User` — with `isSystemAdmin`, `isAccountAdmin`, `tenantAssignments` M2M
- `Role` — with `name`, `isCustom`, `permissions` (String[]), `accountId`
- `TenantUserAssignment` — M2M with `userId`, `tenantId`, optional `roleId`
- `Account` — with `roles` relation for account-level roles

Server actions

- `app/actions/account/*` — account creation, user management
- `app/actions/tenant/*` — tenant configuration, user assignments
- `app/actions/change/*` — change lifecycle with SoD enforcement in approval gates
- `app/actions/signatures.ts` — e-signature workflows with SoD checks at lines 35, 44

Permission guards (implemented)

- `requireAccountPermission()` — guard for account-level operations
- `requireTenantPermission()` — guard for tenant-level operations
- `requireChangePermission()` — guard for change-level operations

End of documentation

REVISION HISTORY

Every change, tracked and signed.

Add one row for every controlled revision. Minor changes (typos, formatting) increment the patch version; substantive edits trigger a fresh review cycle and a new approver round.

Version	Date	Author	Summary of Change	Approver
1.0	2026-06-04	Documentation Team	FIT-only redaction limited to codebase-verified functionality.	Head of Documentation
—	—	—	Reserved for next revision. Do not delete this row.	—

GLOSSARY

Shared language, no ambiguity.

Definitions used throughout this document. Where a term has a specific meaning inside GxP-Desk, the platform-specific definition takes precedence over the generic regulatory term.

CSV	Computerized Systems Validation
GAMP 5	Good Automated Manufacturing Practice, Edition 5 (2nd edition, 2022)
GxP	Good 'x' Practice — covers GMP, GLP, GCP, GDP, GVP
IQ / OQ / PQ	Installation / Operational / Performance Qualification
Part 11	21 CFR Part 11 — US FDA rule on electronic records and electronic signatures
Annex 11	EU GMP Annex 11 — EU rule on computerised systems
URS	User Requirements Specification
FRS	Functional Requirements Specification
RTM	Requirements Traceability Matrix
SOP	Standard Operating Procedure
ALCOA+	Attributable, Legible, Contemporaneous, Original, Accurate (+ Complete, Consistent, Enduring, Available)
ICH Q9	International Council for Harmonisation Quality Risk Management guideline

— End of document —