AG RUNBOOK — Phase 7.2

User Deactivation & Reactivation

Purpose:

This runbook defines a controlled, auditable process for deactivating and reactivating users within a tenant.

The goal is to immediately remove access while preserving audit history and tenant isolation.

Global Constraints:

- Do not delete users
- Do not modify authentication or token logic
- Do not weaken tenant isolation
- Do not bypass audit logging
- Do not remove historical data
- Assume Phase 7.1 (invite-only provisioning) is complete

User Lifecycle States:

- ACTIVE: User can authenticate and access the system
- DISABLED: User is blocked from authentication and all sessions are revoked

Step 1 — Schema Verification:

- Ensure UserStatus enum contains:
- PENDING
- ACTIVE
- DISABLED
- No schema changes should be required if Phase 7.1 is complete

Step 2 — Admin API: Deactivate User:

Endpoint:

POST /api/admin/users/{userId}/deactivate

Behavior:

- Require admin authentication
- Ensure target user belongs to the same tenant
- Set user status to DISABLED
- Revoke all active sessions for the user
- Do not delete user data
- Log audit event:
- action = USER.DEACTIVATE
- actorType = ADMIN
- target = userId
- metadata may include reason

Step 3 — Login Guard Enforcement:

- Ensure DISABLED users cannot log in
- Existing login guard logic must already block DISABLED users
- Do not add new middleware

Step 4 — Admin API: Reactivate User:

Endpoint:

POST /api/admin/users/{userId}/reactivate

Behavior:

- Require admin authentication
- Ensure user belongs to the same tenant
- Set user status to ACTIVE
- Do NOT restore previous sessions
- User must log in again
- Log audit event:
- action = USER.REACTIVATE
- actorType = ADMIN
- target = userId

Step 5 — Audit Taxonomy Verification:

- Ensure USER.DEACTIVATE and USER.REACTIVATE actions exist
- Add actions if missing without renaming existing ones

Success Criteria:

- Deactivated users lose access immediately
- Sessions are revoked on deactivation
- Reactivated users must re-authenticate
- Full audit trail exists for both actions
- No tenant boundary violations occur

Out of Scope:

- User deletion
- Data anonymization
- Bulk deactivation
- UI changes
- Email notifications