

# HRH API – Comprehensive Engineering Specification

This document defines the full architectural blueprint, behavioral contracts, engine rules, validation logic, and API invariants required to implement a robust, dynamic, multi-location HRH approval system.

System Guarantees:

- No approval bypass
- No permission escalation
- Dynamic multi-location scope enforcement
- Ordered workflow control
- Delegation overlays without authority corruption
- Immutable audit history
- Zero hardcoded business logic

## PHASE 0 – SYSTEM FOUNDATIONS & INVARIANTS

Core Invariants:

1. Permission without scope is inactive.
2. Scope without permission is inactive.
3. Workflow state exclusively controls status transitions.
4. Delegation overlays never mutate base permissions.
5. Workflow templates are immutable once versioned.
6. Location hierarchy must remain acyclic.
7. All state transitions must be logged.
8. Soft deletion enforced for critical entities.

Authority Formula:

Effective Authority =

Permission

+ Location Scope Resolution

+ Delegation Overlay

+ Workflow Step Eligibility

+ Active Status Validation

## PHASE 1 – CORE INFRASTRUCTURE & ACCESS CONTROL

Authentication:

- JWT access + refresh tokens
- Password hashing (argon2/bcrypt)
- Token rotation
- Status validation before issuance

User Model:

- UUID primary key
- Unique email constraint
- Status enforcement
- Primary location mapping

Role & Permission Engine:

- Dynamic permission registry
- Many-to-many role-permission mapping
- Immediate propagation on change

Location Engine:

- Tree structure (parent\_id)
- Subtree resolution
- Cycle prevention
- Safe node movement

API Enforcement Parameters:

- ✓ Stateless permission checks
- ✓ Disabled roles ignored
- ✓ Disabled users blocked
- ✓ Location integrity preserved

## **PHASE 2 – SCOPE ENGINE (MULTI-LOCATION AUTHORITY)**

Scope Model:

- user\_id
- permission\_id
- location\_id
- include\_descendants
- valid\_from
- valid\_until
- status

Rules:

- Supports global scope
- Supports subtree inheritance
- Time-bound enforcement
- Overlapping scopes merge logically

Validation:

- ✓ Cross-region approval accuracy
- ✓ Scope expiration auto-block
- ✓ Immediate revocation enforcement

## **PHASE 3 – DELEGATION ENGINE**

Delegation Model:

- delegator\_user\_id
- delegate\_user\_id

- permission\_id
- location\_id
- include\_descendants
- valid\_from
- valid\_until
- status

Constraints:

- Delegate cannot exceed delegator authority
- Expiry automatic
- Revocation immediate

Audit:

- Log original delegator
- Delegation trace included in authority resolution

Validation:

- ✓ Expiry enforcement
- ✓ Escalation prevention
- ✓ Revocation safety

## PHASE 4 – WORKFLOW ENGINE

Core Entities:

- WorkflowTemplates
- WorkflowSteps
- WorkflowInstances
- WorkflowStepInstances

Execution Rules:

1. Template selected by resource + location
2. Instance created per submission
3. Sequential step enforcement
4. Final approval locks resource
5. Adjustment loops supported

Validation:

- ✓ No step skipping
- ✓ No concurrent approvals
- ✓ Version isolation
- ✓ Strict transition validation

## PHASE 5 – LEAVE MANAGEMENT MODULE

Entities:

- LeaveTypes
- LeaveBalances
- LeaveRequests

Flow:

1. Balance validation

2. Create draft
3. Submit → workflow
4. Approval deducts balance
5. Decline preserves balance

Rules:

- Approved leave immutable
- Adjustments logged
- Cross-location validation required

Validation:

- ✓ No negative balances
- ✓ Scope-filtered reporting
- ✓ Cross-region approval support

## PHASE 6 – TIMESHEET MODULE

Entities:

- Timesheets
- TimesheetEntries
- TimesheetPeriods

Flow:

1. Draft creation
2. Submission triggers workflow
3. Approval locks record
4. PDF generation allowed only if Approved

Rules:

- Period locking enforced
- Decline allows resubmission
- Immutable post-approval

Validation:

- ✓ Locked period rejection
- ✓ Approval order enforcement
- ✓ Cross-location validation

## PHASE 7 – REPORTING & AUDIT ENGINE

Audit Fields:

- actor\_id
- action
- resource\_type
- resource\_id
- before\_state
- after\_state
- timestamp
- ip\_address

Requirements:

- Immutable logs
- Scope-aware filtering
- Full approval timeline reconstruction
- Delegation traceability

Validation:

- ✓ No audit tampering
- ✓ Scope enforcement in reports
- ✓ Workflow trace reproducibility

## **PHASE 8 – STRESS TESTING & EDGE VALIDATION**

High-Risk Simulations:

1. Simultaneous approvals
2. Location movement mid-workflow
3. Template modification mid-process
4. Delegation expiry during approval
5. Massive overlapping scopes

Production Readiness Checklist:

- ✓ No bypass paths
- ✓ No escalation paths
- ✓ Delegations auto-expire
- ✓ Location tree integrity maintained
- ✓ Full audit coverage
- ✓ No hardcoded logic