

GOVERNED TEMPLATE RENDERING REFERENCE: MULTI-TENANT ISOLATION DESIGN DEFAULT V2 (DRAFT)

definition 3ef111e9...d1b1

MULTI-TENANT ISOLATION DESIGN · PROJECT ARTIFACT

SPECIRA

Multi-Tenant Design: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template multi_tenant_design v2 · pack: specira_default_delivery

the isolation model is the retrofit that hurts most; designed before the second tenant

§1 Isolation Strategy

mandatory

1 decision

1 evidence rule

validators: isolation_model_decision_carries_evaluation_dimensions ·
tenancy_scope_boundary_explicit · every_pooled_table_has_a_row_level_security_policy ·
scope_diagram_shades_inside_vs_outside_tenancy ·
boundary_crossing_names_the_class_it_carries_and_the_class_it_never_does

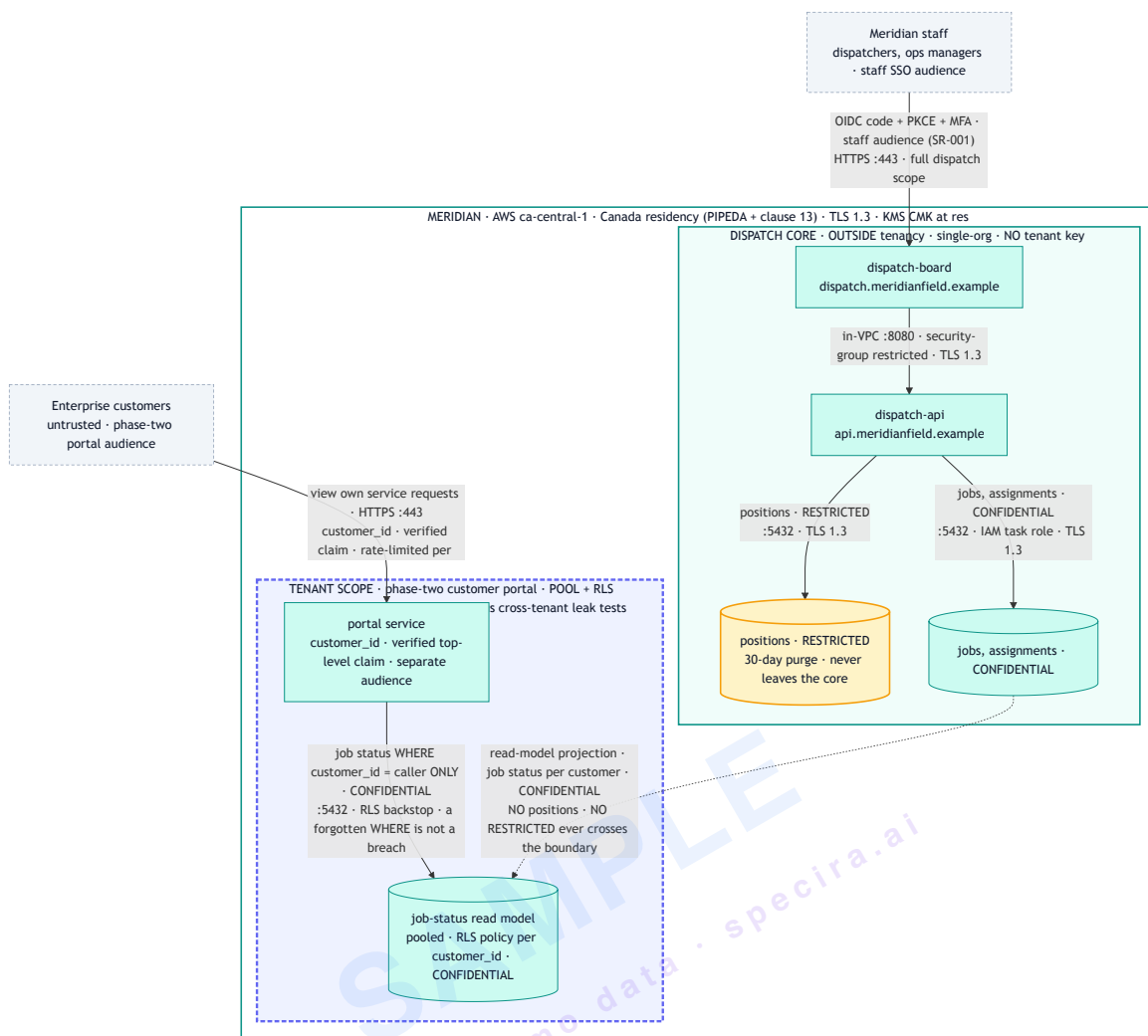
The scope boundary first: what stays OUTSIDE tenancy is recorded like what is inside. Then the model, on all five dimensions.

Scope boundary: the dispatch core (board, assignments, positions) is SINGLE-ORG internal tooling and stays OUTSIDE tenancy; the claim is recorded. Tenancy enters with the phase-two CUSTOMER PORTAL: enterprise customers tracking their own service requests (the contract's portal commitment, schedule 21). **Activation trigger:** the portal commitment's phase-two date confirmed at the contract renewal (elected regimes^[1]). Designed now: the isolation model is the retrofit that hurts most.

Model decision: POOL with row-level security

Dimension	Pool (chosen)	Silo	Bridge
Blast radius	Bounded: read-only job status per customer; no write path, no RESTRICTED classes (positions never reach the portal, labels^[2])	Strongest	Per-service mix
Cost / tenant	Lowest	Database-per-customer: disproportionate for a read-only status view	Mixed
Noisy neighbor	Quotas, §4	Solved at the data tier	Mixed
Compliance	No residency divergence at phase two	n/a	n/a
Ops	One schema, one migration run	N of everything	Escape hatch
Bridge noted: if a customer contract ever demands dedicated storage, that customer silos while the pool remains (portal isolation model^[3]).			

Tenancy context: customer_id as a verified top-level claim in the portal token (a separate audience from staff SSO, [identity model^{\[4\]}](#)); routing, scoping, and storage all derive from it; RLS policies on every portal-visible table as the backstop; a forgotten WHERE clause must not become a breach ([SR-004's isolation face^{\[5\]}](#)).



Tenancy isolation: the scope boundary under the specificity law. Fallback text: inside the Meridian boundary (AWS ca-central-1, Canada residency, [infrastructure register^{\[7\]}](#)), the DISPATCH CORE stays OUTSIDE tenancy (single-org, no tenant key): staff sign in to dispatch-board over OIDC + PKCE + MFA (SR-001); dispatch-api writes jobs and assignments (CONFIDENTIAL) and positions (RESTRICTED · 30-day purge · never leaving the core) to the RDS instance. The TENANT SCOPE holds the phase-two customer portal (POOL + RLS): enterprise customers reach the portal over HTTPS :443 authenticated by a verified customer_id claim (a separate audience), rate-limited per tier; the portal reads the job-status model WHERE customer_id = caller only, RLS the backstop against a forgotten WHERE. The one projection crossing the boundary carries CONFIDENTIAL job status per customer and never a RESTRICTED position ([labels^{\[2\]}](#)). The tenant zone's control is the RLS policy plus continuous cross-tenant leak tests, not a threat-model row; the portal is phase-two, and its threat-model coverage lands when it ships.

§2 Tenant Provisioning

mandatory

1 decision

1 evidence rule

validators: every_provisioning_step_has_a_matching_offboarding_step · deletion_gates_on_legal_hold_citing_retention

Every onboarding step has its mirror; automation theatre is the named failure mode.

Onboard	Mirror (offboard)
Create the customer tenant record	Archive it
Issue the portal identity binding	Revoke and invalidate sessions
Scope the job visibility view	Drop the scope
Apply the tier's quotas	Release them
Stamp the observability tag	Close the cost rollup

Extraction on exit: the customer's job history as a dated export within 30 days. **Deletion:** gated on legal hold ([retention rules](#)^[2]), with the assignment records' seven-year contract retention surviving customer offboarding (the precedence stated); the audit trail survives per the audit rule ([audit events](#)^[4]).

§3 Data Partitioning

mandatory 1 decision 1 evidence rule

validators: partitioning_consequences_match_chosen_model · cross_tenant_query_posture_stated · tenant_id_stamped_at_observability_capture_site

Consequences of the pool: migrations are ONE run (the pooled advantage, stated); cross-tenant queries are forbidden BY POLICY: the RLS backstop plus the query-review rule that keeps cross-customer joins out of the portal codebase. **The road not taken:** silo would have meant per-customer migration fan-outs with per-tenant tracking and production-scale rehearsal; the bridge escape hatch inherits that cost only for a silo'd customer. **Tenant key:** customer_id on every portal-visible row, indexed with the query patterns; the dispatch core carries NO tenant key, the scope boundary made operational. **Observability:** customer_id stamped at the capture site on portal spans and logs ([instrumentation](#)^[6]); the per-customer usage rollup rides the infrastructure cost tags ([environments](#)^[7]) and feeds the tier review.

§4 Noisy Neighbor Prevention

mandatory 1 decision 1 evidence rule

validators: every_tenant_tier_has_documented_quotas · quotas_extend_api_rate_tiers_not_second_system · cross_tenant_leak_tests_run_continuously_not_once

Tier	Rate	Concurrency	Export jobs
Standard	120 req/min	10	1 / day
Premium	300 req/min	25	4 / day

The limits EXTEND the API contract's rate tiers ([limits^{\[8\]}](#)), one limit system, not two. **Enforcement:** rate at the gateway; concurrency at the pool budget; export jobs at the scheduler; the throttled customer receives rate_limited with Retry-After ([error registry^{\[8\]}](#)). **Priority rule:** dispatch traffic outranks portal traffic at the shared read model; the portal degrades first, by design, and says so. **Leak-test law:** the continuous suite authenticates as customer A and asserts zero visibility of customer B across every portal endpoint; registered by id ([register^{\[9\]}](#)), running per release candidate and nightly; a one-time audit is not the control ([cross-tenant rows^{\[5\]}](#)).

§5 Open Questions

mandatory

1 decision

Question	Owner	Answer by	Blocks
Does schedule 21's portal commitment include customer-side user management (which adds an identity-admin surface to the lifecycle table)?	Product owner with the sponsor	At the contract renewal	The provisioning table's identity rows only

Refs References & Package Contents

In the Specira workspace

specira	[1] Compliance matrix: the elected contract regime (schedule 21) app.specira.ai/projects/dispatch-modernization/artifacts/compliance-matrix#regulations
specira	[2] Data classification: labels, retention rules app.specira.ai/projects/dispatch-modernization/artifacts/data-classification
specira	[3] Decision log: the portal isolation-model decision app.specira.ai/projects/dispatch-modernization/artifacts/decision-log
specira	[4] Auth & authz policy: identity model, audit events app.specira.ai/projects/dispatch-modernization/artifacts/auth-authz-policy

specira [5] Security requirements: SR-004's isolation face; cross-tenant rows
app.specira.ai/projects/dispatch-modernization/artifacts/security-requirements

specira [6] Observability: the instrumentation standard the stamp joins
app.specira.ai/projects/dispatch-modernization/artifacts/observability-monitoring#instrumentation

specira [7] Infrastructure & deployment: the cost tags app.specira.ai/projects/dispatch-modernization/artifacts/infrastructure-deployment#environments

specira [8] API contracts: rate tiers, error registry app.specira.ai/projects/dispatch-modernization/artifacts/api-contracts

specira [9] Test cases: the continuous leak-test set app.specira.ai/projects/dispatch-modernization/artifacts/test-cases

Generated by Specira · template multi_tenant_design v2 (draft) · pack specira_default_delivery lineage 3ef111e9...d1b1 · page 1 of 4

SAMPLE
seeded demo data · specira.ai