

GOVERNED TEMPLATE RENDERING REFERENCE: DATA FLOW DIAGRAMS DEFAULT V2 (DRAFT)

definition 7d53ed67...9ad6

DATA FLOW DIAGRAMS · PROJECT ARTIFACT

SPECIRA

Data Flow Diagrams: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template data_flow_diagrams v2 · pack: specira_default_delivery

the table carries the facts; the diagram carries the shape

§1 System Context (Level 0)

mandatory

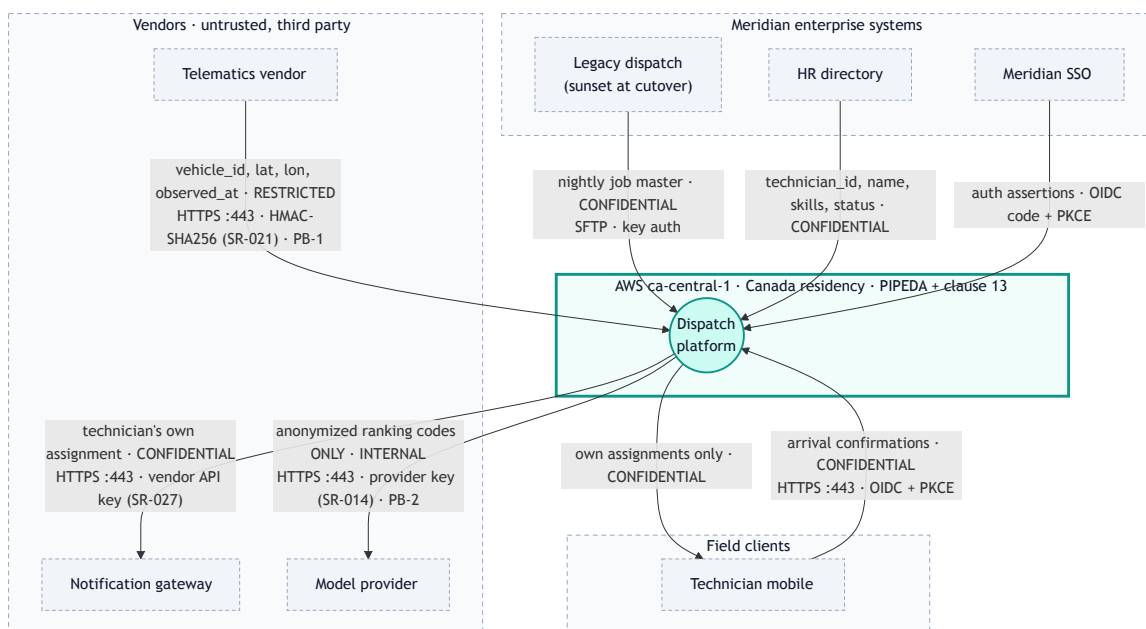
1 decision

1 evidence rule

validators: earn_its_place_rationale_or_omission_recorded ·

context_diagram_contains_no_data_stores · context_has_single_process

The *earn-its-place rationale*, stated once: the privacy assessment and the customer audit both need per-flow data-class annotation the architecture's embedded flow view does not carry (assessment^[1], audit requirements^[2]); the architecture's view is the SOURCE, cited (data flow & privacy^[3]).



Level 0: one process, externals at the edges, NO data stores at this level. The single process is a deliberate abstraction, so the node rule binds the BOUNDARY here: everything inside runs in AWS ca-central-1 under the Canada residency rule (PIPEDA + contract clause 13). The arrows still name their fields, because they cross trust boundaries at this level too. Fallback text: the telematics vendor sends vehicle_id, lat, lon and observed_at (RESTRICTED) over HTTPS 443, authenticated by an HMAC-SHA256 signature (SR-021) across PB-1; the legacy scheduler sends the nightly job master (CONFIDENTIAL) over SFTP with key auth, sunset at cutover; the HR directory syncs technician_id, name, skills and status (CONFIDENTIAL); Meridian SSO asserts identity via OIDC code with PKCE; the platform pushes each technician's own assignment (CONFIDENTIAL) to the notification gateway under a vendor API key (SR-027), and anonymized ranking codes only (no identity, no coordinates; INTERNAL) to the model provider under a provider key (SR-014) across PB-2; technician mobiles confirm arrivals and receive only their own assignments.

§2 Data Flow Details (Level 1)

mandatory

1 decision

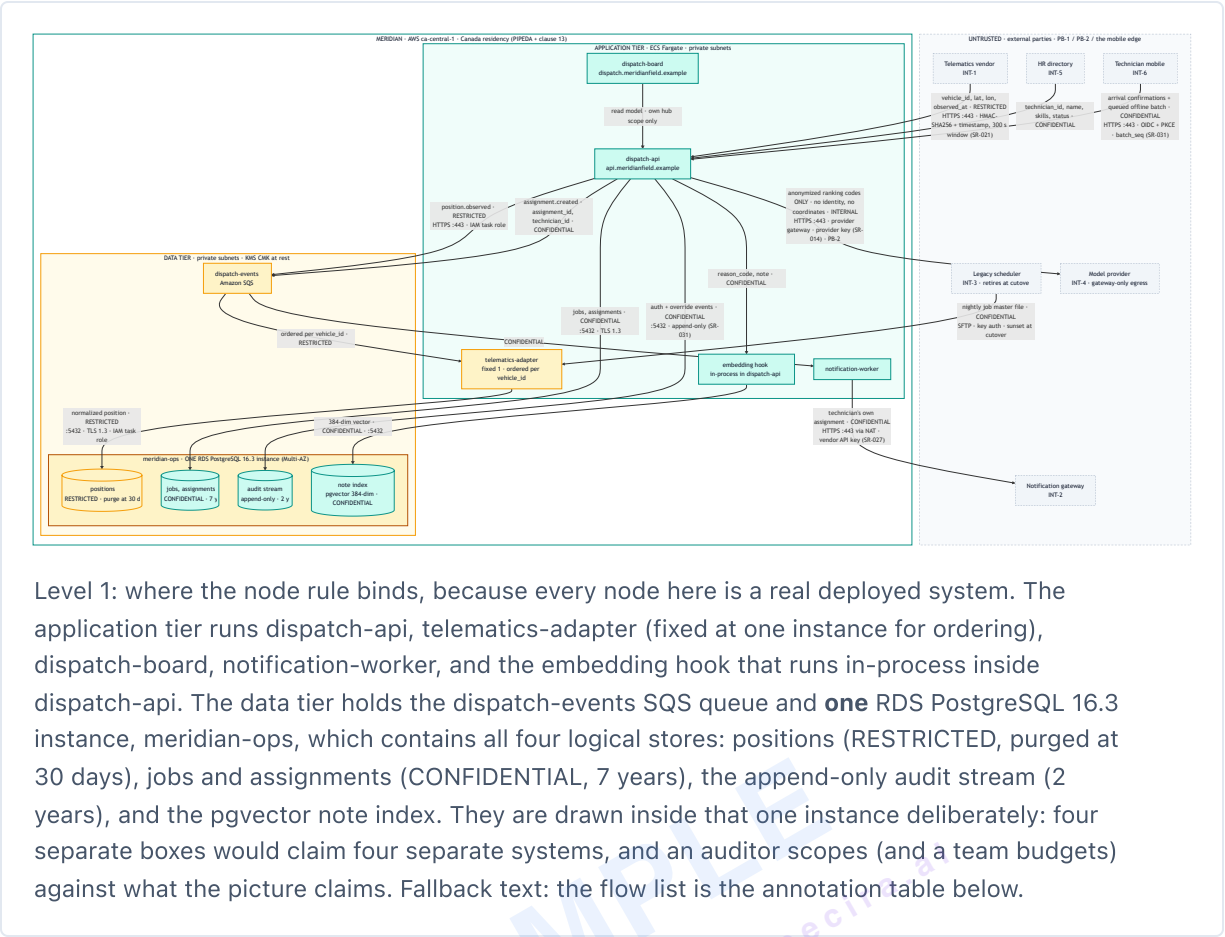
1 evidence rule

validators: every_flow_carries_a_data_class_citation ·

every_flow_resolves_to_an_integration_or_seam_row · no_orphan_arrows ·

level_one_is_maximum_depth

The stores appear for the first time at level one, and nothing goes deeper. The table owns the facts; the diagram owns the shape.



Flow	Payload: the actual fields	Class (cites)	Protocol · auth	Direction · trigger	Resolve
Positions inbound	vehicle_id, lat, lon, observed_at	RESTRICTED (labels ^[4])	HTTPS 443 · HMAC-SHA256 + timestamp, 300s window (SR-021)	Vendor → adapter · webhook delivery	INT-1
Job master nightly	the nightly job master file	CONFIDENTIAL	SFTP · key auth	Legacy → adapter · the 02:00 timer	INT-3
Assignment push	assignment_id, technician_id	CONFIDENTIAL	HTTPS 443 · vendor API key (SR-027)	Worker → gateway · assignment.created	INT-2
Anonymized ranking codes	ranking codes ONLY; no identity, no coordinates	INTERNAL	HTTPS 443 · provider key (SR-014) ·	API → model provider · suggestion request	INT-4

Flow	Payload: the actual fields	Class (cites)	Protocol · auth	Direction · trigger	Resolve
			gateway-only		
Roster sync	technician_id, name, skills, status	CONFIDENTIAL	HTTPS 443 · directory sync	HR → API · directory sync	INT-5
Auth assertions	identity assertions	n/a	HTTPS 443 · OIDC code + PKCE	SSO → board · sign-in	INT-6
Override notes to the index	reason_code, note → 384-dim vector	CONFIDENTIAL worker-conduct	in-process · PostgreSQL 5432 · TLS 1.3	API → embedding hook · override.recorded	the o

Every arrow above has a row; every row resolves; the reconciliation ran at generation, **zero orphans**.

§3 Sensitive Data Paths

mandatory

1 decision

1 evidence rule

validators: every_trust_boundary_crossing_has_a_threat_model_id · crossings_reconcile_with_threat_model_coverage · sensitive_paths_cite_handling_rules_never_restate

Crossing	Highest class	Threat model (cross-cited)
PB-1: vendor → adapter	RESTRICTED	TM-01 ^[7]
PB-2: API → model provider	INTERNAL by design: the anonymization happens BEFORE the crossing	TM-04 ^[7]
The mobile edge	CONFIDENTIAL (own assignments)	TM-05, TM-06 ^[7]
The INT-3 legacy edge	CONFIDENTIAL	Waived with expiry (coverage ^[7])

Reconciliation: these crossings and the threat model's analyzed-or-waived set are THE SAME SET, checked both directions; signed by the security owner.

Sensitive path, narrated for the auditor, a position's life: observed at the vehicle (vendor custody) → crosses PB-1 under signature verification ([SR-021^{\[8\]}](#)) → the adapter validates bounds ([VR-01^{\[9\]}](#)) → the store holds it 30 days ([retention rules^{\[4\]}](#)) → the board renders it band-masked off dispatch surfaces ([labels^{\[4\]}](#)) → the purge hard-deletes on schedule. It never reaches the model provider (the anonymized-code boundary), never enters logs ([logging^{\[10\]}](#)), and never leaves the residency region ([data flow & privacy^{\[3\]}](#)). *Handling rules cited at every hop; restated at none.*

§4 Open Questions

mandatory

1 decision

Question	Owner	Answer by	Blocks
Does the customer audit's scope include the note-index store (which would add the embedding path to the narrated set)?	N. Duval with the security owner	At the audit scoping call	The narrative's second path only

Refs References & Package Contents

In the Specira workspace

specira	[1] Privacy impact assessment: the audience needing per-flow annotation app.specira.ai/projects/dispatch-modernization/artifacts/privacy-impact
specira	[2] Compliance matrix: the customer audit's needs app.specira.ai/projects/dispatch-modernization/artifacts/compliance-matrix#audit
specira	[3] Architecture: the source data-flow view; residency placement app.specira.ai/projects/dispatch-modernization/artifacts/architecture
specira	[4] Data classification: labels, retention rules app.specira.ai/projects/dispatch-modernization/artifacts/data-classification
specira	[5] Integration inventory: INT-1...INT-6 the flows resolve to app.specira.ai/projects/dispatch-modernization/artifacts/integration-inventory
specira	[6] Event-driven architecture: the override.recorded seam app.specira.ai/projects/dispatch-modernization/artifacts/event-driven-architecture#catalog
specira	[7] Threat model: TM-01, TM-04, TM-05, TM-06; crossing coverage app.specira.ai/projects/dispatch-modernization/artifacts/threat-model

specira [8] Security requirements: SR-021 app.specira.ai/projects/dispatch-modernization/artifacts/security-requirements#sr-021

specira [9] Business rules: VR-01 bounds validation app.specira.ai/projects/dispatch-modernization/artifacts/business-rules#validation

specira [10] Observability: the logging content law app.specira.ai/projects/dispatch-modernization/artifacts/observability-monitoring#logging

Generated by Specira · template data_flow_diagrams v2 (draft) · pack specira_default_delivery lineage 7d53ed67...9ad6 · page 1 of 5

SAMPLE
seeded demo data · specira.ai