

GOVERNED TEMPLATE RENDERING REFERENCE: SECURITY REQUIREMENTS DEFAULT V2 (DRAFT)

definition 33b30d03...dfb7

SECURITY REQUIREMENTS · PROJECT ARTIFACT

SPECIRA

Security Requirements: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template security_requirements v2 · pack: specira_default_delivery
depth: standard · tier: elevated (L2)

§1 Scope, Drivers & Assurance Tier

mandatory 1 decision 1 evidence rule

validators: assurance_tier_declared_with_trigger_values · conditional_sections_match_trigger_signals

What is protected, what demands it, and the assurance level the trigger signals select. Scaling down is recorded with trigger values; silence is never a tier.

In scope: the dispatch board, API, recommendation module, telematics adapter, notification worker, and the data they carry (architecture^[1]). Out of scope: payroll and job pricing; their systems of record, unchanged.

Trigger	Value	Evidence	Effect
Personal data	true	Technician location (data flow ^[1])	L2 baseline · classification engaged
Enterprise contracts	true	Clauses 12 to 14 (contracts ^[5])	Traceability engaged
AI features	true	Recommendation module	§4 engaged
Payments	false	n/a	PCI family omitted

Trigger	Value	Evidence	Effect
Health data	false	n/a	HIPAA family omitted

DECISION: TIER ELEVATED (L2)

Agreed with E. Sandoval, July 13, 2026. Abuse-derived rows engaged (insider misuse of overrides); payment and health families omitted, triggers false, recorded here.

§2 Security Requirements Register

mandatory2 decisions1 evidence rule

validators: every_row_has_driver_citation · statements_free_of_subjective_terms · verification_method_from_closed_enum

The artifact's core. Per row: a stable id, one verifiable "shall" statement, the driver cited (threat id, regulation, or contract clause, never restated), the verification method from the closed set, an owner role, and a status. A row missing a field is a slogan.

Id	Statement	Driver	Verification	Owner	Status
SR-001	Dispatcher and manager accounts shall authenticate through Meridian SSO with multi-factor enabled by default	contract12.3[5]	configuration	eng lead	implemented
SR-004	The board shall deny assignment actions to read-only roles server-side, not interface-only	TM-03insidermisuse[2]	dynamic test + code review	eng lead	verified: US-1 row AT-5[3]
SR-006	Job intake shall reject any skill value outside the governed taxonomy, naming the offending value and logging the rejection	TM-02malformedintake[2]; realized by ERR-02/03[4]	dynamic test	eng lead	verified
SR-009	Every override shall be logged with dispatcher id, reason code, and timestamp, retained seven years	union agreement 8 · contract14[5]	dynamic test	eng lead	implemented

Id	Statement	Driver	Verification	Owner	Status
SR-011	Dispatcher sessions shall expire after 12 idle hours and require re-authentication on hub change	contract 12.3^[5]	config + dynamic test	eng lead	implemented
SR-018	ABUSE-DERIVED The board shall alert the operations manager when one dispatcher's override rate exceeds three times the hub median over a rolling week	TM-03 insider misuse^[2]	dynamic test, seeded data	eng lead	approved
SR-021	Telematics webhook signatures shall be verified on every request; signing tokens rotate quarterly	TM-01 spoofed feed^[2]	configuration + dynamic test	fleet (S. Grewal)	implemented: INT-1^[1]
SR-027	Secrets shall live in the managed vault (none in code or configuration files) and rotate on role change	baseline (MVSP 2.7)	static analysis + config audit	eng lead	verified
SR-030	Security-event logging shall ship enabled by default; no opt-in security	baseline (secure defaults)	configuration	eng lead	implemented
SR-031	Override audit entries shall be append-only; no interface or role may edit or delete them inside the retention window	union agreement 8	code review + dynamic test	eng lead	implemented
Category coverage		Rows			
Secure defaults		SR-001 · SR-030			

Category coverage	Rows
Access enforcement	SR-004
Input handling	SR-006
Session management	SR-011
Cryptography & residency	SR-033 · SR-034 (§3)
Secrets	SR-027
Logging & audit	SR-009 · SR-030 · SR-031
Abuse-derived	SR-018
Output encoding	Not applicable, with rationale: the board renders no untrusted markup

EVIDENCE: NO ORPHANS, NO WAIVERS, NO SILENT CATEGORIES

Every row's driver resolves to its threat, clause, or named baseline; every engaged category is represented or named not-applicable with rationale; waivers: none open. Legacy "threat landscape" prose does not exist here; threats live in the [threat model](#)^[2] and appear only as driver citations.

§3 Data Protection & Classification

mandatory

1 decision

1 evidence rule

validators: data_classes_map_to_protection_rows · retention_residency_reconcile_with_architecture

Data class	Held by	Protection rows
Technician location: personal, restricted	Adapter, API cache	SR-033 encrypted in transit and at rest, stays in Canada, per PIPEDA + clause 13 ^[5]
Assignment history: confidential	Event log	SR-034 archive at 7 years; positions purge at 30 days, matching the architecture lifecycle (cited ^[1])
Reason codes: internal	API	baseline rows

Payment and health families omitted; triggers false, recorded in §1.

§4 AI & Model-Provider Security

conditional · engaged: AI trigger true

1 decision

1 evidence rule

validators: ai_section_present_when_ai_signal_true · provider_commitments_cite_agreement_clauses

Id	Statement	Driver	Status
SR-014	Model calls shall route through the provider gateway; no location or personal data crosses; ranking inputs are anonymized codes	<u>TM-04^[2]</u> · <u>ADR-5^[1]</u>	verified
SR-015	The provider agreement shall confirm both zero-data-retention AND no-training: distinct promises, each cited	<u>agreement 4.2^[6]</u>	approved
SR-016	Suggestion outputs shall be constrained to the qualified-technician set the system supplied; a model cannot name a technician it was not offered	<u>FR-013^[4]</u>	implemented

§5 Supply Chain Security

mandatory

1 decision

1 evidence rule

validator: supply_chain_target_is_named_standard_level

SR-040 : the build pipeline shall meet **SLSA level 2** by cutover: signed provenance on every artifact; owned by the engineering lead; target October 1, 2026. **SR-041** : the software inventory stays current with license and provenance per component, reconciled with the sourcing register (architecture §6^[1]; SBOM-041). **SR-042** : dependencies pinned; critical vulnerabilities patched within 14 days, highs within 30; verification by dependency-scan evidence.

§6 Security Testing Gates

mandatory

1 decision

1 evidence rule

validator: testing_gates_carry_numeric_exit_criteria

Gate	Cadence / trigger	Exit criteria	Owner
Static analysis	every merge	zero high severity open	feature team
Dependency scan	weekly	zero criticals at release	eng lead

Gate	Cadence / trigger	Exit criteria	Owner
Dynamic scan	pilot env, per release	highs dispositioned before deploy	K. Yamada
Penetration test	before Oct 1 cutover	zero open critical/high; mediums dispositioned with owners (report attached^[7])	N. Duval

Execution (environments, tooling, scheduling) lives in the [test strategy^{\[8\]}](#), referenced not restated.

§7 Incident Response: Project Deltas

mandatory

1 decision

1 evidence rule

validator: ir_deltas_only_no_org_procedure_text

Deltas only; the organizational plan governs execution ([runbook^{\[9\]}](#)). **Severity:** suspected exposure of technician location data is P1. **Notification:** affected enterprise customers within 72 hours per [contract clause 14^{\[5\]}](#); PIPEDA breach assessment by the privacy owner. Owner: N. Duval (legal and operations).

§8 Compliance Traceability

conditional · engaged: regulated data + enterprise contracts

1 decision

1 evidence rule

validator: traceability_resolves_both_ways

Clause / obligation	Requirement rows
PIPEDA safeguarding	SR-033 · SR-034
Enterprise contract 12.3 (authentication)	SR-001
Enterprise contract 13 (residency)	SR-033
Enterprise contract 14 (audit + notification)	SR-009 · §7 delta
Union agreement 8 (override logging)	SR-009

Reverse check: every driver named in the register appears here; payment and health families excluded with trigger values recorded in §1. Deferred: none.

§9 Open Questions

mandatory

1 decision

Question	Owner	Answer by	Blocks
Does the union agreement require a consent notice to dispatchers on override logging?	N. Duval	Aug 8, 2026	SR-009 wording only, not its implementation

Omission note (how §4 renders without AI scope): "§4 AI & Model-Provider Security omitted: AI-features trigger false. Rationale recorded in adaptation event #1."

Refs

References & Package Contents

In this export package

- package [5] Enterprise contract extracts: clauses 12 to 14 ./contracts/enterprise-clauses.docx
- package [6] Model-provider agreement: data-handling clause 4.2 ./contracts/provider-agreement-4-2.docx
- package [7] Penetration test report (at cutover; placeholder until run) ./security/pentest-cutover.html
- package [9] Operations runbook: incident execution ./operations-runbook.html

In the Specira workspace

- specira [1] Architecture: data flow, INT-1, sourcing, ADR-5 app.specira.ai/projects/dispatch-modernization/artifacts/architecture
- specira [2] Threat model: TM-01..TM-06 (STRIDE analysis lives there) app.specira.ai/projects/dispatch-modernization/artifacts/threat-model
- specira [3] Story set: US-1 row AT-5 (permission denial instance) app.specira.ai/projects/dispatch-modernization/artifacts/user-stories
- specira [4] Functional spec: FR-013 app.specira.ai/projects/dispatch-modernization/artifacts/frd-recommendation-rules
- specira [8] Test strategy: CI gates and execution app.specira.ai/projects/dispatch-modernization/artifacts/test-strategy