GOVERNED TEMPLATE RENDERING REFERENCE: AUTH & AUTHORIZATION POLICY DEFAULT V2 (DRAFT)

definition 80d8a009…0bf9

AUTH & AUTHORIZATION POLICY · PROJECT ARTIFACT

SPECIRA

Auth & Authorization Policy: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template auth_authz_policy v2 · pack: specira_default_delivery

assurance anchors to classification; the handshake is the artifact

§1 Assurance Levels

mandatory | 1 decision | 1 evidence rule

validators: assurance_level_cites_classification_register · assurance_anchor_table_present_with_numeric_ceilings

How sure must we be it's really them: a decision anchored to the highest data classification a session touches, never a default. The anchor table IS the decision artifact.

Decision: elevated assurance (two factors, phishing-resistant option) for every staff role. Sessions touch Restricted data, technician location (classification labels[1]). Agreed: E. Sandoval with N. Duval, July 15, 2026; resolves SR-001[2]'s posture statement.

Highest class touched	Assurance taken	Ceiling inherited
Public / Internal only	baseline (single factor)	re-auth ≤ 30 days
Confidential	elevated (two factors)	idle ≤ 1 h · absolute ≤ 24 h
Restricted ← this project	**elevated, hardware-bound offered**	policy pair in §6, within ceiling
future payroll scope (none today)	high (hardware-bound required)	idle ≤ 15 min · absolute ≤ 12 h

Federation trust: Meridian SSO is the IdP (sourcing · internal reuse[3]); assertion protection at the protected level (signed, audience-bound). **Step-up**: none at pilot (no action class exceeds the session floor); *recorded so the absence is a decision*.

§2 Authentication Strategy

mandatory · 1 decision · 1 evidence rule

validators: credential_rules_numeric_no_rotation_theater · recovery_paths_specified

Factors, credential rules as numbers, and the recovery path; recovery is an attack surface, so "contact support" is not a design.

Rule	Value
Staff factors	SSO password + platform authenticator; passkey (phishing-resistant) offered to all, **required** for the operations-manager role
Password minimum	`14 characters, breach-list screened`
Rotation	**none periodic** (rotation theater retired; reset on compromise signals only)
Lockout	`10 failures → 15-minute cool-off`
Recovery	Meridian identity desk with manager confirmation; never self-serve email reset for staff accounts
Adaptive	New-device sign-in requires the second factor even inside a valid SSO session

§3 Identity Model

mandatory · 1 decision · 1 evidence rule

validators: lifecycle_states_have_actors · every_leaver_trigger_has_owner_and_sla

Where identities live and every lifecycle transition with its actor; the leaver path is where most real-world access debt accrues.

Source: federated. Meridian SSO is authoritative for staff; no native accounts.

State	Entered by	Actor / owner
`invited`	Directory group membership	Identity team
`active`	First SSO sign-in	n/a
`suspended`	Directory suspension	Identity team

State	Entered by	Actor / owner
`deprovisioned`	Directory removal	Identity team

Leaver path: directory-sync deprovisioning within **4 business hours** of HR termination (owner: identity team); dispatch-role removal propagates to session revocation **immediately** (owner: engineering lead). Just-in-time creation exists for first sign-in but **never stands in for the leaver signal**; the sync is the signal.

§4 Permission Model

mandatory · 1 decision · 1 evidence rule

validators: permission_model_decision_has_what_why_who_how · no_wildcard_admin_cell_in_matrix · scoping_rules_server_enforceable

The model is a decision with alternatives evaluated, then the matrix, explicit cells only. Admin earns rows like everyone else.

> Decision · role-based with a hub-scope attribute
> **What**: RBAC (role → permission), ReBAC (relationship graph), ABAC (predicate rules). **Why considered**: the entity graph is shallow and sharing is role-shaped, not object-shaped. No user-driven "share this job" exists; the one cross-cutting rule (a dispatcher acts within her hub) is a single scope attribute, not a rule engine's worth. **Who**: E. Sandoval with A. Reyes. **How & when**: walked against the data model's five entities and the four screens, July 15. **Findings**: ReBAC rejected (no per-object sharing to model; engine dependency unjustified); pure ABAC rejected (one attribute does not need a policy engine); RBAC-with-scope wins on explainability and audit ease (rights-model decision[4]).

Role	Jobs	Assignments	Overrides
Dispatcher	`read/write · hub`	`create · hub`	`create, with rea`
Operations manager	`read`	`read`	`read + exception`
Technician	`none`	`own · read + confirmations write`	`none`
Fleet manager	`none`	`none`	`none`
Platform admin	`read-only`	`read-only`	`read-only`

Enforcement: read-only means the server denies writes, not that the button is hidden (SR-004[2]). **Scoping**: hub scope on every dispatcher grant, ownership scope on technician

reads; both server-enforced.

§5 Machine Identity

conditional · service-to-service paths exist, ENGAGED | 1 decision | 1 evidence rule

validators: machine_identities_enumerated_or_explicitly_absent · machine_rotation_rules_are_periods

Humans are half the identity story; every service-to-service path from the integration register gets an identity, a rotation period, and a blast radius.

Path (from the integration register)	Identity & secret	Rotation	Blast radius
Telematics webhook ingress	Vendor-signed tokens (SR-021[2])	`quarterly`	Position poisoning, bounded by the adapter seam
Adapter & notification worker	Platform service accounts, short-lived runtime tokens, no static secrets	`per-token TTL`	Internal queue only
Notification gateway	Vendor API key in the managed vault (SR-027[2])	`quarterly + on role change`	Message delivery only
Model-provider gateway	Provider key in the vault; gateway-only egress (SR-014[2])	`quarterly`	Anonymized codes only cross (PB-2[3])

§6 Session Management

mandatory | 1 decision | 1 evidence rule

validators: session_timeouts_numeric_within_aal_ceiling · revocation_on_role_change_immediate

Both ceilings, numeric, inside the assurance level's ceiling, plus every way a session ends besides time.

Rule	Value
Idle	`60 minutes → soft lock, SSO re-authentication`

Rule	Value
Absolute	`12 hours (the shift length) → full sign-out`
Sign-out / credential reset	Immediate termination
Role change	Revocation immediate; propagated to active sessions within 60 s
Hub transfer	Re-authentication required
Concurrent	One board session per dispatcher account; the day view allows one mobile session alongside

Refines: the posture statement SR-011[2]: this pair is the precise form of its "12 idle hours" wording; the requirement's restatement is queued for its next regeneration (§10).

§7 SSO Integration

conditional · enterprise IdP in play, ENGAGED | 1 decision | 1 evidence rule

validators: sso_flows_named_exactly_deprecated_forbidden · mapping_rows_resolve_to_matrix_roles

The protocol named exactly, deprecated flows forbidden by name, and the directory mapping, every row resolving to a §4 matrix role.

Protocol: the authorization-code flow with proof-of-code-exchange; exact-match redirect URIs; **implicit and password flows forbidden by name**.

Directory group	→ Matrix role (§4)
`dispatch-toronto`	Dispatcher, hub scope = Toronto
`ops-managers`	Operations manager
`field-techs`	Technician
`fleet`	Fleet manager

Deprovisioning: the 4-business-hour SLA. The identity team owns the sync, the engineering lead owns in-app revocation; verified quarterly against the HR leaver list.

§8 Break-Glass Access

conditional · production incident path exists, ENGAGED | 1 decision | 1 evidence rule

validators: break_glass_requires_dual_approval_and_audit · break_glass_timebox_is_numeric

Emergency access designed in daylight: dual approval, a numeric time-box, and audit before access flows.

Rule	Value
Requester	The on-call engineer
Approval	**Dual**: engineering lead AND N. Duval (or named alternates)
Grants	Read access to production diagnostics + the feature-flag console; **never job or assignment writes**
Time-box	`4 hours, auto-expiry`
Audit	Who, when, what, why, written to the append-only audit **before access flows** (SR-031[2])
Review	Post-use, at the next weekly sync

§9 Auth Audit Events

mandatory · 1 decision · 1 evidence rule

validators: audit_event_set_closed_with_required_fields · event_retention_cites_classification_rule

A closed event set with required fields; "we log authentication stuff" is not auditable.

Events: sign-in · sign-out · failed authentication · factor enrollment and reset · role or scope change · session revocation · break-glass activation and expiry. **Required fields, every event**: timestamp, actor, target, outcome, source.

Resolution: the security requirements' logging rows resolve here (SR-030, SR-009[2]); retention follows the classification register's audit-record rule (retention[1]).

§10 Open Questions

mandatory · 1 decision

Question	Owner	Answer by	Blocks
Reconcile the SR-011 wording ("12 idle hours") with this policy's precise pair (60-min idle lock / 12-h absolute) at the requirements register's next regeneration	E. Sandoval	`Aug 8, 2026`	Nothing at runtime; the policy is authoritative

Question	Owner	Answer by	Blocks
Passkey requirement for dispatchers (beyond operations managers)	N. Duval, with the union briefing	Aug 22, 2026	§2's factor table only

Refs References & Package Contents

In the Specira workspace

specira	[1] Data classification: labels (assurance anchor), audit-record retention rule app.specira.ai/projects/dispatch-modernization/artifacts/data-classification
specira	[2] Security requirements: SR-001, SR-004, SR-009, SR-011, SR-014, SR-021, SR-027, SR-030, SR-031 app.specira.ai/projects/dispatch-modernization/artifacts/security-requirements
specira	[3] Architecture: sourcing (internal reuse: Meridian SSO), integration register, PB-2 app.specira.ai/projects/dispatch-modernization/artifacts/architecture
specira	[4] Decision log: rights-model decision (RBAC with hub scope) app.specira.ai/projects/dispatch-modernization/decisions/rights-model