# 5Tech Platform — User Guide

**User Guide** · `sensorium-platform-manual` · **Revision Draft (Preliminary, PROPOSED) · 2026-07-18 · Status: Preliminary**

> **PRELIMINARY — PROPOSED VALUES.** This guide describes intended functionality of the 5Tech Platform. Values marked ‡ are proposed, industry-typical figures (security suites, retention periods, SLA targets, browser versions, cadences) supplied so no item is left blank. They are **not final and not contractual**; they are confirmed as part of deployment and may change. Exact screen labels, navigation, and role names are subject to change. A remaining `[TBD]` marks a legal/contractual term (warranty/license) that must not be invented. See §13 for service terms.

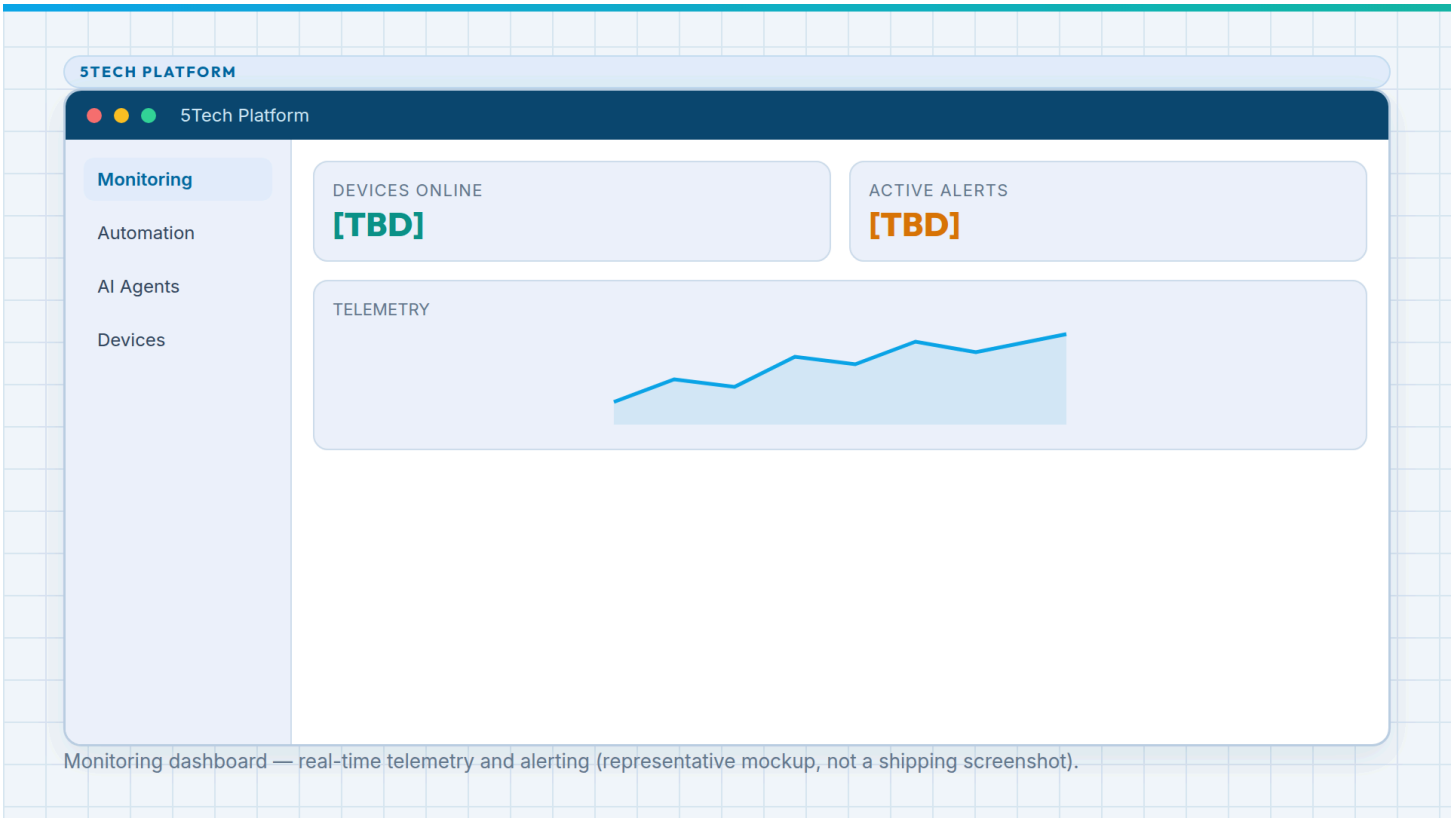


*Figure FIG-001 — The 5Tech Platform monitoring dashboard: live telemetry, KPIs, and active alerts.*

# 1. Overview & concepts

### 1.1 What the 5Tech Platform is

The **5Tech Platform** is the software — the *Decide* — layer of the 5Tech ecosystem. It turns field data into monitoring, alerts, and human-in-the-loop action. 5Tech's purpose is to *"bridge the gap between complex physical operations and digital intelligence,"* with the auditability that industrial enterprises require. The Platform is where that data is made useful.

It receives telemetry from the **Sensorium™ Gateway** — the *Connect* layer that aggregates field devices such as Zone Awareness sensors and SmartBolt modules over BLE and publishes it over MQTT — and presents it through three working layers: **Monitoring**, **Automation**, and **AI Assistance**. It can integrate with your existing **SCADA** and **ERP** systems so that the decisions people make can drive real operational actions.

### 1.2 The three layers


*Figure FIG-002 — Monitoring, Automation, and AI Assistance layers, fed by the Sensorium™ Gateway and integrated with SCADA and ERP.*

| LAYER | SUBTITLE | WHAT IT DOES | WHERE IN THIS GUIDE |
|---|---|---|---|
| **Monitoring** | Dashboards & alerts | Real-time telemetry visualization and alerting | §5 |
| **Automation** | Workflows & integrations | Rule-based logic: trigger ERP actions, sync devices, integrate across systems | §6 |
| **AI Assistance** | AI-assisted helpers | Triage, Compliance, Reporting, and Summary helpers — they suggest, flag, and report; a person decides | §7 |

The four AI-assisted helpers — **Triage**, **Compliance**, **Reporting**, and **Summary** — sit inside the AI Assistance layer and are introduced in §7. They are decision-support only: none of them takes autonomous action or enforces policy.

### 1.3 Where the Platform sits in the ecosystem

The 5Tech ecosystem follows a **Sense** → **Connect** → **Decide** chain:

1. **Sense** — Sensorium™ field devices (Zone Awareness, SmartBolt) detect conditions in the field.
2. **Connect** — the Sensorium™ Gateway aggregates and pre-processes their data and uplinks it over MQTT.
3. **Decide** — the **5Tech Platform** (this product) turns that data into monitoring, automation, and AI-assisted recommendations that people act on, which can flow out to SCADA/ERP and back to devices.

Packaged **Solutions** — Fleet Management and Construction Sites Monitoring — are built on this chain and use the Platform as their software layer.

### 1.4 Key concepts and terms

| TERM | MEANING IN THIS GUIDE |
|---|---|
| **Site** | A physical location or asset grouping whose devices report to the Platform. |
| **Device** | A field unit whose data reaches the Platform via the Sensorium™ Gateway. |
| **Telemetry** | The stream of measurements a device reports (values over time). |
| **Event** | A discrete occurrence derived from telemetry (e.g. a threshold crossing). |
| **Alert** | An event surfaced to operators for attention, carrying a severity. |
| **Workflow** | An automation rule: a trigger, optional conditions, and one or more actions. |
| **Integration** | A connection between the Platform and an external system (SCADA, ERP). |
| **AI-assisted helper** | An AI-assisted function (Triage, Compliance, Reporting, or Summary) that suggests, flags, or reports — a person decides. |
| **Policy** | The configurable rules and thresholds that govern how a helper behaves. |
| **Action** | The output of a workflow, or a person acting on a helper's suggestion (notify, trigger ERP action, sync a device). |
| **Audit log** | The Platform's deterministic, tamper-evident system-of-record (§8) — distinct from the AI Reporting helper. |

## 2. About this guide

- **Audience.** Operators, supervisors, and administrators who use the 5Tech Platform. No coding is assumed; administration tasks assume the appropriate access level (§4).
- **Scope.** Day-to-day use of Monitoring, Automation, and AI Assistance, plus access control, auditability, administration, maintenance, security, troubleshooting, and support. Deployment, commissioning, and integration engineering are delivered as 5Tech services (§13.2) and are out of scope here.
- **Conventions.** Numbered lists are procedures — perform one step at a time, in order. ‡ marks a proposed, industry-typical value supplied so the guide carries no blank; it is not final or contractual and is confirmed at deployment. `[TBD]` marks a legal/contractual term that must not be invented. Figures are referenced as *Figure FIG-00N*.
- **Related documents.** See §13.4.

## 3. Safety & operating limits

This is a **software product**: it has no physical hazards and uses no hazard symbols. This short chapter states the operating limits you must understand before relying on the Platform. Access, roles, security, and data handling are covered in §4, §8, and §11.

### 3.1 Not a safety-rated protective system

> **NOTICE — Decision-support only, not a safety system.** The 5Tech Platform's monitoring, alerts, and AI-assisted helpers are **decision-support tools, not a safety-rated protective system**. They do **not** replace machine safeguarding, emergency-stop circuits, interlocks, or a safety-instrumented system (SIS), and must **not** be the sole means of protecting personnel or equipment. This is consistent with the field devices, which are not safety controllers. Continued protection does not depend on the Platform, its network path, or its availability.

### 3.2 Human-in-the-loop principle

The Platform is built so that a **person decides**. The AI-assisted helpers (§7) analyze data to **suggest, flag, and report** — they never take autonomous action or enforce policy on their own. Automation workflows (§6) execute only the rules a person has configured and enabled, and act on live systems (including SCADA/ERP), so they are tested before being relied on. Alerts require human acknowledgement (§5.2); acknowledging an alert does not by itself clear the underlying condition.

---

## 4. Access, roles & permissions

Access to the Platform is governed by **role-based access control (RBAC)**: what you can see and do depends on the role your administrator assigns and the sites you are scoped to.

### 4.1 Signing in

1. Open a supported web browser (supported browsers and minimum versions: §11.5).
2. Navigate to your organization's Platform URL (provided by your 5Tech administrator).

3. Sign in with your organization credentials. Authentication is by **single sign-on (SSO via SAML 2.0 / OIDC)‡** with **multi-factor authentication (MFA)‡** where enabled (§11.3).
4. Verify that the correct **site** is selected in the top bar before you begin.

If sign-in fails, see §12 (Troubleshooting) and §13 (Support).

### 4.2 Roles & permissions — the RBAC matrix

The Platform enforces the **definitive** role model below. Every account is assigned exactly one role and is scoped to one or more sites; the role determines the permissions, and the scope determines which sites those permissions apply to. Administrators can scope any role to specific sites.

| PERMISSION | VIEWER | OPERATOR | SUPERVISOR | ADMINISTRATOR |
|---|---|---|---|---|
| View dashboards & telemetry | ✓ | ✓ | ✓ | ✓ |
| View reports & summaries | ✓ | ✓ | ✓ | ✓ |
| Acknowledge alerts | — | ✓ | ✓ | ✓ |
| Create / edit / enable workflows | — | ✓ | ✓ | ✓ |
| Configure AI-helper policies (Triage · Compliance · Reporting · Summary) | — | — | ✓ | ✓ |
| View the audit log (§8) | — | — | ✓ | ✓ |
| Export data (telemetry / reports / audit) | — | — | ✓ | ✓ |
| Manage integrations (SCADA / ERP) | — | — | — | ✓ |
| Manage users & roles | — | — | — | ✓ |
| Manage security, retention & deployment settings | — | — | — | ✓ |

> **NOTICE.** Changes to workflows and AI-helper policies affect live operations. Only accounts with the appropriate role should make them, changes should be reviewed before enabling, and every change is recorded in the audit log (§8).

---

# 5. Monitoring — dashboards & alerts

The Monitoring layer provides **real-time telemetry visualization and alerting**. The monitoring dashboard is shown in *Figure FIG-001* (this guide's cover).

### 5.1 Reading the monitoring dashboard

The dashboard presents your selected site's live state — key indicators, telemetry charts, and a panel of active alerts. Exact cards, layout, and labels are preliminary.

**To open a dashboard**

1. Sign in and confirm the correct site is selected (§4.1).
2. Open the **Monitoring** workspace from the navigation rail.
3. Select the dashboard for the site or asset you want to view.
4. Confirm the data is live — the freshness / last-updated indicator should be current.

### 5.2 Working with alerts

Alerts surface events that need attention, ranked by **severity** (higher severities are more urgent).

**To acknowledge an alert**

1. In the **Monitoring** workspace, open the **Active alerts** panel.
2. Select the alert to view its detail (source device, time, severity, related telemetry).
3. Take any required operational action first; then select **Acknowledge**.
4. Verify the alert moves out of the active list and is recorded in history.

> **NOTICE.** Acknowledging an alert records that it was seen and handled (and is written to the audit log, §8); it does not by itself resolve the underlying condition. Confirm the condition has cleared in the telemetry.

### 5.3 Relationship to the AI-assisted helpers

The **Triage** helper (§7.1) can prioritize incoming events so the most critical alerts rise to the top of the Active alerts panel. What you see in Monitoring is therefore shaped by the Triage policy — if alert prioritization looks wrong, review the Triage settings with an administrator.

# 6. Automation — workflows & integrations

The Automation layer is the **logic layer**. It lets you trigger ERP actions, sync devices, and integrate across systems without writing code — by building **workflows**.

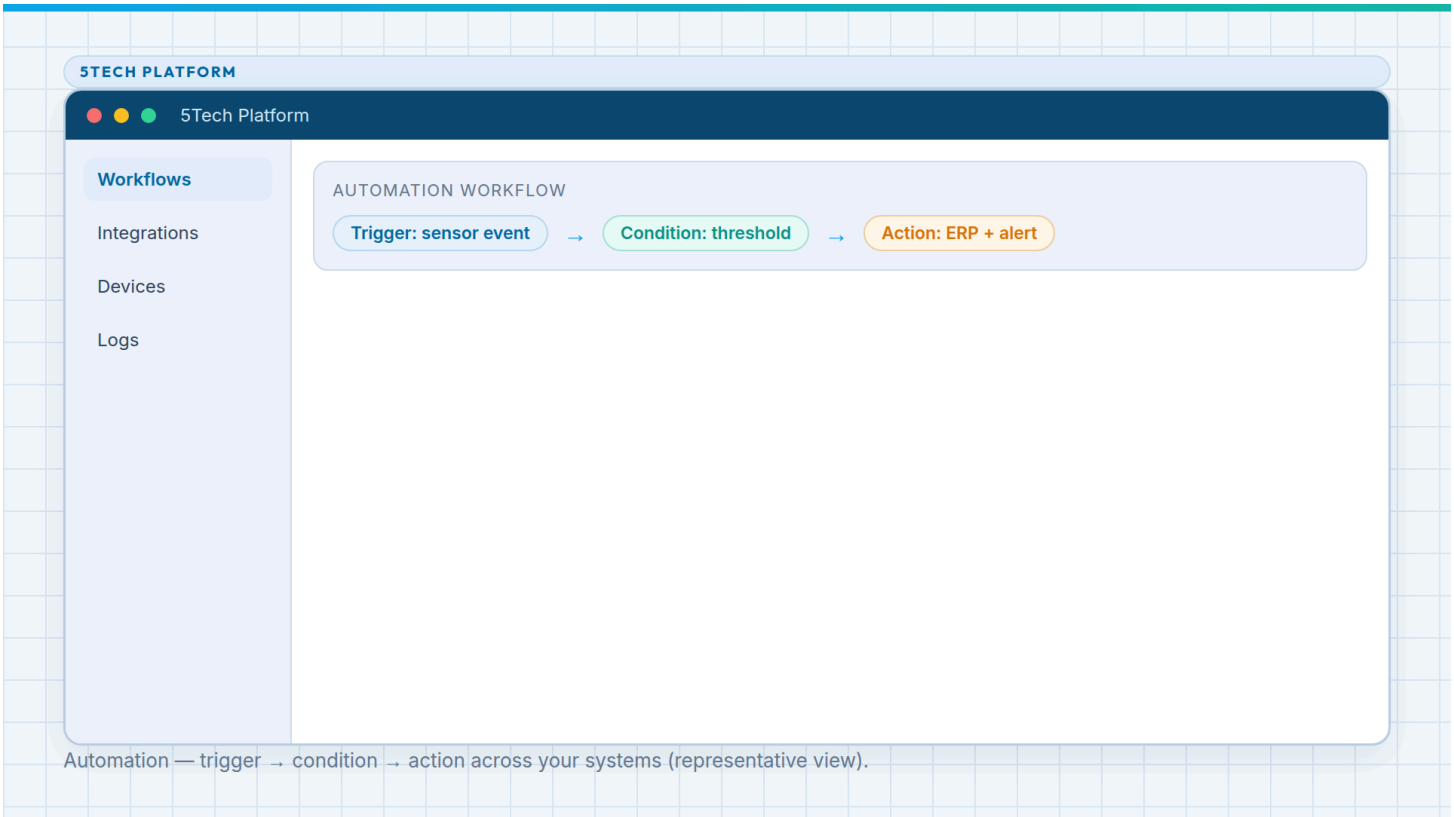


*Figure FIG-005 — The automation workflow builder: a trigger, conditions, and actions wired into a rule.*

### 6.1 Anatomy of a workflow

A workflow has three parts:

- **Trigger** — what starts it (for example, an alert or a sensor event).
- **Condition(s)** — optional tests that must be true for the workflow to continue.
- **Action(s)** — what it does: notify an operator, trigger an ERP action, sync a device, or call another integrated system.

*Figure FIG-005* shows these wired together on the builder canvas.

### 6.2 Creating a workflow

**To create a workflow**

1. Open the **Automation** workspace from the navigation rail (requires Operator role or higher — see §4.2).
2. Create a new workflow and give it a clear, descriptive name.

3. Add a **Trigger** block and choose the event that should start the workflow.
4. Add any **Condition** blocks needed to scope when the workflow runs.
5. Add one or more **Action** blocks (notify, ERP action, device sync, integration call).
6. Review the wired workflow end to end for correctness.
7. Save the workflow. It remains inactive until you enable it in the next step.

**To enable a workflow**

1. Open the saved workflow.
2. Confirm the trigger, conditions, and actions are correct.
3. Toggle the workflow to **Enabled**.
4. Verify it appears as active and, where possible, test it with a controlled trigger before relying on it in production.

> **NOTICE.** Enabled workflows act on live systems, including SCADA/ERP actions. Test in a controlled way before enabling in production, and change one workflow at a time. Enable/disable and edit events are recorded in the audit log (§8).

### 6.3 Integrations (SCADA & ERP)

The Platform integrates with existing **SCADA** and **ERP** systems so workflows can read context from — and push actions to — the systems you already run. Establishing an integration (endpoints, credentials, field mapping) is part of deployment and is delivered as a 5Tech service (§13.2).

Once an integration exists, reference it from a workflow's **Action** block (§6.2) — for example, "create an ERP work order" or "sync a device setting."

---

## 7. AI Assistance — configuring the AI-assisted helpers

The AI Assistance layer provides **AI-assisted helpers** that **analyze data to suggest, flag, and report**. They are **human-in-the-loop**: a helper never takes autonomous action or enforces policy on its own — a person reviews its output and decides. Four helpers are available.

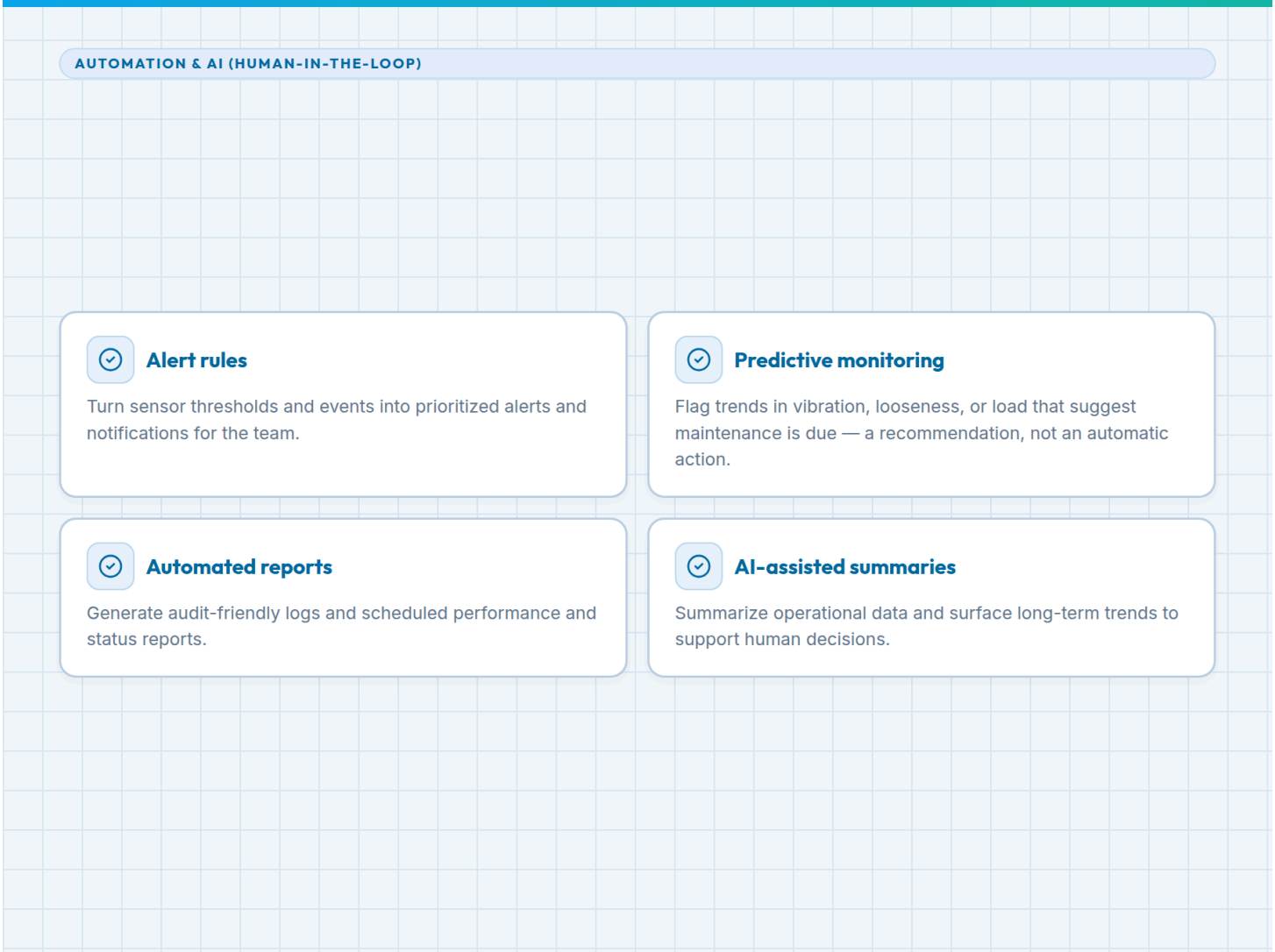


*Figure FIG-003 — The four AI-assisted helpers — Triage, Compliance, Reporting, and Summary — and what each suggests, flags, or reports. A person decides.*

| HELPER | WHAT IT DOES |
|---|---|
| **Triage** | Prioritizes and routes critical events for operator attention |
| **Compliance** | Flags policy, safety, and threshold/trend issues **for human review only** |
| **Reporting** | Produces human-readable briefings and scheduled reports (not the audit log — see §8) |
| **Summary** | Gives supervisors operational oversight and long-term trends |

Each helper is governed by a **policy** — the rules and thresholds you configure. Helpers only suggest, flag, and report; people decide and act. Configuring helper policies requires Supervisor role or higher (§4.2), and every policy change is recorded in the audit log (§8).

### 7.1 Triage — prioritizing critical events

Triage helps surface which events matter most, so operators see the most critical alerts first (§5.3). It suggests a priority; operators still review and acknowledge each alert.

**To configure Triage**

1. Open the **AI Assistance** workspace and select **Triage** (requires Supervisor role or higher, §4.2).
2. Review the current prioritization rules and thresholds.
3. Adjust how event severity and priority are determined for your site.
4. Save the settings; the change and its effective version are recorded in the audit log (§8).
5. Verify the change in **Monitoring** — confirm alerts are ordered as intended.

### 7.2 Compliance — flagging policy & safety issues for review

Compliance watches telemetry and configuration against your policy, safety, and threshold rules and **flags conditions for human review only** — for example, a reading drifting toward a threshold, or an operating condition that departs from policy. It **flags and suggests; it does not gate, stop, block, or enforce anything**, and it makes no compliance determination — a person reviews each flag and decides.

**To configure Compliance**

1. Open the **AI Assistance** workspace and select **Compliance** (Supervisor role or higher).
2. Review the policy, safety, and threshold conditions it watches.
3. Update thresholds and conditions to match your operating and policy requirements.
4. Save the settings; the change and its effective version are recorded in the audit log (§8).
5. Validate with a controlled scenario before relying on its flags in production.

> **NOTICE.** Compliance only raises flags for human review; it does not act on its own and does not certify compliance. Review changes with the responsible owner before enabling them on a live site.

### 7.3 Reporting — briefings & scheduled reports

Reporting produces the human-readable briefings and scheduled reports that make the Platform's activity easy to review — for example a daily operations briefing or a periodic status report.

> **NOTICE.** Reporting is an AI-assisted helper that **generates readable summaries from data**. It is **not** the Platform's authoritative record: the deterministic, tamper-evident **audit log (§8)** is the system-of-record, and it exists independently of this helper.

**To configure Reporting**

1. Open the **AI Assistance** workspace and select **Reporting** (Supervisor role or higher).
2. Choose which briefings/reports are produced and their schedule (e.g. daily).
3. Set the recipients or destinations for briefings and report exports.
4. Save. Confirm the reports you require are being produced. The configuration change is recorded in the audit log (§8).

### 7.4 Summary — operational oversight & trends

Summary gives supervisors a higher-level, plain-language view of operations and trends over time.

**To use Summary**

1. Open the **AI Assistance** workspace and select **Summary**.
2. Choose the site(s) and time range for the overview.
3. Review the highlighted trends and operational-oversight indicators.
4. Follow any trend of concern back into **Monitoring** (§5) for the underlying telemetry.

### 7.5 The event-to-action loop

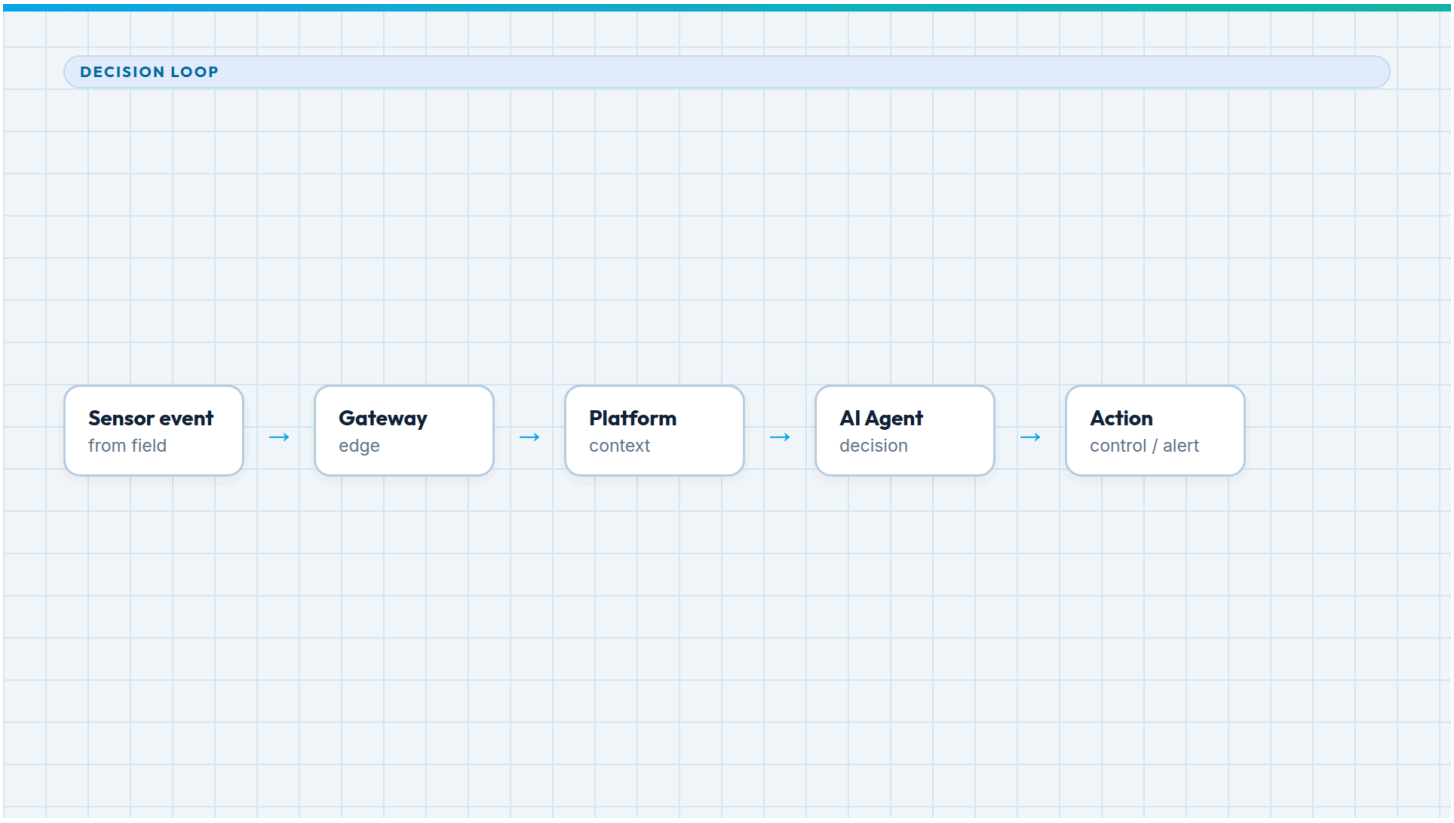


*Figure FIG-004 — The event-to-action loop: a sensor event is prioritized and checked against policy by the helpers, which present a suggestion; a person reviews it and decides on the action.*

The helpers assist a loop from field to action that a **person** closes, as shown in *Figure FIG-004*:

1. A **sensor event** arrives from the field via the Sensorium™ Gateway.
2. The **AI-assisted helpers** analyze it — prioritizing it (Triage) and flagging any policy or trend concern (Compliance) — and present a suggestion to an operator.
3. After a person reviews it and decides, an **action** results — an operator alert, an automation workflow (§6), or a SCADA/ERP action.
4. Outcomes feed back as new telemetry; Reporting and Summary keep the activity reviewable, and the audit log (§8) keeps it verifiable.

---

## 8. Auditability & system of record

Auditability is a **core function of the Platform**, delivered by a **deterministic, tamper-evident audit log** — the authoritative system-of-record for who did what and when. It is **separate from the AI "Reporting" helper (§7.3)**: Reporting generates human-readable briefings from data, whereas the audit log is a fixed, machine-verifiable record that does not depend on any AI function.

### 8.1 What the audit log is

- **Deterministic and append-only.** Entries are written once and never edited; the log cannot be altered or deleted by any user, **including administrators**.
- **Tamper-evident.** Entries are cryptographically chained (hash-chained‡) so that any alteration to a past entry is detectable, and each entry carries a synchronized UTC‡ timestamp.
- **Independent of the AI helpers.** It records facts, not AI interpretations, and continues to operate regardless of the Reporting, Summary, Triage, or Compliance helpers.

### 8.2 What is recorded

The audit log records, at minimum:

- Sign-in / sign-out and authentication events (including MFA and failed attempts).
- Role and permission changes, and user / site provisioning.
- Workflow create / edit / enable / disable (§6).
- AI-helper policy changes with before/after values and effective version (§7).
- Alert acknowledgements (§5.2).
- Integration additions, edits, and removals (§6.3).
- Data exports and configuration/security-setting changes (§11).

### 8.3 Using the audit log

1. Open the **Administration** workspace and select **Audit log** (requires Supervisor role or higher, §4.2).
2. Filter by site, user, time range, or event type.
3. Review entries; each is read-only.
4. Export the filtered record for an audit in an open format (CSV / JSON) where you have export permission (§4.2, §10.3).

The audit log is retained for **7 years‡** (or per your contract) and is covered by the same encryption and residency controls as the rest of your data (§11).

---

## 9. Administration

Administration tasks require Administrator role (§4.2). Exact administration screens and options are preliminary.

#### 9.1 Users & access

**To add a user**

1. Open the **Administration** workspace and go to user management.
2. Add the user with their name and organizational email.
3. Assign the appropriate role (§4.2).
4. Scope the user to the correct site(s).
5. Save and confirm the user receives access per your SSO configuration (§11.3).

Review users and their access periodically, and remove access promptly when it is no longer needed. User and role changes are recorded in the audit log (§8).

#### 9.2 Sites & devices

Sites and their devices are provisioned as part of deployment. Day-to-day, an administrator can confirm that a site's devices are reporting through the Sensorium™ Gateway and that telemetry is current in **Monitoring** (§5.1). Device configuration lives with the Gateway and field devices — see their manuals (§13.4).

#### 9.3 Integrations

Manage SCADA/ERP integrations from the **Administration** workspace (§6.3). Adding, editing, or removing an integration affects every workflow that depends on it — change with care and

verify dependent workflows afterward. Integration changes are recorded in the audit log (§8).

---

## 10. Maintenance

Platform maintenance keeps your deployment recoverable, current, and portable. For the cloud service, 5Tech performs most of this on your behalf; for on-premises / edge deployments (§11.4), the tasks are shared with your team per the deployment runbook. Values below are ‡ proposed and confirmed at deployment.

### 10.1 Backup & restore

- **Cloud.** Data is backed up automatically with **encrypted daily backups‡** and point-in-time recovery to within **15 min‡** (the recovery-point objective, §13.3). Backups are retained **30 days‡**. Restores are verified periodically‡.
- **On-premises / edge.** Backups run per the deployment runbook to storage you control; verify restores on your own schedule.

**To request a restore (cloud)**

1. Contact 5Tech support (§13) with the site, the data affected, and the target point in time.
2. Confirm the restore scope and expected recovery point with support.
3. Verify the restored data in **Monitoring** (§5) and the audit log (§8) once complete.

### 10.2 Software updates & patch cadence

- **Cloud.** Updates are applied by 5Tech on a rolling basis with **no user action**. Feature releases occur roughly **monthly‡**; security patches are applied within **30 days‡** of vendor release, and **critical** patches within **7 days‡**. Maintenance windows that may affect availability are announced at least **5 business days‡** in advance.
- **On-premises / edge.** Releases are delivered **quarterly‡** with out-of-band **critical** security patches, applied by 5Tech or by your team per the deployment agreement.

### 10.3 Data export & portability

Your data is portable and not locked in:

- Export telemetry, alerts, reports, and the audit log in **open formats (CSV / JSON)‡** through the UI and the REST API‡, where you have export permission (§4.2).
- Request a **full-tenant export** at any time; it is provided within **30 days‡** in open formats.

- Retention periods and residency for exported and stored data are covered in §11.

---

## 11. Security, data & deployment

Security and data handling are core to a platform whose value is auditability and trust. The controls below are ‡ proposed and confirmed as part of deployment; the audit log (§8) records changes to any of them.

### 11.1 Encryption in transit

All network traffic is encrypted with **TLS 1.2 / 1.3‡** — the browser/API traffic to the Platform over HTTPS, and the MQTT telemetry ingest from the Sensorium™ Gateway over MQTT-over-TLS. No plaintext transport is offered.

### 11.2 Encryption at rest

Stored data — databases, object storage, and backups — is encrypted at rest with **AES-256‡** using managed keys‡.

### 11.3 Authentication & MFA

- **Single sign-on (SSO)** via **SAML 2.0 / OpenID Connect (OIDC)‡** against your identity provider, so accounts follow your organization's joiner/leaver process.
- **Multi-factor authentication (MFA)‡** (authenticator / TOTP‡) enforced where enabled.
- Idle sessions time out after **30 min‡**. Authentication events are recorded in the audit log (§8).

### 11.4 Deployment model

- **Cloud (default).** Multi-tenant SaaS, hosted and maintained by 5Tech.
- **Optional single-tenant cloud, on-premises, or edge appliance‡** where data must remain on infrastructure you control. Feature parity between models is confirmed at deployment‡.

### 11.5 Supported browsers

Use a current, supported desktop browser — the current and previous major version of:

| BROWSER | MINIMUM VERSION‡ |
|---|---|
| Google Chrome | ≥ 114‡ |
| Microsoft Edge | ≥ 114‡ |
| Mozilla Firefox | ≥ 115 ESR‡ |
| Apple Safari | ≥ 16‡ |

JavaScript and cookies must be enabled; a minimum viewport of **1280 × 720‡** is recommended.

### 11.6 Data retention & residency

- **Retention (‡ proposed, configurable per deployment).** Telemetry **13 months‡** (rolling); alerts & events **24 months‡**; the audit log **7 years‡** (or per contract).
- **Residency.** Cloud data is hosted in your **selected region (Canada, EU, or US)‡**; on-premises / edge deployments (§11.4) keep all data on infrastructure you control.

---

## 12. Troubleshooting

Try the steps below first. If a problem persists, contact support (§13) with the site name, the time it occurred, and any alert or workflow identifiers.

| SYMPTOM | POSSIBLE CAUSE | ACTION |
|---|---|---|
| Cannot sign in | Wrong credentials, expired access, MFA, or SSO/IdP outage | Confirm credentials and MFA; check with your administrator that access is active and SSO is up; see §4.1, §11.3 |
| Dashboard shows stale or no data | Telemetry not reaching the Platform (Gateway/device/uplink) | Check the freshness indicator; confirm the Gateway is online (Gateway manual, §13.4); contact support if data does not resume |
| Expected alert did not appear | Triage, thresholds, or event not generated | Review Triage (§7.1) and alert thresholds with an administrator |
| Too many / mis-ranked alerts | Triage not tuned for the site | Adjust Triage (§7.1); validate in Monitoring |
| Workflow did not run | Workflow disabled, trigger not matched, or condition false | Confirm the workflow is enabled (§6.2); review its trigger and conditions |
| ERP/SCADA action failed | Integration not configured or unavailable | Verify the integration in Administration (§9.3); contact support if it remains unavailable |
| Missing menu or action | Insufficient role | Confirm your role with an administrator (§4.2) |

## 13. Support & service levels

**5Tech** — *Future Innovative Vision Engineering* — is an automation and informatics company headquartered in Vancouver, BC, Canada.

- **Web:** https://5tech.ca
- **Email:** info@5tech.ca
- **HQ:** Vancouver, BC, Canada

### 13.1 Support & maintenance support

For ongoing help, 5Tech offers **Monitoring & Maintenance Support** — a support arrangement to help you tune alerts, rules, and workflows and keep the deployment healthy.

- **Support hours‡:** 08:00–18:00 PT, Monday–Friday (excluding holidays).
- **Critical-incident response target‡:** within 4 business hours; after-hours escalation per contract‡.

### 13.2 Deployment & onboarding services

Deployment, integration, and training are delivered as services, not covered by this guide:

- **Pilot & Proof-of-Value** — a focused pilot/MVP to prove value.
- **Deployment & Integration Support** — help to roll out and integrate the Platform: commissioning, training, and ERP/EAM/SCADA integration.
- **Monitoring & Maintenance Support** — ongoing support to tune and maintain the deployment (§13.1).

### 13.3 Service levels (SLA) & terms

| ITEM | TARGET (‡ PROPOSED) |
|---|---|
| Availability / uptime (cloud) | **99.5 %‡** monthly, excluding announced maintenance |
| Recovery-point objective (RPO) | **≤ 15 min‡** (cloud); on-prem per runbook |
| Recovery-time objective (RTO) | **≤ 4 h‡** (cloud); on-prem per runbook |
| Support hours | 08:00–18:00 PT, Mon–Fri‡ (§13.1) |
| Warranty / license terms | `[TBD]` — legal/contractual, provided in the subscription agreement; not stated here because it must not be invented |

SLA figures are ‡ proposed targets and are confirmed in your subscription agreement; on-premises targets depend on the customer-controlled environment.

### 13.4 Related documents

- **Gateway datasheet:** `datasheets/sensorium-gateway-datasheet/` — the Connect layer that feeds the Platform.
- **Gateway manual:** `manuals/sensorium-gateway-manual/` — operation and configuration of the Gateway.
- **Field devices:** Sensorium™ Zone Awareness and Sensorium™ SmartBolt datasheets — the Sense layer.
- **Solutions:** Fleet Management and Construction Sites Monitoring — outcomes built on this chain.

When contacting support, have ready: the site name, the time of the issue, the affected users or roles, any alert/workflow identifiers, and (for administrators) the relevant audit-log entries (§8).

---

### Figures

| ID | TITLE | FILE | ASPECT | PURPOSE |
|---|---|---|---|---|
| FIG-001 | Monitoring Dashboard | `images/dashboard_monitoring.png` | 16:9 | Cover / hero — the monitoring workspace |
| FIG-002 | Platform Architecture | `diagrams/platform_architecture.png` | 16:9 | Three layers + SCADA/ERP integration |
| FIG-003 | Automation & AI Overview | `diagrams/ai_agents_overview.png` | 4:3 | The four AI-assisted helpers (Triage · Compliance · Reporting · Summary) and what each suggests, flags, or reports |
| FIG-004 | Decision Loop | `diagrams/decision_loop.png` | 16:9 | Sensor event → helper suggestion → a person decides → action |
| FIG-005 | Automation Workflow Builder | `images/automation_workflow_builder.png` | 16:9 | The automation workflow view (UI mockup) |

---

*This guide is preliminary and subject to change. Values marked ‡ are proposed and confirmed at deployment; a remaining `[TBD]` is a legal/contractual term. See `revision.md` for change control and `references.md` for sources. Web publication target: `/resources/manuals/platform/`.*