CLIENT VOLUME 2

KESHI ECTS

ECTS Operations and Deployment Guide

Client-facing operations reference focused on runtime topology, deployment posture, monitoring, incident escalation, backup, restore, and recovery. This volume is intended for operations managers, client IT, service oversight, and governance stakeholders.

AUDIENCE
Operations, support, client IT

FOCUS
Runtime and continuity

VERSION
1.0 | March 10, 2026

Deployment

Monitoring

Incident response

Recovery

1. Operations Scope

This guide explains how the ECTS service is operated from a client-facing perspective. It describes what runtime components exist, what must be monitored, how incidents are escalated, and how continuity objectives are framed.

Use this guide for

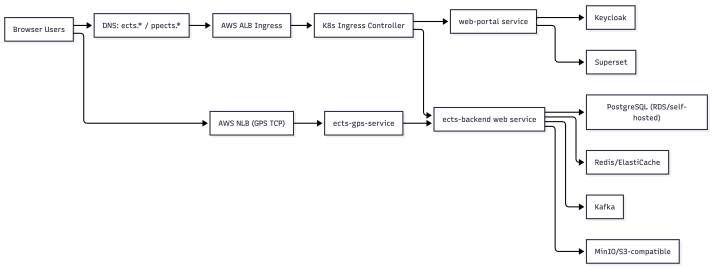
- Service introduction for client operations teams
- Production support readiness reviews
- Incident management alignment and escalation planning
- Business continuity and recovery discussions

Not covered here

- Developer workstation setup
- Source-level engineering diagnostics
- Private implementation internals and repository detail

2. Runtime Topology and Deployment

The production platform combines a public web entry point, protected portal components, backend service processing, identity control, storage layers, and monitoring support.



Deployment-oriented view of the major runtime components and supporting services.

Operational runtime groups

- Public documentation and portal entry surfaces
- Identity and session management
- Portal frontend and backend business services
- Databases, object storage, and configuration backing stores
- Reporting and analytics paths
- Monitoring, logging, and backup control points

Deployment expectations

AREA	EXPECTATION	OPERATIONAL IMPACT
Frontend availability	Portal entry points remain reachable and authenticated users can load core pages.	Loss directly affects all users.
Backend service health	Business APIs respond within normal performance bounds.	Module pages may partially or fully fail if backend health degrades.
Identity path	Authentication and token refresh remain available.	Users cannot access protected content when identity is unavailable.
Reporting path	Analytics content loads after its expected extended wait window.	Report access may degrade independently of the rest of the portal.

3. Monitoring and Service Objectives

Monitoring is used to detect service degradation before it becomes an extended outage and to provide evidence during incident response and recovery validation.

What is monitored

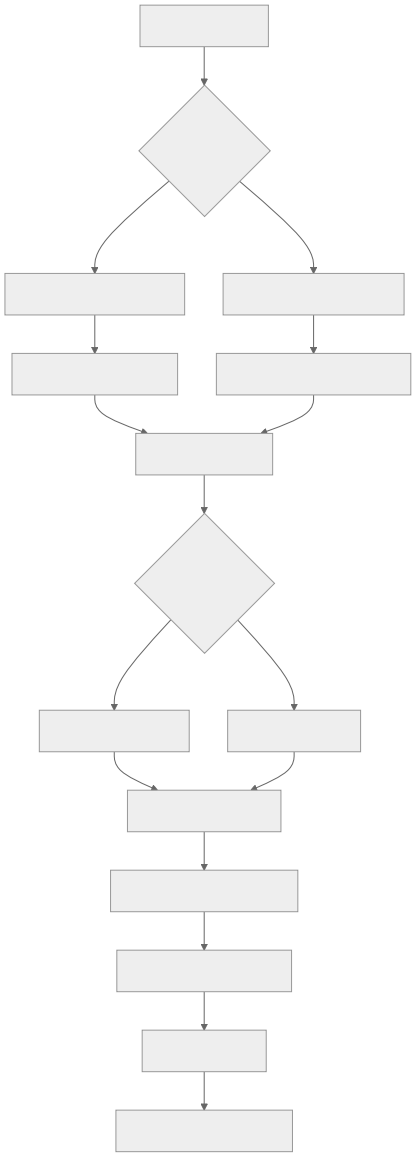
- Portal availability and protected page load success
- Authentication and authorization path health
- Backend API health and request behavior
- Report page load success and analytics availability
- Device telemetry freshness and command execution outcomes
- Backup job completion and recovery readiness signals

Client-facing service objectives

OBJECTIVE	TARGET
Portal availability	99.5% monthly successful access to core user workflows
Authentication path availability	99.9% successful identity handoff for valid users
Report page completion	99.0% successful report page load completion
Critical incident acknowledgement	15 minutes

4. Incident Response Model

Incidents are managed through a structured workflow that moves from detection to validation, containment, restoration, and closure.



Operational incident flow from alert or symptom through resolution and review.

Major phases

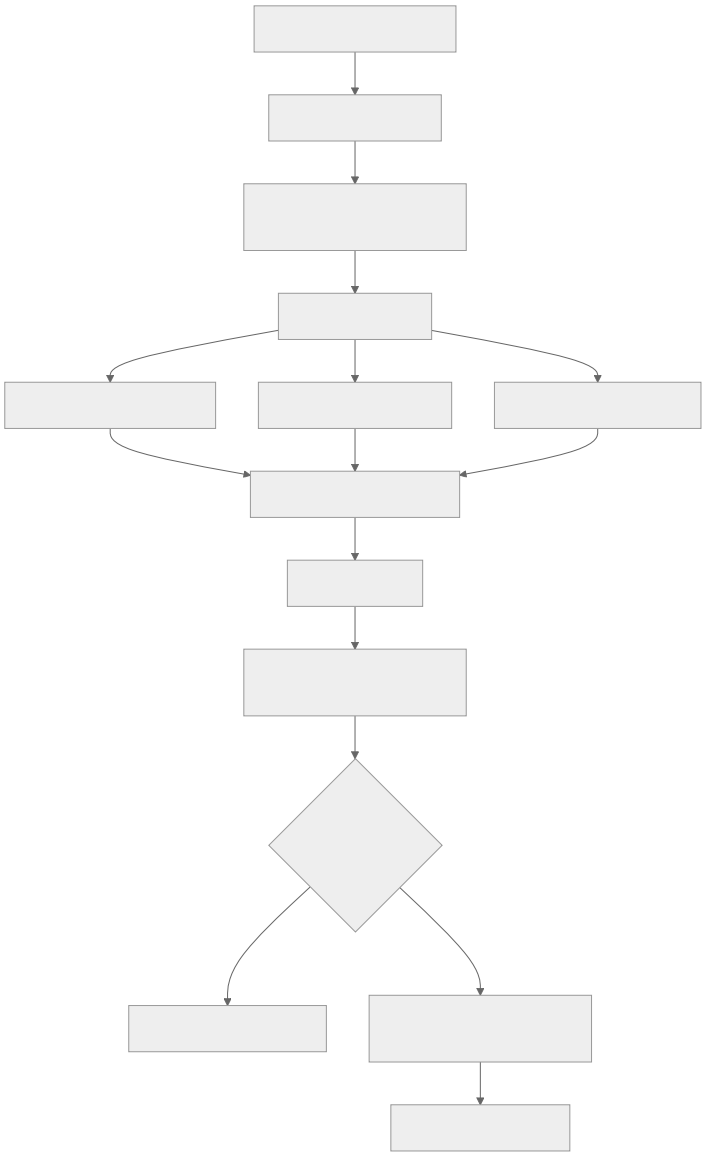
1. **Detect and qualify.** Confirm whether the symptom is a true incident, a role/access issue, or expected asynchronous behavior.
2. **Contain and communicate.** Limit operational impact and inform relevant client and delivery stakeholders.
3. **Restore service.** Recover the affected capability and verify representative user flows.
4. **Close and review.** Document root cause, outcome, and any follow-up controls or fixes.

Escalate immediately when

- Users cannot authenticate or session establishment fails broadly.
- Multiple protected pages fail across core modules.
- Alert queues, device telemetry, or report pages fail persistently.
- Operational data is stale, unavailable, or materially inconsistent.

5. Backup, Restore, and Recovery

Continuity planning covers transactional records, attachments, identity-related exports, and runtime configuration required to restore service safely.



Recovery flow from backup selection through restoration, smoke checks, and closure.

Recovery objectives

SCENARIO	RTO	RPO
Full platform outage	4 hours	30 minutes
Single service outage	1 hour	15 minutes
Report subsystem outage	2 hours	1 hour

Backup operation and restore rehearsal are treated as part of normal service readiness, not one-time project closeout artifacts.

Protected data classes

DATA ASSET	PROTECTION APPROACH	RETENTION PROFILE
Transactional platform data	Scheduled full and incremental database backup strategy	35 days
Telemetry-related storage	Regular snapshot or backup coverage across data stores	14 days
Documents and attachments	Object-storage backup and restore workflow	35 days
Configuration and identity exports	Controlled export and snapshot retention for recovery support	35 to 90 days

6. Operational Readiness Checklist

This page can be used during handover, operational readiness review, or steady-state governance checks.

Readiness checks

- Operational owners know the escalation path and expected response windows.
- Representative login, module access, and reporting tests are defined.
- Monitoring ownership and notification routing are understood.
- Backup execution and restore validation evidence is available.

Evidence typically requested

- Current environment and deployment summary
- Latest incident runbook or support process reference
- Recent backup success and restore rehearsal confirmation
- Named contact points for operations and escalation

CLIENT VOLUME 2

Operate With Clarity

This volume is intended to support steady-state service governance, client IT review, and continuity planning around the ECTS platform.

Best paired with

- Client Documentation Pack
- Technical Overview

Publication

Publication: ECTS documentation portal

Prepared by: Keshi ECTS Engineering Team

Revision: 1.0, March 10, 2026