



SERVICE SPECIFICATION / MANAGED OPERATIONS

Break-fix triage and field dispatch

GHT-SVC-034 · Revision 1.0 · 06 September 2026 · 1 / 3

Incident intake, remote checks, site access, vendor boundaries, technician skills, tools, parts, field work, acceptance testing, and cause notes form one connected path; timing, travel, and rates stay contract-specific.

Intended outcome

A complete incident record from the first symptom through triage, field work, tested restoration, owner confirmation, asset updates, and preventive follow-up.

Service scope

Break-fix begins with a symptom, not a diagnosis. Triage distinguishes user, endpoint, cable, power, network, carrier, platform, account, vendor, environmental, and change-related causes before deciding whether remote work, customer action, vendor escalation, or field dispatch is appropriate.

A field visit needs a site contact, access window, safety conditions, asset and location, known-good test, scope authority, parts plan, escalation contact, and restoration criteria. Coverage, arrival targets, travel, minimums, after-hours rates, parts, and third-party delays are contract-specific.

How the system fits together

01 Intake	Reporter, site, time, symptom, impact, service, safety, contacts and access
02 Triage	Dependencies, monitoring, history, remote tests, owner, severity and escalation
03 Field mission	Skill, tools, parts, site window, work authority, stop conditions and remote bridge
04 Restoration evidence	Service test, readings, photos, config, parts, cause, owner acceptance and prevention

Typical project triggers

- Repeat dispatches close with “working now” but no tests, cause, or change record
- Technicians arrive without site access, owner contacts, parts, drawings, or acceptance criteria
- Carrier, landlord, platform, equipment, and cabling ownership is disputed during an outage
- Remote teams cannot see current topology, labels, serials, photos, or configuration history



GHT-SVC-034 / BREAK-FIX TRIAGE AND FIELD DISPATCH

Delivery and acceptance

Revision 1.0 · 06 September 2026 · 2 / 3

The final project scope identifies quantities, locations, dependencies, and the evidence required at each delivery stage.

01 Qualify the incident

Capture reporter, time, site, affected service and users, symptoms, scope, recent changes, alarms, safety, business impact, contacts, access, and current workaround.

Acceptance evidence: Timestamped incident record, impact statement, symptom evidence, change context, contacts, and severity under the contracted model.

02 Triage dependencies

Use approved remote checks, topology, monitoring, power, link, configuration, carrier, account, and vendor evidence to isolate the likely layer and define the next safe test.

Acceptance evidence: Triage timeline, tested hypotheses and results, dependency owner, escalation record, and dispatch decision.

03 Dispatch a defined task

Send site, contact, access, safety, asset, tools, parts, remote bridge, method, stop conditions, change authority, and acceptance tests to the assigned field resource.

Acceptance evidence: Dispatch brief, acknowledgement, part custody, arrival and access record, before photos, tests, and approved changes.

04 Prove restoration and learn

Validate the affected service with the owner, capture final readings and configuration, update assets and labels, document temporary or permanent repair, and open preventive follow-up.

Acceptance evidence: Owner-confirmed service test, after photos, test results, parts and change record, cause classification, exceptions, and follow-up owner.

Handover deliverables

- Incident intake, severity, escalation, and dispatch model
- Site, asset, dependency, vendor, contact, access, and spare readiness record
- Remote-triage and field-mission templates
- Timestamped test, change, parts, photo, and restoration evidence
- Cause and recurrence review, updated documentation, exception list, and preventive follow-up

Closeout: GHT and the customer review the agreed evidence, record unresolved exceptions and owners, and confirm acceptance against the signed project scope.



GHT-SVC-034 / BREAK-FIX TRIAGE AND FIELD DISPATCH

Planning and scope boundaries

Revision 1.0 · 06 September 2026 · 3 / 3

Customer and site inputs

- Sites, hours, contacts, access, safety, escort, parking, travel, and after-hours conditions
- Covered services, assets, dependencies, monitoring, remote access, vendors, warranties, and support status
- Severity, coverage window, response target, escalation, authority, rates, minimums, and exclusions
- Common spares, approved substitutions, custody, procurement, shipping, and return process
- Dispatch brief, communication cadence, acceptance tests, evidence, cause categories, and preventive follow-up

Constraints and coordination

- Coverage windows, arrival or response targets, travel, after-hours rates, minimums, parts, and third-party coordination are contract- and location-specific
- Restoration can be delayed by site access, unsafe conditions, hidden pathways, carrier or vendor ownership, unavailable parts, licensing, warranties, or required approvals
- A temporary workaround must be labeled, documented, risk-accepted by the owner, and assigned a permanent-resolution owner
- Remote access and changes require customer authorization, least privilege, protected credentials, logging, backup, and rollback appropriate to the system

Commercial scope and responsibilities

This specification describes the service framework. The signed statement of work defines included equipment, quantities, software licenses, integrations, access windows, schedule, pricing, warranty, and support coverage. Additional construction, electrical work, recurring subscriptions, and ongoing support require an explicit line item.

The customer appoints an acceptance owner and provides authorized access, required site information, and decisions. GHT records assumptions, coordinates assigned work, and submits changes for agreement before expanding the scope.

Technical references

National Institute of Standards and Technology — SP 800-61 Rev. 3: Incident Response Recommendations
| Source review: 2026-08-20

National Institute of Standards and Technology — SP 800-128: Security-Focused Configuration Management
| Source review: 2026-08-20

Cybersecurity and Infrastructure Security Agency — Cross-Sector Cybersecurity Performance Goals | Source review: 2026-08-20

Service guide and project discussion | Source review: 2026-09-06