SERVICE SPECIFICATION / PHYSICAL SECURITY

Intrusion alarms and monitoring

GHT-SVC-020 • Revision 1.0 • 06 September 2026 • 1 / 3

Sensors, zones, users, arming rules, communication paths, verification, notification, and response instructions, working as one system.

Intended outcome

Named zones and users, tested sensors and communication paths, current contacts, notification evidence, and documented response instructions.

Service scope

An intrusion system supervises defined conditions such as doors, windows, motion, glass breakage, duress, or equipment state. It needs zone naming, arming partitions, user permissions, communication paths, maintenance tests, and response instructions that reflect how the facility operates.

Monitoring is not automatically continuous or police dispatch. Coverage windows, verification steps, contacts, response targets, permits, and central-station services are contract- and jurisdiction-specific and must be stated explicitly.

How the system fits together

01 Detect	Contacts, motion, glass break, duress, environmental or equipment inputs
02 Control	Panel, zones, partitions, users, arming rules, local annunciation
03 Communicate	IP, cellular, or other supported paths with supervised failure states
04 Respond	Local procedure, owner notification, verification, and separately contracted monitoring

Typical project triggers

- Unknown zones or recurring nuisance alarms
- Changes in occupancy, perimeter, hours, or protected assets
- Dependence on a single aging communication path
- No current contact list, test record, permit owner, or response procedure

Delivery and acceptance

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

01 Map risk and operation

Identify entry points, protected areas, hours, user behavior, pets or environmental motion, existing zones, communications, permits, and response ownership.

Acceptance evidence: Risk-and-zone survey, existing-device test notes, contact owner, and jurisdictional questions.

02 Design detection and response

Select zone types and placement, partitions, arming behavior, notification paths, verification steps, communication diversity, and documented coverage window.

Acceptance evidence: Zone list, device plan, communication diagram, event-to-response matrix, and monitoring assumptions.

03 Install and program

Install and label field devices, establish users and partitions, program event handling, coordinate any monitoring account, and train named administrators.

Acceptance evidence: Device inventory, zone text, user-role record, programmed event list, and monitoring account handoff where contracted.

04 Test the full signal path

Exercise sensors, tamper, low-battery, communications loss, arming, entry and exit timing, notifications, and contracted monitoring procedures without causing an unintended dispatch.

Acceptance evidence: Zone-by-zone test sheet, signal receipt evidence, notification samples, contact-list confirmation, and exception log.

Handover deliverables

- Zone and device schedule
- Partition, user, timing, and event-response configuration
- Communication and power diagram
- Zone-by-zone and end-to-end signal test evidence
- Contact list, administrator training, permit-owner notes, and maintenance plan

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

Planning and scope boundaries

Revision 1.0 • 06 September 2026 • 3 / 3

Customer and site inputs

- Protected spaces, event types, operating hours, and arming owners
- Door, glass, motion, temperature, dust, pets, and other environmental conditions
- Local notification, owner contact, verification, and monitoring requirements
- Available IP, cellular, power, battery, and pathway conditions
- Jurisdictional permit, registration, dispatch, and false-alarm rules

Constraints and coordination

- Detection cannot guarantee prevention or a specific response outcome
- Central-station hours, verification, response targets, and dispatch processes are separately contracted and jurisdiction-specific
- Fire alarm, life safety, and intrusion are distinct scopes even when platforms can exchange status
- Wireless range, batteries, environmental motion, user behavior, and communication outages affect performance

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

Security Industry Association — ANSI/SIA CP-01-2019: Features for False Alarm Reduction | Source review: 2026-08-20

Security Industry Association — At-a-Glance Guide to SIA Standards | Source review: 2026-08-20

Cybersecurity and Infrastructure Security Agency — Physical Security | Source review: 2026-08-20

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