DOC-OPS-0003 - Escalation and Incident Response Guide

Document ID: DOC-OPS-0003
Owner: Field Operations Director
Approver: COO
Version: 1.4
Status: Published
Effective date: 2026-01-01
Review date: 2027-01
Applicability: All operations staff, on-call responders, and functions supporting incident response
Source system: Policy repository; incident records in the operations incident platform

Fictional document created for the GS Reference Enterprise. Not real policy.

PURPOSE

This standard states how Compass One classifies an operational incident, how quickly it must be answered, who holds escalation authority, and what must be preserved afterwards. It exists so that response time is a function of impact rather than of who happens to notice the incident.

SCOPE

The standard covers operational incidents affecting Compass One services, field operations, and customer-facing delivery. Security incidents follow the security incident reporting procedure.

- This standard applies to every operational incident affecting a Compass One service.
- A security incident is handled through DOC-SEC-0002 rather than this standard.

DEFINITIONS

- An incident is an unplanned event that degrades a Compass One service.
- Severity 1 is an incident causing complete loss of a customer-facing service.
- Severity 2 is an incident causing partial degradation of a customer-facing service.
- Severity 3 is an incident with limited impact on a single customer.
- The incident commander is the individual accountable for coordinating the response.
- Evidence is any record supporting later reconstruction of the incident.

POLICY STATEMENTS

Severity determines every downstream obligation in this standard. Response windows, notification duties, and review requirements all derive from the assigned severity.

SEVERITY CLASSIFICATION

- An incident affecting more than one hundred customers is classified as Severity 1.
- An incident involving loss of customer data is classified as Severity 1.
- A safety event involving injury is classified as Severity 1.
- An incident with an available workaround is classified as Severity 2.
- Severity is assigned by the on-call operations lead at declaration.

- Severity may be raised at any point during an active response.

RESPONSE WINDOWS

- A Severity 1 incident requires acknowledgement within fifteen minutes.
- A Severity 1 incident requires an assigned incident commander within thirty minutes.
- A Severity 2 incident requires acknowledgement within one hour.
- A Severity 3 incident requires acknowledgement within one business day.
- A Severity 1 response must continue uninterrupted until service is restored.

NOTIFICATION

- The on-call operations lead must be notified first for every incident.
- A Severity 1 incident requires executive notification within one hour.
- Executive notification is directed to the COO.
- A Severity 1 incident involving customer data requires notification to the CISO.
- A Severity 2 incident requires executive notification when unresolved after four hours.
- Customer notification for a Severity 1 incident is issued within four hours.

ESCALATION AUTHORITY

- The incident commander has authority to escalate to any Compass One function.
- The incident commander may authorize an emergency change during a Severity 1 incident.
- Severity 2 escalation to the executive team requires Field Operations Director approval.
- Any responder may raise the severity of an active incident.

COMMUNICATION

- The incident commander owns all internal incident communication.
- A Severity 1 incident requires a status update every thirty minutes.
- A Severity 2 incident requires a status update every two hours.
- External communication requires approval from the VP Customer Experience.
- Speculation about cause is prohibited in customer communication.

BUSINESS CONTINUITY

- A Severity 1 incident lasting beyond four hours requires continuity plan activation.
- The continuity plan is activated by the Field Operations Director.
- Continuity activation requires notification to the COO.

EVIDENCE PRESERVATION

- Every responder must preserve logs relevant to an active incident.
- Evidence must be preserved before any remediation that alters system state.
- Incident evidence is retained for twenty four months.
- Deletion of incident evidence during an active investigation is prohibited.

POST-INCIDENT REVIEW

- A Severity 1 incident requires a post-incident review.

- A Severity 2 incident requires a review when customer impact exceeds two hours.
- The post-incident review must be completed within five business days.
- The post-incident review is owned by the incident commander.
- A post-incident review must identify at least one corrective action.
- Corrective actions are tracked to closure by the Field Operations Director.

RESPONSIBILITIES

- The Field Operations Director owns this standard.
- The on-call operations lead is accountable for initial severity assignment.
- The incident commander is accountable for the coordinated response.
- The Technical Support Director owns customer notification.
- Information Security owns evidence handling for a security incident.

EXCEPTIONS

- An exception to a response window requires Field Operations Director approval.
- A planned maintenance event is not classified as an incident.
- Every exception must be recorded in the incident record.

RELATED STANDARDS

- Security incident reporting is stated in DOC-SEC-0002.
- Customer escalation routing is stated in DOC-CUS-0001.
- Information handling requirements are stated in DOC-SEC-0005.