**Cybersecurity Templates**

**Incident Handling Guide**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Incident Handling Guide** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document ID:** | IR‑DIR‑MOD‑[####] | **Owner:** | [Head of CSIRT / Security Operations] |
| **Approver:** | [CISO / Operations Governance Board] | **Effective date:** | [YYYY‑MM‑DD] |

Contents

[Incident Handling Guide 4](#_Toc207236483)

[1. Scope & Interfaces 4](#_Toc207236484)

[2. Guiding Principles 4](#_Toc207236485)

[3. Roles & RASCI 4](#_Toc207236486)

[5. Activation & Escalation 6](#_Toc207236487)

[6. Procedure by Phase (PICERL) 6](#_Toc207236488)

[6.1 Preparation (Continuous) 6](#_Toc207236489)

[6.2 Identification (Detect & Triage) 6](#_Toc207236490)

[6.3 Containment 6](#_Toc207236491)

[6.4 Eradication 7](#_Toc207236492)

[6.5 Recovery 7](#_Toc207236493)

[6.6 Lessons Learned (Review & Improve) 7](#_Toc207236494)

[7. Communications 7](#_Toc207236495)

[8. Evidence & Chain‑of‑Custody 8](#_Toc207236496)

[9. Legal, Regulatory & Insurance 8](#_Toc207236497)

[10. Tooling & Automation 8](#_Toc207236498)

[11. Metrics & Targets 8](#_Toc207236499)

[12. Training & Exercises 9](#_Toc207236500)

[13. Version Control & Change History 9](#_Toc207236501)

[Appendices — Drop‑in Aids 9](#_Toc207236502)

[Appendix A — Severity & Priority Crosswalk 9](#_Toc207236503)

[Appendix B — Initial Investigation Prompt Sheet 10](#_Toc207236504)

[Appendix D — Evidence Register (Template) 10](#_Toc207236505)

[Appendix E — Situation Report (SITREP) Mini‑Template 10](#_Toc207236506)

[Appendix F — Contact Roster (extract) 10](#_Toc207236507)

[Appendix G — Remediation Action Plan (brief) 11](#_Toc207236508)

[Appendix H — Closeout Checklist 11](#_Toc207236509)

[Appendix I — Readiness Checklist (Quarterly) 11](#_Toc207236510)

# Incident Handling Guide

**Purpose**  
Provide a practical, end-to-end guide for handling cybersecurity incidents. This document translates policy into actionable steps that responders, leaders, and partners can follow under pressure. It defines roles, workflows, quality gates, and templates to preserve evidence, minimize impact, comply with obligations, and facilitate effective learning.

**Audience**  
CSIRT/IR teams, SOC analysts, SRE/IT, Legal/Privacy, Communications, Product/Business owners, and auditors.

# 1. Scope & Interfaces

**Scope:** All security incidents affecting [Organization] systems, data, and services (on-prem, cloud, SaaS), including third-party incidents where [Organization] is accountable.

**Out of scope:** Physical-only incidents without information‑system impact (refer to Safety/Physical Security SOP).

**Interfaces:** Business Continuity/DR, Crisis Management, Change Management, Risk Management, Legal/Privacy, Communications/PR, Vendor/Insurer procedures, Knowledge Management (playbooks, known errors).

# 2. Guiding Principles

1. **Safety first; act fast, act safely.** Contain impact quickly while preserving evidence.
2. **Single source of truth.** One incident record with mandatory metadata; link related changes/risks/knowledge.
3. **Least privilege & need‑to‑know.** Access to incident data is role‑based; sensitive artifacts are segregated.
4. **Time is a metric.** Track discovery, activation, containment, eradication, recovery, and review times.
5. **Learning is mandatory.** No closeout without lessons, action owners, and due dates.
6. **Plain language communications.** Consistent cadence, clear audience targeting, archived updates.

# 3. Roles & RASCI

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Role** | **Core Responsibilities** | **R** | **A** | **S** | **C** | **I** |
| **Incident Handler (Lead)** | Orchestrates response; maintains log; drives decisions; enforces cadence | **R** |  |  | Legal, Comms | Execs |
| **CSIRT Lead / SecOps Manager** | Activates CSIRT; sets priority; assigns resources; approves containment | **R** | **A** |  | Legal, Comms | Execs |
| **Evidence Custodian (Forensics)** | Manages evidence store; hashes; chain‑of‑custody | **R** |  |  | Legal |  |
| **Engineering/SRE SMEs** | Execute containment/eradication/recovery; testing & validation | **R** |  |  | Handler |  |
| **Communications Lead** | Internal/external comms; SITREPs; media/regulator/customer messaging | **R** |  |  | Legal, Execs | Staff |
| **Legal/Privacy** | Notification thresholds, privilege, holds, contracts, regulator engagement |  |  | **S** | Handler, Comms |  |
| **Senior Exec (Sponsor)** | Strategic decisions; risk acceptance; external commitments |  | **A** |  | Legal, Comms | Board |
| **IT Service Desk** | Intake, ticketing, paging, initial classification | **R** |  |  | Handler |  |

RASCI: Responsible, Accountable, Support, Consulted, Informed.

**4. Severity, Urgency & Priority**

* **Impact:** High / Medium / Low — based on service criticality, data sensitivity, user/customer effect, financial/regulatory risk.
* **Urgency:** High / Medium / Low — based on spread potential, containment state, regulatory clocks, peak operations.
* **Priority:** P1–P4 from crosswalk of Impact × Urgency (see Appendix A).

**Cadence by Priority (default):**

* **P1:** Stand up the war room immediately. Updates continuous/hourly; exec/legal/comms engaged.
* **P2:** Hourly updates; cross-team coordination.
* **P3:** Daily updates.
* **P4:** As needed; backlog if appropriate.

# 5. Activation & Escalation

**Triggers (examples):** life/safety risk; critical service outage; suspected/confirmed exposure of restricted data; uncontrolled lateral movement; ransomware; legal/regulatory deadlines.

**Activation Steps (≤ 15 minutes for P1/P2):**

1. Open incident record; assign **Incident Handler** and **Evidence Custodian**.
2. Convene bridge/war room; publish first **SITREP** due time.
3. Apply initial containment where safe; start chain‑of‑custody for artifacts.
4. Classify severity/priority; launch comms to stakeholders per matrix.
5. Log decisions as they occur; time‑stamp in UTC.

**De-escalation:** Reduce priority only after containment is verified, no spread is observed within the agreed-upon window, and the user/service impact is minimized.

# 6. Procedure by Phase (PICERL)

## 6.1 Preparation (Continuous)

* Maintain CSIRT roster with primary/backup contacts.
* Keep playbooks for common incidents (phishing, ransomware, unauthorized access, DDoS, data loss, supply‑chain).
* Pre-stage evidence repository with restricted access; document hashing procedure and custody forms.
* Test paging/bridge tools; ensure hard‑copy packs exist (in case of SaaS outage).
* Run exercises; update gaps in plan, playbooks, and tooling.

## 6.2 Identification (Detect & Triage)

* **Intake:** Service desk, SIEM/EDR, user report, vendor alert.
* **Triage questions:** what/where/when; initial vector; affected accounts/systems; data class; current spread.
* **Initial actions:** snapshot logs/metrics; label artifacts; classify Impact/Urgency; set **Priority**.

**Outputs:** Incident ID; first SITREP time; initial containment decision; roles assigned.

## 6.3 Containment

* **Short‑term:** isolate hosts/accounts; disable risky integrations; increase logging; deploy rules/blocks; enable feature flags.
* **Workarounds:** reversible; documented risks; monitoring added; rollback plan; **expiry criteria** set.
* **Safety check:** do no additional harm; coordinate with owners of dependent systems.

**Exit:** spread halted; user impact stabilized; evidence preserved; comms updated.

## 6.4 Eradication

* Remove malicious artifacts; rotate credentials/tokens; patch or reconfigure; cleanse or rebuild images.
* Validate through scans/tests; confirm no persistence/C2 remains; close attacker paths.

**Exit:** Systems are ready for controlled restoration; a back-out plan is prepared.

## 6.5 Recovery

* Restore services in waves (canary/blue‑green as applicable); monitor for relapse.
* Reconcile data; perform health checks; confirm SLOs; notify stakeholders of status.

**Exit:** systems stable; monitoring normal over **[X]** time; user issues resolved.

## 6.6 Lessons Learned (Review & Improve)

* Hold Post‑Incident Review (PIR) within **[5–10] business days** of closure or stabilization.
* Document root cause(s), contributing factors, control gaps, timeline, and what worked/failed.
* Create Action Register: owner, due date, success metric; track to completion.
* Update playbooks, detections, runbooks, and training based on findings.

# 7. Communications

**Principles:** accuracy over speed; plain language; acknowledge uncertainty; time‑box updates.

**Channels:** bridge/war room, email/SMS paging, status page (internal/external), exec briefings, regulator/customer communications via Legal/Comms.

**SITREP Content (one page):** summary; scope/impact; actions (done/next); risks/needs; next update time. (Template in Appendix E.)

**Holding statements (external):** prepared by Comms; reviewed by Legal; stored under Communications Plan.

**Records:** Archive all communications in the incident folder; mark as legally privileged when appropriate.

# 8. Evidence & Chain‑of‑Custody

* **Evidence store:** encrypted; restricted; immutable logs where possible.
* **Register:** each item labeled with ID, description, collection details, SHA‑256 hash, location, and transfer history.
* **Handling:** preserve originals; analyze copies; document every touch; keep timestamps in UTC.
* **Privacy:** minimize personal data; redact where feasible; apply legal hold when instructed.

# 9. Legal, Regulatory & Insurance

* **Notification assessment:** determine triggers (e.g., regulated data exposure, sector obligations, contract terms).
* **Counsel engagement:** route legal questions and regulator engagement through Legal/Privacy.
* **Insurance:** follow policy conditions (panel firms, notification deadlines, consent for vendors).
* **Discovery:** maintain privilege where appropriate; log decisions and approvals.

# 10. Tooling & Automation

* **Ticketing/ITSM:** single incident record; status, owners, SLA clocks, related changes/risks/KB.
* **Monitoring/SIEM/EDR/APM:** alerting and evidence export; retain for required durations.
* **Orchestration/SOAR:** automate common containment actions with approval gates.
* **Knowledge Base:** store playbooks, known errors, and lessons learned for reuse.

# 11. Metrics & Targets

|  |  |  |
| --- | --- | --- |
| **Metric** | **Definition** | **Target** |
| **MTTD** | First alert → incident opened | ↓ over time |
| **MTTA** | Incident opened → CSIRT activated | ≤ [X] min (P1) |
| **MTTC** | Incident opened → containment | ≤ [Y] h (by priority) |
| **MTTR** | Incident opened → recovery | ↓ over time |
| **SITREP Timeliness** | % updates on time | ≥ 95% |
| **Evidence Integrity** | % artifacts with hash + custody | 100% |
| **Action Closure** | % PIR actions closed on time | ≥ 90% |

# 12. Training & Exercises

* Induction and annual refresh for CSIRT and key partners.
* Tabletop exercises at least **[annually]**; scenario packs for ransomware, data breach, BEC, zero-day, cloud misconfig.
* Drill paging/bridge; verify contact lists and assembly locations; test evidence workflow.
* Capture findings and update this guide, playbooks, and rosters.

# 13. Version Control & Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Summary** |
| 1.0 | [YYYY‑MM‑DD] | [Name] | Initial release |

# Appendices — Drop‑in Aids

## Appendix A — Severity & Priority Crosswalk

|  | **Urgency Low** | **Urgency Medium** | **Urgency High** |
| --- | --- | --- | --- |
| **Impact Low** | P4 | P3 | P2 |
| **Impact Medium** | P3 | P2 | P1 |
| **Impact High** | P2 | P1 | **P1** |

**Default Cadence & Approvals by Priority**

* **P1:** War room now; exec/legal/comms on bridge; regulator/insurer assessment; updates continuous/hourly.
* **P2:** CSIRT on bridge; hourly updates; daily exec brief.
* **P3:** Daily updates; service owner engaged.
* **P4:** Planned response; track in backlog if appropriate.

## Appendix B — Initial Investigation Prompt Sheet

* Initial vector?
* Post-exploit activity? Compromised accounts/privilege?
* Persistence or lateral movement?
* C2 observed?
* Data accessed/exfiltrated? Type/volume?
* Impacted services, users, tenants, regions?
* What controls failed/succeeded?
* Regulatory/contractual exposure?
* Immediately following the best action with the least risk?

**Appendix C — Decision Log (One‑liners)**

Format: [UTC] — **Decision:** [what] — **Options:** [A/B/C] — **Owner:** [name] — **Approvals:** [names] — **Rationale:** [brief]

## Appendix D — Evidence Register (Template)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Artifact** | **Source/Collector** | **Date/Time (UTC)** | **Hash (SHA‑256)** | **Location/Label** | **Transfers/Notes** |
| 1 |  |  |  |  |  |  |

## Appendix E — Situation Report (SITREP) Mini‑Template

**Header:** [INC‑ID] | Priority [P#] | Time (UTC) [YYYY‑MM‑DD HH:MMZ] | Handler [name] | SITREP v#

* **Summary:** one paragraph in plain language
* **Scope/Impact:** services/users/data (confirmed vs suspected)
* **Actions:** done / in‑flight / next
* **Risks/Needs:** decisions, resources, blockers
* **Next update:** [UTC]

## Appendix F — Contact Roster (extract)

| **Role** | **Primary** | **Backup** | **Work** | **Mobile** | **Email** |
| --- | --- | --- | --- | --- | --- |
| CSIRT Lead |  |  |  |  |  |
| Incident Handler |  |  |  |  |  |
| Evidence Custodian |  |  |  |  |  |
| Communications Lead |  |  |  |  |  |
| Legal/Privacy |  |  |  |  |  |
| Service Owner(s) |  |  |  |  |  |
| Vendor (IR retainer) |  |  |  |  |  |

## Appendix G — Remediation Action Plan (brief)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Action** | **Owner** | **Start** | **Due** | **Dependencies** | **Status** |
|  |  |  |  |  |  |

## Appendix H — Closeout Checklist

* ☐ RCA completed and approved
* ☐ Lessons & actions logged with owners/dates
* ☐ Evidence sealed (hashes verified)
* ☐ Notifications (regulatory/contractual) completed
* ☐ Residual risk recorded; review date set
* ☐ Playbooks/runbooks/detections updated
* ☐ Final executive summary filed
* ☐ Permissions tightened to read‑only; archive manifest updated

## Appendix I — Readiness Checklist (Quarterly)

* CSIRT roster current; alternates listed
* Contact lists verified; paging tested
* Evidence store healthy; procedure walk‑through completed
* Playbooks reviewed and exercised
* Monitoring/log retention baselines validated
* Insurance/regulatory contacts current
* This guide reviewed and republished (hard and soft copies)