**Cybersecurity Templates**

**Incident Handling Procedure**

**August 2025**

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

|  |
| --- |
| **Incident Handling Procedure** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** | [v1.0] | **Owner:** | [CISO / Head of Security] |
| **Review Cycle:** | [Annually / Bi‑annually] | **Effective date:** | [YYYY‑MM‑DD] |

Contents

[Incident Handling Procedure 3](#_Toc207302518)

[1. Purpose 3](#_Toc207302519)

[2. Scope 3](#_Toc207302520)

[3. References & Alignment 4](#_Toc207302521)

[4. Definitions 4](#_Toc207302522)

[5. Roles & Responsibilities 5](#_Toc207302523)

[6. Incident Classification & Severity 6](#_Toc207302524)

[6.1 Categories (examples) 6](#_Toc207302525)

[6.2 Severity Matrix 6](#_Toc207302526)

[7. Activation & Escalation 7](#_Toc207302527)

[8. Incident Handling Procedure (PICERL) 8](#_Toc207302528)

[9. Communications Plan 10](#_Toc207302529)

[10. Evidence Handling & Documentation 10](#_Toc207302530)

[11. Regulatory, Contractual & Insurance Considerations 11](#_Toc207302531)

[12. Tooling & Data Sources (Examples) 11](#_Toc207302532)

[13. Metrics & Reporting 11](#_Toc207302533)

[14. Training, Testing & Continual Improvement 11](#_Toc207302534)

[15. Acceptance & Approvals 12](#_Toc207302535)

[Appendix A – Triage Intake Form (use in tickets) 12](#_Toc207302536)

[Appendix B – Communications Matrix (example) 12](#_Toc207302537)

[Appendix C – Evidence Register (chain of custody) 13](#_Toc207302538)

[Appendix D – Action Register (post-incident) 13](#_Toc207302539)

[Appendix E – Severity Triggers (tailor) 13](#_Toc207302540)

[Appendix F – Quick Checklists 13](#_Toc207302541)

# Incident Handling Procedure

# 1. Purpose

This procedure establishes a consistent, auditable approach for handling cybersecurity incidents at **[Organization Name]**. It defines roles, activation triggers, severity levels, step-by-step actions (from detection through lessons learned), decision authorities, and communication expectations so that incidents are contained quickly, evidence is preserved, operations are restored safely, and improvements are captured.

**Goals**

* Minimize business impact (safety, financial, legal, reputational).
* Protect confidentiality, integrity, and availability of systems and data.
* Ensure accurate documentation for legal, regulatory, insurance, and forensic needs.
* Drive continual improvement of controls and readiness.

# 2. Scope

This procedure applies to:

* All employees, contractors, vendors, and third parties interacting with **[Organization Name]** information assets.
* All environments (on-prem, cloud, hybrid), networks, applications, endpoints, OT/IoT as applicable, and data processed by or on behalf of **[Organization Name]**.
* All security events suspected to be or confirmed as incidents, including privacy breaches, malware/ransomware, unauthorized access, data exfiltration, DDoS, business email compromise (BEC), insider misuse, supply chain compromise, and loss/theft of devices or media.

Out-of-scope events (e.g., physical safety incidents, non-cyber emergencies) are handled in accordance with the relevant enterprise procedures, with cross-notification as required.

# 3. References & Alignment

* NIST SP 800‑61 (Computer Security Incident Handling Guide) phases are used to structure the lifecycle.
* Related internal documents: Information Security Policy, Access Control Standard, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), Crisis Communications Plan, Privacy Breach Procedure, Digital Forensics SOPs, Cyber Insurance Notification Guide.

# 4. Definitions

* **Security Event:** Any observable occurrence in a system or network (e.g., alert, anomaly, log entry). Events may indicate a potential issue, but are not necessarily incidents.
* **Security Incident:** An event or series of events that actually or potentially jeopardizes the confidentiality, integrity, or availability of systems/data, or violates security policy/acceptable use.
* **CSIRT:** Cyber Security Incident Response Team—multi-disciplinary responders activated per this procedure.
* **Incident Commander (IC):** Person leading the response operationally (typically the Incident Handler/IR Manager); accountable for tactical decisions.
* **Major Incident:** Severity 1 or 2 incident (see §6) requiring executive visibility and coordinated response.
* **Evidence:** Any data, artifact, or record relevant to the incident (e.g., disk images, memory captures, logs, screenshots, emails, tickets).

# 5. Roles & Responsibilities

Maintain a current roster with primary/secondary contacts and 24×7 methods. Consider role cards/battle cards for quick reference.

**Executive Sponsor / SEMT (as needed)**

* Provide strategic direction, risk appetite decisions (e.g., service shutdown, ransom posture consistent with policy/law), resource allocation, and stakeholder oversight.

**CISO / Incident Owner**

* Accountable executive for cybersecurity. Authorizes plan activation, external notifications, and risk trade-offs. Approves major communications.

**Incident Commander (IC) / Incident Handler**

* Leads end-to-end response; sets objectives per phase; runs war room; coordinates workstreams; ensures documentation completeness; enforces evidence preservation; requests executive decisions.

**Security Operations (SOC) / Detection & Analysis**

* Monitors controls, triages alerts, declares incidents per criteria, enriches with threat intel, assigns initial severity, and opens the incident record.

**Forensics & Threat Intel**

* Collects and preserves evidence (chain of custody), performs root cause, scope, and attribution analysis; recommends eradication/hardening.

**IT Operations / Platform & Network**

* Executes containment, eradication, and recovery actions (e.g., segmentation, isolation, patching, re-imaging, restores). Validates service health.

**Privacy / Legal**

* Advises on regulatory thresholds and timelines; preserves privilege; coordinates with law enforcement/regulators; reviews comms; manages discovery holds.

**Communications / PR**

* Drafts and releases internal/external statements, customer notices, and FAQ; manages media inquiries; runs status cadence.

**HR**

* Supports cases involving personnel; coordinates employee notices and training follow-ups.

**Vendor Management / Third‑Party Risk**

* Engages affected service providers; validates contractual obligations for logs, assistance, and notifications.

**Service Desk / Business Units (First Responders)**

* Report suspected incidents; collect initial facts; avoid destructive actions; support containment/recovery under IC direction.

**RACI (summary)**

* **Accountable:** CISO (overall), IC (execution)
* **Responsible:** SOC, IT Ops, Forensics, Comms, Legal/Privacy
* **Consulted:** Business Owners, Risk/Compliance, Vendor Mgmt, HR
* **Informed:** Executives/Board, Employees, Customers (as applicable)

# 6. Incident Classification & Severity

Severity drives activation, comms cadence, and response SLAs. Categories can be multi-select and may change as new facts emerge.

## 6.1 Categories (examples)

Unauthorized access; data breach/exfiltration; malware/ransomware; DDoS/availability; BEC/fraud; insider misuse; vulnerability exploitation; supply chain / third‑party compromise; lost/stolen device/media; cloud misconfiguration.

## 6.2 Severity Matrix

| **Severity** | **Business Impact (examples)** | **Typical Actions** | **Initial Targets** |
| --- | --- | --- | --- |
| **Sev 1 – Critical** | Widespread disruption of critical services; confirmed sensitive data exfiltration; regulator/press attention likely | Full CSIRT activation, executive bridge within 30 min; immediate containment; legal & comms engaged; 24×7 operations | **TTA:** IC ≤15 min, Exec ≤30 min; hourly updates |
| **Sev 2 – High** | Significant impact to key services or high‑risk data; lateral movement suspected; multiple business units affected | CSIRT activation; focused containment; enhanced monitoring; prepare external notifications | **TTA:** IC ≤30 min; updates every 2–4 h |
| **Sev 3 – Medium** | Limited impact; isolated systems/users; partial data exposure not sensitive | IR lead & SMEs engaged; targeted containment/eradication; BAU comms via ticket | **TTA:** IC ≤4 h; daily updates |
| **Sev 4 – Low** | Minimal impact; no persistence; policy violations; scanning/probing | Local handling per playbook; monitor for escalation | **TTA:** IC ≤1 business day |

**Priority** may be adjusted based on regulatory deadlines, fraud risk, or customer impact.

# 7. Activation & Escalation

* **Trigger:** SOC or business detects indicators meeting category/severity thresholds. Any employee may report via [hotline/email/portal].
* **Open Record:** Create an incident in **[IR platform/ticket ID]**; link alerts, assets, and stakeholders.
* **Notify:** Page IC and core CSIRT based on severity; if IC not reachable within SLA, escalate to **[delegate]**; cascade per on-call tree.
* **War Room:** Stand up a secure collaboration space (virtual + out‑of‑band) and dedicated comms bridge; restrict to need‑to‑know; enable recording of decisions and timelines.

**Escalation Matrix** (tailor)

* Sev 1: IC + Full CSIRT + Execs + Legal/Comms within 30 min.
* Sev 2: IC + CSIRT core; brief Execs within 2 h.
* Sev 3–4: IC + SMEs; notify business owner; no executive bridge unless escalation triggers are met.

**De-escalation:** When impact is contained, no active threat, and monitoring shows stability for [X] hours—IC may de-escalate with CISO concurrence.

# 8. Incident Handling Procedure (PICERL)

The lifecycle is iterative; revisit earlier steps as new information emerges.

**Phase 1 – Preparation (steady state)**

1. Maintain CSIRT roster with primary/secondary contacts and 24×7 methods.
2. Keep IR runbooks/playbooks (e.g., ransomware, BEC, web compromise, insider misuse) current and tested.
3. Ensure logging/telemetry (EDR, NDR, cloud, identity, SaaS) covers critical assets; validate log retention meets investigative and regulatory needs.
4. Pre-stage evidence collection kits and forensics tooling; validate chain‑of‑custody forms.
5. Define out-of-band communications (e.g., alternate chat/bridge/SIMs) and mass notification capability.
6. Align with BCP/DR; validate backup integrity and restoration procedures; perform tabletop and technical exercises at a defined frequency.

**Deliverables:** CSIRT roster; on-call schedule; playbook library; comms matrices; evidence forms; tabletop reports; tool readiness checklist.

**Phase 2 – Identification (Detection & Triage)**

1. **Intake:** Receive alert/report; capture reporter, time, and summary; instruct do‑not‑touch to prevent evidence destruction.
2. **Initial Assessment:** SOC validates signal; gathers indicators of compromise (IOCs), affected accounts/assets, and business context.
3. **Declare Incident:** If criteria met, assign category and initial severity; open/confirm IR record; notify IC per §7.
4. **Scoping Hypothesis:** Draft working theory of entry point, spread, persistence, and impact; list unknowns and data gaps.

**Deliverables:** Incident record; initial timeline; severity; stakeholder list; scoping notes; decision log.

**Phase 3 – Containment**

1. **Short‑Term (Immediate):** Isolate affected hosts, disable compromised accounts/tokens, geofence IPs, block indicators, suspend risky integrations; prefer reversible actions.
2. **Evidence First:** Snapshot volatile data (memory, processes, network connections) before reboot or reimage when feasible.
3. **Long‑Term (Stabilize):** Segment networks, rotate keys/secrets, apply mitigations, enable heightened logging; consider temporary compensating controls (e.g., disable SSO self-enrollment, enforce MFA step‑up).
4. **Decision Points:** Balance business impact versus risk of further compromise; obtain executive approval for high-impact actions.

**Deliverables:** Containment plan, isolation list, evidence register entries, change tickets, and blocklists.

**Phase 4 – Eradication**

1. Remove malware/tools/backdoors; rotate credentials; close exploited vectors (patch/config changes).
2. Hunt for persistence and lateral movement (scheduled tasks, startup items, IAM anomalies, cloud keys, implants).
3. Validate eradication (clean scans, no new alerts, closed egress paths).

**Deliverables:** Remediation checklist, eradication validation results, and updated IOCs.

**Phase 5 – Recovery**

1. Restore systems from trusted backups; re-image where necessary; reintroduce to production in a controlled manner.
2. Monitor closely (heightened logging, tripwires) for **[X]** hours/days post‑restore.
3. Re-enable standard controls and decommission temporary mitigations when safe.

**Deliverables:** Recovery plan; service validation results; handover to operations; incident status change to "Monitoring" then "Closed" when acceptance criteria met.

**Phase 6 – Lessons Learned (Post‑Incident Review)**

1. Within **[≤10 business days]** of closure, hold a blameless review with all stakeholders.
2. Document root cause(s), contributing control gaps, timeline accuracy, and response strengths/weaknesses.
3. Create an **Action Register** with owners and due dates (e.g., control improvements, playbook updates, training needs).
4. Update risk register; inform leadership and, where appropriate, customers/partners of long-term remediations.

**Deliverables:** PIR report, action register, updated documentation, and metrics entry.

# 9. Communications Plan

Treat incident communications as sensitive and confidential, with a need-to-know basis. Use legal privilege where applicable.

**Principles**

* Confirm facts before public statements; coordinate with Legal and CISO.
* Use pre-approved templates for employees, customers, partners, and media.
* Keep executives apprised at a cadence matching severity; avoid speculation.
* Have an out-of-band channel ready in case corporate email/chat is affected.

**Cadence (example)**

* Sev 1: Executive brief within 30 min; hourly status; daily written summary.
* Sev 2: Executive brief within two h; every 2–4 h thereafter.
* Sev 3–4: Daily or as material changes occur.

**Status Report Content**  
Current risk; impacted users/services; timeline; actions taken; next steps; decisions pending; external obligations; requests for resources.

**External Notifications**  
Customers, regulators, law enforcement, insurers, and affected partners/vendors—track who, what, when, and by whom.

# 10. Evidence Handling & Documentation

* Maintain a centralized incident record with: who reported, when, type/category, severity, systems/users affected, actions taken, approvals, communications, attachments, and links to tickets/PRs.
* Preserve evidence following the chain‑of‑custody (unique ID, collector, timestamps, hashes, physical/logical location, handling history). Store in a restricted repository.
* Time‑sync systems (NTP) to support accurate timelines.
* Do not alter or access suspect data beyond what is necessary to collect; when in doubt, consult Forensics.

**Minimum Incident Log Fields**  
Date/time reported; reporter; summary; indicators; scope; decisions; containment actions; eradication actions; recovery steps; communications made; outstanding risks; closure criteria.

# 11. Regulatory, Contractual & Insurance Considerations

* Determine whether breach notification is required (jurisdictional privacy laws, sectoral regulations, contract terms). Engage Privacy/Legal to scope affected personal data and timelines.
* Review cyber insurance policy triggers and notification procedures; preserve insurer privilege requirements.
* If criminal activity is suspected, coordinate with Legal before contacting law enforcement.

# 12. Tooling & Data Sources (Examples)

* **Detection:** SIEM, EDR/NDR, CASB, CSPM, IDS/IPS, email security, WAF, DLP, IAM alerts.
* **Investigation:** EDR live response, forensic imaging, sandboxing, packet capture, cloud audit logs, M365/GWS audit, IAM/SSO logs.
* **Containment/Recovery:** NAC/SD‑WAN controls, firewall ACLs, EDR isolate, MDM quarantine/wipe, golden images, backup/restore, IaC pipelines.
* **Collaboration:** IR platform, ticketing, secure chat/bridge, decision log, comms templates.

# 13. Metrics & Reporting

Track and review at least quarterly:

* Mean Time to Detect (MTTD), Contain (MTTC), Eradicate (MTTE), Recover (MTTRc), Close (MTTClo).
* % incidents by category & severity; % repeat incidents; control failure points.
* % actions closed from PIRs within target.
* Exercise/test coverage and findings.
* Utilize trends to inform prioritization of control improvements and staffing.

# 14. Training, Testing & Continual Improvement

* Conduct tabletop exercises **[≥ annually]** and technical simulations for high-risk scenarios (e.g., ransomware, BEC, third-party compromise).
* After each exercise/incident, update playbooks, this procedure, and training content.
* Maintain an annual readiness checklist (contacts validated, backups tested, tools updated, evidence kits verified, comms templates current).

# 15. Acceptance & Approvals

By approving this document, approvers affirm that teams are resourced and empowered to execute this procedure.

* **CISO:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_
* **CIO/Exec Sponsor:** \_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_

## Appendix A – Triage Intake Form (use in tickets)

**Reporter & Source**: [Name, contact, channel]  
**Date/Time (TZ)**: [YYYY‑MM‑DD hh:mm]  
**Summary**: [What was observed?]  
**Indicators**: [Hashes, IPs, URLs, subjects, usernames]  
**Assets/Users Affected**: [Hosts, apps, accounts]  
**Business Context**: [Criticality, data sensitivity]  
**Initial Actions Taken**: [If any]  
**Requested Urgency**: [Low/Med/High]  
**Attachments**: [Screenshots, logs]

## Appendix B – Communications Matrix (example)

| **Stakeholder** | **Sev 1** | **Sev 2** | **Sev 3** | **Sev 4** | **Channel** | **Template** |
| --- | --- | --- | --- | --- | --- | --- |
| Executive Leadership | 30 min | 2 h | 24 h | – | Phone + Brief | Exec‑Status‑01 |
| Employees | 4 h | 24 h | As needed | – | Email/Intranet | Staff‑Notice‑01 |
| Customers | As required | As required | – | – | Email/Portal | Customer‑Notice‑01 |
| Regulator/LE | Per law | Per law | – | – | Legal channel | Reg‑Notify‑01 |
| Insurer | On trigger | On trigger | – | – | Policy channel | Ins‑Notify‑01 |

## Appendix C – Evidence Register (chain of custody)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Evidence ID** | **Collected By** | **Date/Time (TZ)** | **Source/Location** | **Description** | **Hash/Checksum** |
|  |  |  |  |  |  |

## Appendix D – Action Register (post-incident)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Action** | **Owner** | **Due Date** | **Status** | **Notes/Blockers** |
|  |  |  |  |  |  |

## Appendix E – Severity Triggers (tailor)

* **Sev 1**: Confirmed exfiltration of regulated data; widespread outage of Tier‑0 services; active destructive malware; credible extortion impacting critical services; material fraud in progress.
* **Sev 2**: Lateral movement detected; compromise of privileged account; multiple departments affected; high‑risk misconfiguration exploited.
* **Sev 3**: Single host malware; suspicious authentication patterns; isolated data exposure of non-sensitive data.
* **Sev 4**: Port scans, policy breaches without impact, false positives.

## Appendix F – Quick Checklists

**First Responder (all staff)**

1. Stop interacting with suspicious content/host.
2. Do **not** power‑off/reimage unless directed.
3. Capture what you see (screenshots, filenames, timestamps).
4. Report immediately via [hotline/portal].

**SOC / On‑Call**

1. Validate alert; correlate signals; check criticality.
2. Open incident; assign category/severity; page IC.
3. Start timeline; secure logs; snapshot volatile data (when feasible).
4. Draft initial scoping; propose containment options.

**Incident Commander**

1. Stand up war room; set objectives and cadence.
2. Approve containment; assign workstreams; ensure comms.
3. Track decisions; manage risks and escalations.
4. Define exit criteria for each phase; plan PIR.

**IT Ops**

1. Execute isolation/segmentation.
2. Patch/rotate secrets; reimage/restore.
3. Validate service health; monitor post-restore.
4. Close temporary controls when safe.

**Comms/Legal/Privacy**

1. Prepare internal/external updates; preserve privilege.
2. Assess notification thresholds and timelines.
3. Coordinate with insurer and, if needed, law enforcement.
4. Archive comms artifacts with the incident record.