**Cybersecurity Templates**

**Incident Directory Model**

**August 2025**

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

|  |
| --- |
| **Incident Directory Model** |

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

Contents

[Incident Directory Model 4](#_Toc207233352)

[1. Scope & Applicability 4](#_Toc207233353)

[2. Governance & Roles 4](#_Toc207233354)

[3. Naming & Identification Standards 5](#_Toc207233355)

[4. Top-Level Directory Taxonomy 5](#_Toc207233356)

[5. Per‑Incident Folder Structure (Under /10\_LIVE\_INCIDENTS and /20\_CLOSED\_INCIDENTS) 6](#_Toc207233357)

[6. Metadata Model (Per‑Incident Record) 8](#_Toc207233358)

[7. Access Control, Security & Privacy 8](#_Toc207233359)

[8. Working Conventions 9](#_Toc207233360)

[9. Retention & Disposition 9](#_Toc207233361)

[10. Operational Setup (How to Implement) 9](#_Toc207233362)

[11. Metrics & Health 10](#_Toc207233363)

[12. Templates (Drop‑in Forms) 10](#_Toc207233364)

[12.1 Incident Intake & Directory README (paste into 00\_README.md) 10](#_Toc207233365)

[12.2 Chain‑of‑Custody Form (for /00\_EVIDENCE/01\_CHAIN\_OF\_CUSTODY/) 11](#_Toc207233366)

[12.3 Decision Log (for /70\_APPROVALS\_AND\_DECISIONS/) 11](#_Toc207233367)

[12.4 Situation Report (SITREP) Mini‑Template (for /80\_REPORTS\_AND\_SITREPS/) 11](#_Toc207233368)

[12.5 Contact & Call‑Tree Table (for /40\_CONTACTS\_AND\_ROLES/) 11](#_Toc207233369)

[12.6 Assembly Locations (if applicable) 11](#_Toc207233370)

[13. Escalation & Declaration Aids (Reference) 12](#_Toc207233371)

[14. Closeout Checklist (store in /90\_CLOSEOUT/) 12](#_Toc207233372)

[15. Version Control & Change History 12](#_Toc207233373)

# Incident Directory Model

**Purpose**  
Define a consistent, auditable **directory structure, metadata model, and working conventions** for storing and managing all incident artifacts from detection through lessons learned. This model ensures that responders can quickly find the correct information, leadership has a reliable status, evidence is preserved, and compliance requirements are met.

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

# 1. Scope & Applicability

Applies to all **cybersecurity and technology incidents** handled by [Organization], including third-party incidents where [Organization] retains accountability. Covers on-prem, cloud, and SaaS environments. Excludes physical-only incidents unless they affect information systems or regulated data.

**Interfaces:** Incident Handling SOP (PICERL), Major Incident Mgmt, Business Continuity/DR, Communications/PR, Legal/Privacy, Risk Mgmt, Change Mgmt, Knowledge Mgmt.

# 2. Governance & Roles

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Access** |
| **Directory Steward (Records Manager)** | Maintains this model; performs monthly quality checks; enforces retention and access rules. | Full |
| **Incident Handler (Lead)** | Creates incident directories; ensures metadata completeness; approves evidence sealing. | Incident‑specific |
| **Evidence Custodian (Forensics)** | Manages /00\_EVIDENCE subtree; hashes, chain‑of‑custody forms; controls sharing. | Restricted |
| **Communications Lead** | Publishes SITREPs; maintains /60\_COMMS and external statements. | Incident‑specific |
| **Legal/Privacy** | Oversees confidentiality, discovery, breach notification, and records. | Incident‑specific |

**RACI:** Directory Steward = Accountable; Incident Handler = Responsible for per‑incident structure; Legal/Privacy = Consulted; Audit/Exec = Informed.

# 3. Naming & Identification Standards

* **Incident ID:** INC‑[YYYY]‑[####] (zero-padded). Example: INC‑2025‑0123.
* **Folder Prefixing:** Two-digit order codes to keep consistent sort order (e.g., 10\_, 20\_). Avoid spaces; use \_ separators.
* **Datetime:** UTC in ISO‑8601, e.g., 2025‑08‑27T14:30Z.
* **File Names:** [INC‑ID]\_[artifact]\_[phase]\_[vX.Y]\_[YYYY‑MM‑DD]T[HHMM]Z.[ext].  
  Example: INC‑2025‑0123\_SITREP\_containment\_v1.2\_2025‑08‑27T1430Z.docx.
* **Classification Tags:** Public/Internal/Confidential/Restricted included at record level; no sensitive data in file names.

# 4. Top-Level Directory Taxonomy

Create the following top-level folders in the incident repository (e.g., SharePoint/Drive/Confluence/Git‑LFS/ECM). Do **not** delete or renumber.

* /00\_GOVERNANCE
* /10\_LIVE\_INCIDENTS
* /20\_CLOSED\_INCIDENTS
* /30\_KNOWLEDGE\_BASE
* /40\_CONTACTS\_AND\_ROLES
* /50\_FORMS\_AND\_TEMPLATES
* /60\_REPORTS\_AND\_METRICS
* /70\_EXERCISES\_AND\_READINESS
* /80\_THIRD\_PARTY\_AND\_LEGAL
* /90\_ARCHIVE

**Brief description**

* **00\_GOVERNANCE:** This document; policies; retention schedules; access matrices.
* **10\_LIVE\_INCIDENTS:** One folder per active incident (see §5).
* **20\_CLOSED\_INCIDENTS:** Read-only copies of completed incidents (sealed evidence; see §9).
* **30\_KNOWLEDGE\_BASE:** Playbooks, known errors, FAQs, runbooks.
* **40\_CONTACTS\_AND\_ROLES:** CSIRT org chart, call trees, assembly locations, vendor lists.
* **50\_FORMS\_AND\_TEMPLATES:** Intake forms, SITREP, decision log, chain‑of‑custody, RCA templates.
* **60\_REPORTS\_AND\_METRICS:** KPI dashboards, monthly/quarterly reports, audit packs.
* **70\_EXERCISES\_AND\_READINESS:** Tabletop outputs, drills, lessons learned.
* **80\_THIRD\_PARTY\_AND\_LEGAL:** Contracts, DPAs, insurer, counsel guidance.
* **90\_ARCHIVE:** Time-boxed storage before final disposition.

# 5. Per‑Incident Folder Structure (Under /10\_LIVE\_INCIDENTS and /20\_CLOSED\_INCIDENTS)

Create a subfolder for each incident: INC‑YYYY‑####\_[short‑title]. Inside, create the following standard structure:

INC‑2025‑0123\_PaymentPortal\_AuthBypass/

* 00\_README.md
* 00\_EVIDENCE/
* 01\_CHAIN\_OF\_CUSTODY/
* 02\_LOGS/
* 03\_TRACES\_AND\_PCAP/
* 04\_IMAGES\_AND\_DISK/
* 05\_SCREENS\_ARTIFACTS/
* 10\_INTAKE\_AND\_CLASSIFICATION/
* 20\_CONTAINMENT/
* 30\_ERADICATION/
* 40\_RECOVERY/
* 50\_RCA\_AND\_LESSONS/
* 60\_COMMS/
* 70\_APPROVALS\_AND\_DECISIONS/
* 80\_REPORTS\_AND\_SITREPS/
* 90\_CLOSEOUT/

**00\_README.md (required):**

* Incident ID, Title, Current State, Priority (P1–P4), Severity rationale
* Incident Handler (Lead & Backup), Communications Lead, Evidence Custodian
* Scope summary (services, regions, tenants)
* Assembly/bridge links, war room details, next update time
* Links: ticketing/ITSM, dashboards, detection alerts, RFC/changes

**00\_EVIDENCE/**

* **Chain‑of‑Custody:** form per artifact; signer, date/time (UTC), SHA‑256, storage/label.
* **Logs:** immutable snapshots; time windows noted; exported in text/JSON where possible.
* **Traces & PCAP:** packet captures, flow logs; large files in object store with pointers.
* **Images & Disk:** forensic images; separated and encrypted at rest; access logged.
* **Screens & Artifacts:** screenshots, error payloads, config diffs (redacted as needed).

**10\_INTAKE\_AND\_CLASSIFICATION/**

* Intake form, initial triage notes, detection source(s), first‑seen timestamp (UTC), incident type, suspected data classes, initial impact/urgency, decision log entries.

**20\_CONTAINMENT/**

* Workarounds and interim controls; approvals; monitoring updates; rollback notes.

**30\_ERADICATION/**

* Malware removal steps; credentials rotations; patching/upgrades; provider tickets.

**40\_RECOVERY/**

* Service restore plans; validation/health checks; data reconciliation; smoke tests.

**50\_RCA\_AND\_LESSONS/**

* RCA (5‑Whys/Fishbone/Fault Tree); contributing factors; control gaps; ATT&CK mapping; action items with owners and due dates; lessons and playbook updates.

**60\_COMMS/**

* Internal SITREPs; external statements; regulator/insurer/customer notices; Q&A.

**70\_APPROVALS\_AND\_DECISIONS/**

* Approvals (containment, eradication, recovery, notifications), legal holds, exceptions.
* Decision log (timestamped); risk acceptances with expiry dates.

**80\_REPORTS\_AND\_SITREPS/**

* SITREP versions; incident summaries; executive briefs; board updates.

**90\_CLOSEOUT/**

* Closure checklist, metrics snapshot, residual risk entry, final sign‑offs, archive manifest.

# 6. Metadata Model (Per‑Incident Record)

**Mandatory Fields:**

* Incident ID; Title; Status (New/Triage/Containment/…/Closed); Classification (Public/Internal/Confidential/Restricted); Priority (P1–P4); Severity rationale; Incident Type; Detection Source; First Seen (UTC); Current State; Owner (Handler) + Backup; Communications Lead; Evidence Custodian; Affected Services/CIs; Data Sensitivity; Regulatory Drivers (Y/N + details); Assembly/Bridge; Next Update Due; Linked Records (Incidents/Changes/Risks/KB); Tags.

**Calculated Fields (recommended):**

* Impact band; Urgency level; Time since first seen; Time in state; SLA adherence; Open actions.

**Quality Gates:**

* Create only if **Mandatory Fields** are populated; block closure if RCA or Lessons are missing; block archival if evidence hashes/index are absent.

# 7. Access Control, Security & Privacy

* **RBAC:** Default read access to CSIRT; restrict /00\_EVIDENCE and /80\_THIRD\_PARTY\_AND\_LEGAL to need‑to‑know.
* **Encryption:** Encrypt evidence at rest; encrypt in transit; prohibit emailing raw evidence.
* **PII/PHI/PCI:** Redact where feasible; store regulated data only under /00\_EVIDENCE with enhanced controls.
* **Audit Trails:** Enable access logs; preserve for retention period; quarterly access reviews.
* **Legal Hold:** Custodian flags incident; suspends disposition; records hold scope/dates.

# 8. Working Conventions

* **Time:** Use UTC for all timestamps and filenames.
* **Versioning:** Append vX.Y; major bumps when content materially changes.
* **Decision Log:** Chronological, terse bullet format; include owner, option trade‑offs, rationale.
* **SITREP Cadence:** P1: continuous/hours; P2: hourly; P3: daily; P4: as needed.
* **Tools:** Store links to ticketing/monitoring within 00\_README.md and 80\_REPORTS\_AND\_SITREPS/.

# 9. Retention & Disposition

|  |  |  |
| --- | --- | --- |
| **Artifact Category** | **Default Retention** | **Notes** |
| Incident Records (folder) | Incident close + 3 years | Longer if legal hold/audit requires |
| Evidence (all) | Incident close + 5 years | Hashes + chain‑of‑custody mandatory |
| Communications (external) | Incident close + 7 years | Regulator/customer notifications |
| Metrics & Reports | Rolling 3 years | For trend analysis |

**Disposition Workflow:**

1. Directory Steward runs quarterly report of items due; 2) Legal/Privacy concurrence; 3) Secure deletion; 4) Update archive manifest in 90\_ARCHIVE.

# 10. Operational Setup (How to Implement)

1. **Provision Repository:** Create top‑level taxonomy (§4); enable RBAC groups; enable versioning and immutable storage for /00\_EVIDENCE.
2. **Automate Creation:** Build an “Open Incident” workflow that:
   1. Generates folder tree (§5) from template
   2. Creates 00\_README.md with metadata placeholders (§6)
   3. Seeds SITREP, decision log, and chain‑of‑custody forms (§12)
   4. Applies labels: sensitivity, retention, legal hold (off by default)
   5. Grants role-based permissions.
3. **Sync with ITSM:** Mirror incident ID and status; auto‑update 00\_README.md from ticket fields.
4. **Backups:** Nightly backups for all directories; maintain restore tests quarterly.
5. **Quality Checks:** Monthly RACI review, metadata completeness score, evidence hashing verification.

# 11. Metrics & Health

|  |  |  |
| --- | --- | --- |
| **KPI** | **Definition** | **Target** |
| Metadata Completeness | % incidents with all mandatory fields | ≥ 98% |
| Evidence Integrity | % artifacts with recorded SHA‑256 + custody | 100% |
| SITREP Timeliness | % updates within cadence | ≥ 95% |
| Closure Readiness | % closed with RCA + lessons + approvals | ≥ 95% |
| Archive Hygiene | Items past retention with proper disposition | 100% |

# 12. Templates (Drop‑in Forms)

## 12.1 Incident Intake & Directory README (paste into 00\_README.md)

# [INC‑YYYY‑####] — [Short Title]

\*\*Status:\*\* New / Triage / Containment / Eradication / Recovery / Monitoring / Closed

\*\*Priority:\*\* P1 / P2 / P3 / P4

\*\*Severity Rationale:\*\* [why]

\*\*Handlers:\*\* Lead [name] • Backup [name]

\*\*Comms Lead:\*\* [name]

\*\*Evidence Custodian:\*\* [name]

\*\*First Seen (UTC):\*\* [timestamp]

\*\*Detection Source:\*\* [SIEM/EDR/User/Vendor/Other]

\*\*Summary (≤5 lines):\*\*

\*\*Scope:\*\* [services/regions/tenants]

\*\*Data Sensitivity:\*\* None / Internal / Confidential / Restricted (PII/PHI/PCI/Secrets)

\*\*Assembly/Bridge:\*\* [link]

\*\*Next Update Due:\*\* [UTC time & cadence]

\*\*Linked Records:\*\* [INC/CHG/RISK/KB]

\*\*Key Links:\*\* [dashboards, alerts, runbooks]

## 12.2 Chain‑of‑Custody Form (for /00\_EVIDENCE/01\_CHAIN\_OF\_CUSTODY/)

* Artifact ID / Description
* Source / Collector
* Date/Time (UTC)
* Hash (SHA‑256)
* Location/Label
* Transfers (from/to, date/time, purpose, signatures)
* Access Restrictions

## 12.3 Decision Log (for /70\_APPROVALS\_AND\_DECISIONS/)

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

## 12.4 Situation Report (SITREP) Mini‑Template (for /80\_REPORTS\_AND\_SITREPS/)

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

1. Summary: [plain language]
2. Scope/Impact: [services/users/data]
3. Actions: [done / in‑flight/next]
4. Risks/Needs: [decisions, resources, blockers]
5. Next update: [UTC]

## 12.5 Contact & Call‑Tree Table (for /40\_CONTACTS\_AND\_ROLES/)

| **Role/Team** | **Name** | **Title** | **Work** | **Mobile** | **Alt** | **Email** |
| --- | --- | --- | --- | --- | --- | --- |
| CSIRT Lead |  |  |  |  |  |  |
| Incident Handler (Primary) |  |  |  |  |  |  |
| Incident Handler (Backup) |  |  |  |  |  |  |
| Communications Lead |  |  |  |  |  |  |
| Legal/Privacy |  |  |  |  |  |  |
| Vendor (IR retainer) |  |  |  |  |  |  |

## 12.6 Assembly Locations (if applicable)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Level** | **Name** | **Address** | **City/State/Zip** | **Phone** | **Email** |
| Primary |  |  |  |  |  |
| Secondary |  |  |  |  |  |
| Tertiary |  |  |  |  |  |

# 13. Escalation & Declaration Aids (Reference)

* **Escalation Triggers:** Life/safety risk, critical service outages, regulated data exposure, uncontrolled spread, or legal/regulatory clocks.
* **Declaration Guide:** If the incident meets declaration criteria, document the decision in /70\_APPROVALS\_AND\_DECISIONS/ and notify stakeholders per the Communications Plan.
* **Call‑Tree Activation:** Maintain up-to-date call trees under /40\_CONTACTS\_AND\_ROLES/; record outcomes in Decision Log.

# 14. Closeout Checklist (store in /90\_CLOSEOUT/)

* ☐ RCA complete and approved
* ☐ Lessons captured; playbooks updated
* ☐ Evidence sealed; hashes verified
* ☐ External notifications completed
* ☐ Residual risk recorded & owner assigned
* ☐ Metrics snapshot saved
* ☐ Final executive brief stored
* ☐ Permissions flipped to read‑only
* ☐ Archive manifest updated; retention labels applied

# 15. Version Control & Change History

**Version:** 1.0  
**Prepared by:** [Name, Title]  
**Approved by:** [Approver, Title]  
**Effective Date:** [YYYY‑MM‑DD]

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