**Cybersecurity Templates**

**Incident Report Models**

**August 2025**

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

|  |
| --- |
| **Incident Report Models** |

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

Contents

[Incident Report Models 4](#_Toc207316568)

[Model A — Rapid Incident Report (1‑Page Intake) 4](#_Toc207316569)

[A1. Snapshot 4](#_Toc207316570)

[A2. What Happened (Facts Only) 4](#_Toc207316571)

[A3. Impact (Initial) 5](#_Toc207316572)

[A4. Actions & Next Steps 5](#_Toc207316573)

[A5. Communications & Notifications 5](#_Toc207316574)

[Model B — Standard Incident Report (Operational) 5](#_Toc207316575)

[B1. Administrative 5](#_Toc207316576)

[B2. Timeline of Events 5](#_Toc207316577)

[B3. Technical Details 5](#_Toc207316578)

[B4. Impact & Classification 6](#_Toc207316579)

[B5. Containment, Eradication & Recovery 6](#_Toc207316580)

[B6. Communications Log 6](#_Toc207316581)

[B7. Evidence Register (Summary) 6](#_Toc207316582)

[B8. Root Cause & Lessons 6](#_Toc207316583)

[B9. Close‑Out & Approvals 6](#_Toc207316584)

[Model C — Forensic & Chain‑of‑Custody Annex 7](#_Toc207316585)

[C1. Collection Details 7](#_Toc207316586)

[C2. Analysis Notes 7](#_Toc207316587)

[C3. Legal & Regulatory 7](#_Toc207316588)

[Appendices (Tailor to Your Environment) 7](#_Toc207316589)

[D1. Severity Reference (example) 7](#_Toc207316590)

[D2. Notification Matrix (placeholders) 7](#_Toc207316591)

[D3. Drop‑Down Vocabularies (suggested) 8](#_Toc207316592)

[D4. Field Dictionary (governance) 8](#_Toc207316593)

# Incident Report Models

Three complementary, professional report models you can tailor to your organisation. Use Model A for rapid intake, Model B for full operational reporting, and Model C for forensic or evidence purposes. Bracketed fields are placeholders; checkboxes and tables are intended to be form-fillable.

**How to Use**

1. Pick the model that matches the incident phase and audience.
2. Keep **one Incident ID** across all models.
3. Attach logs, screenshots, hashes, and artifacts; reference them in the Evidence table.
4. Avoid speculation—record facts, timestamps, and sources.
5. On closure, ensure PIR/RCA actions are tracked to completion.

**Shared Header (all models)**

* **Incident ID:** [INC‑YYYY‑####]
* **Title:** [Short, factual]
* **Date/Time First Observed (UTC):** [YYYY‑MM‑DD HH: MM]
* **Date/Time Reported:** [YYYY‑MM‑DD HH: MM]
* **Reported By / Contact:** [Name, role, phone/email]
* **Owner (Incident Lead):** [Name]
* **Business Unit / System Owner:** [Name]
* **Classification:** [Internal / Confidential / Restricted]

# Model A — Rapid Incident Report (1‑Page Intake)

For immediate triage and executive awareness within the first hours.

## A1. Snapshot

* **Severity (Initial):** [Low / Medium / High / Critical]
* **Status:** [Pending / Confirmed / Contained / Recovering]
* **Detection Source:** [User / SOC / EDR / SIEM / Third‑party]
* **Incident Type:** [Phishing / Malware / Ransomware / BEC / Web / DoS/DDoS / Insider / Misconfig / Data Exposure / Other]

## A2. What Happened (Facts Only)

* **Summary (≤120 words):** [What, where, when]
* **Affected Scope:** [Users/Endpoints/Apps/Regions]
* **Known IoCs/TTPs:** [Domains, hashes, IPs; MITRE tags]

## A3. Impact (Initial)

* **Confidentiality:** [None / Limited / Sensitive / Regulated]
* **Integrity:** [None / Minor / Moderate / Major]
* **Availability:** [None / Degradation / Outage]
* **Business Impact (early view):** [Minimal / Moderate / Significant / Severe]

## A4. Actions & Next Steps

* **Containment Taken:** [Isolation, blocks, resets]
* **Immediate Risks Remaining:** [Yes/No + notes]
* **Planned Next Actions (with ETA):** [Bullets]

## A5. Communications & Notifications

* **Stakeholder Updates:** [Time, audience, channel]
* **Regulatory/Customer Notice Needed:** [Yes/No/Assessing]
* **Dependencies/Help Needed:** [Legal, Privacy, Comms, Vendors]

# Model B — Standard Incident Report (Operational)

A complete report for operational recordkeeping, management reporting, and audit.

## B1. Administrative

* **Environment:** [On‑prem / Cloud (provider, account)]
* **Primary Systems/Assets:** [IDs/Hostnames]
* **Data Category:** [Public / Internal / Confidential / Restricted]
* **Linked Tickets/Cases:** [IDs across ITSM/EDR/SIEM]

## B2. Timeline of Events

| **#** | **Timestamp (UTC)** | **Source** | **Event/Action** | **Owner** |
| --- | --- | --- | --- | --- |
| 1 | 2025‑08‑28 10:43 | EDR | Host isolated | SOC |
| 2 | 2025‑08‑28 10:57 | User | Phish reported | Service Desk |
| … | … | … | … | … |

## B3. Technical Details

* **Initial Vector:** [Email / Web / Credentials / Supply chain / Insider / Other]
* **IoCs:** [Domains, URLs, IPs, hashes]
* **TTPs Observed:** [MITRE ATT&CK mapping]
* **Accounts/Identities Affected:** [Users, service accounts]
* **Lateral Movement/Persistence:** [Describe]
* **Data at Risk/Exfil Evidence:** [Yes/No + details]

## B4. Impact & Classification

* **CIA Assessment:**
  + C: [0–3]
  + I: [0–3]
  + A: [0–3]
* **Business Impact:** [Minimal / Moderate / Significant / Severe]
* **Severity (Final):** [Low / Medium / High / Critical]
* **Regulatory Trigger:** [Yes/No + regulation/contract]

## B5. Containment, Eradication & Recovery

* **Containment Actions:** [Steps, timestamps]
* **Eradication Actions:** [Malware removal, patches]
* **Recovery Actions:** [Restores, validation]
* **Validation Checks:** [What verified return to normal]

## B6. Communications Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Timestamp (UTC)** | **Audience** | **Channel** | **Key Message** | **Next Update** |
|  |  |  |  |  |

## B7. Evidence Register (Summary)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item ID** | **Description** | **Source/Tool** | **Collected By** | **Collected At (UTC)** | **Hash** |
|  |  |  |  |  |  |

## B8. Root Cause & Lessons

* **Root Cause:** [Human error / Control failure / Vulnerability exploit / Third‑party / Unknown]
* **Contributing Factors:** [Bullets]
* **Lessons Learned:** [Bullets]
* **Corrective/Preventive Actions:** [Action, owner, due date]

## B9. Close‑Out & Approvals

* **Residual Risk:** [None / Low / Medium / High]
* **PIR Completed On:** [YYYY‑MM‑DD]
* **Approvals:**
  + Incident Lead: [Name, date]
  + System Owner: [Name, date]
  + Security Leader: [Name, date]

# Model C — Forensic & Chain‑of‑Custody Annex

Use when artifacts are collected or external authorities may be involved.

## C1. Collection Details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item ID** | **Asset/Path** | **Description** | **Method/Tool** | **Collector** | **Time (UTC)** | **Hash (Algo)** |
|  |  |  |  |  |  |  |

* **Acquisition Notes:** [Write‑blockers, imaging settings, scope]
* **Preservation:** [Storage location, access controls]
* **Transfers:** [When, to whom, purpose]

## C2. Analysis Notes

* **Triage Findings:** [Screenshots, parsed logs]
* **Timeline Reconstruction:** [Reference event IDs]
* **Malware/Script Analysis:** [Static/dynamic summary]

## C3. Legal & Regulatory

* **Case/Law‑Enforcement Reference:** [If applicable]
* **Disclosure Holds:** [Legal hold IDs]
* **Retention:** [X years / as per policy]

# Appendices (Tailor to Your Environment)

## D1. Severity Reference (example)

|  |  |  |
| --- | --- | --- |
| **Severity** | **Typical Indicators** | **Examples** |
| Low | Limited scope, no sensitive data, contained quickly | Single workstation adware, blocked phishing |
| Medium | Limited outage/data access, no confirmed exfil | Malware on the file server, credential stuffing attempts |
| High | Multi-service impact, suspected data access, or lateral movement | Ransomware on a subnet, admin account compromise |
| Critical | Org-wide outage or confirmed regulated data exfiltration | Widespread crypto‑locker, cloud tenant breach |

## D2. Notification Matrix (placeholders)

| **Trigger** | **Audience** | **Deadline** | **Channel** | **Owner** |
| --- | --- | --- | --- | --- |
| Personal data breach | Regulator | 72h (jurisdictional) | Portal | Privacy/DPO |
| Service outage (SLA) | Customers | Contractual | Status page/email | Comms |
| Payment data exposure | Card brands/Acquirer | Per PCI | Program contact | Legal |

## D3. Drop‑Down Vocabularies (suggested)

* **Incident Type:** Phishing, Malware, Ransomware, BEC, Data Exposure, Web App, DoS/DDoS, Insider, Misconfiguration, Third‑party, Other
* **Detection Source:** User, SOC, SIEM, EDR, MSSP, Third‑party, Law Enforcement
* **Status:** Pending, Confirmed, Contained, Recovering, Resolved, Closed
* **Data Sensitivity:** Public, Internal, Confidential, Restricted

## D4. Field Dictionary (governance)

* **Incident ID:** Unique key across all models.
* **CIA Ratings:** 0–3 scale per dimension; combine with business impact for final severity.
* **Evidence Hash:** Use a consistent algorithm (e.g., SHA-256); record per item.
* **TTPs (MITRE):** Tag techniques to aid trend analysis.