**Cybersecurity Templates**

**Incident Handling Policy**

**August 2025**

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

|  |
| --- |
| **Incident Handling Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy ID:** | [SEC-POL-IR-###] | **Owner:** | [CISO / Head of Security] |
| **Approver:** | [Executive Sponsor] | **Effective date:** | [YYYY‑MM‑DD] |

Contents

[Incident Handling Policy 4](#_Toc207311389)

[1. Purpose 4](#_Toc207311390)

[2. Scope 4](#_Toc207311391)

[4. Policy Statements 4](#_Toc207311392)

[4.1 Governance 4](#_Toc207311393)

[4.2 Preparation 4](#_Toc207311394)

[4.3 Detection & Monitoring 5](#_Toc207311395)

[4.4 Reporting & Escalation 5](#_Toc207311396)

[4.6 Evidence & Forensics 5](#_Toc207311397)

[4.7 Post‑Incident Activities 5](#_Toc207311398)

[4.8 Compliance & Enforcement 5](#_Toc207311399)

[5. Roles & Responsibilities 5](#_Toc207311400)

[6. Incident Lifecycle & Time Targets 6](#_Toc207311401)

[6.1 Classification & Severity (examples) 6](#_Toc207311402)

[6.2 Status Codes 7](#_Toc207311403)

[6.3 Core Activities 7](#_Toc207311404)

[7. Communications 7](#_Toc207311405)

[8. Evidence Handling & Recordkeeping 7](#_Toc207311406)

[9. Third‑Party & Regulatory Interface 7](#_Toc207311407)

[10. Metrics & Continual Improvement 8](#_Toc207311408)

[11. Training & Exercises 8](#_Toc207311409)

[12. Compliance, Exceptions, and Sanctions 8](#_Toc207311410)

[13. Review & Maintenance 8](#_Toc207311411)

[Appendix A — RACI (sample) 8](#_Toc207311412)

[Appendix B — Severity Matrix (tailor) 9](#_Toc207311413)

[Appendix C — Notification Matrix (placeholders) 9](#_Toc207311414)

[Appendix D — Ticketing & Records 10](#_Toc207311415)

[Appendix E — Playbooks Index (examples) 10](#_Toc207311416)

# Incident Handling Policy

# 1. Purpose

To ensure a consistent, timely, and practical approach to information security incident handling that minimizes business impact, preserves evidence, meets legal/regulatory duties, and drives continual improvement.

# 2. Scope

Applies to all [Organisation] personnel (employees, contractors, interns), systems, data, networks, and third-party services processing [Organisation] information. Covers the full incident lifecycle: **prepare → detect → report → assess/triage → contain → eradicate → recover → communicate → close → learn**.

**3. Definitions**

* **Information Security Incident:** A single event or series of events that threatens the confidentiality, integrity, or availability of information or services.
* **Event:** Observable occurrence relevant to system or network operations that may indicate an incident.
* **Personal Data Breach:** [jurisdiction-specific definition; e.g., GDPR Art. 4(12)].
* **RCA:** Root Cause Analysis to identify underlying causes and corrective actions.

# 4. Policy Statements

## 4.1 Governance

* [Organisation] **shall** maintain documented procedures, playbooks, and communication plans supporting this policy.
* Roles, responsibilities, and authorities **shall** be defined, assigned, and communicated.
* Incident records **shall** be classified and handled as confidential.

## 4.2 Preparation

* Maintain an Incident Response Plan (IRP), contact lists, notification matrices, and scenario playbooks (e.g., phishing, ransomware, BEC, data loss, DDoS).
* Conduct training and exercises at least **annually**; lessons learned **shall** feed updates to policy, IRP, and controls.

## 4.3 Detection & Monitoring

* Operate logging and monitoring to detect anomalous activities and alerts across endpoints, network, cloud, applications, and identity systems.
* Use defined **use cases** and thresholds for triage; integrate threat intel where applicable.

## 4.4 Reporting & Escalation

* All personnel **shall immediately** report suspected or confirmed incidents to [Service Desk / SOC] via [email/phone/ticket URL].
* The IR Manager **shall** assign severity and status and initiate response; major incidents trigger [Major Incident / Crisis] processes.
* Authorised roles per the Notification Matrix shall make external notifications (e.g., regulators, customers, law enforcement).

4.5 **Response (Containment → Eradication → Recovery)**

* Respond according to IRP/playbooks with priority on safety, containment, business continuity, and evidence preservation.
* Changes to production during response **shall** follow emergency change procedures with retrospective review.

## 4.6 Evidence & Forensics

* Evidence **shall** be collected, handled, stored, and transferred under a chain‑of‑custody with access controls and integrity checks (e.g., hashing).

## 4.7 Post‑Incident Activities

* For significant incidents, conduct PIR within **10 business days** of closure; document lessons, RCA, corrective actions, and control improvements.
* Track actions to completion and verify effectiveness.

## 4.8 Compliance & Enforcement

* Non-compliance may result in disciplinary action per HR policy. Exceptions require documented risk acceptance and approval by the executive.

# 5. Roles & Responsibilities

Tailor roles to your structure. Use the RACI in Appendix A for task-level mapping.

* **Board / Risk Committee:** Oversight of cyber risk and IR posture.
* **Executive Sponsor:** Approves policy/IRP; ensures resourcing; crisis decision‑making.
* **CISO / Security Lead:** Owns policy/IRP; ensures capability, training, metrics, and continuous improvement.
* **IR Manager (Major Incident Lead):** Runs incident lifecycle; assigns severity/status; coordinates teams; ensures comms and documentation.
* **SOC / IT Helpdesk:** First line intake, triage, containment support, ticket/status updates.
* **System/Data Owners:** Provide SMEs, approve recovery steps, validate service restoration.
* **Privacy / DPO:** Assess personal data breaches; advise on regulatory notifications and data subject communications.
* **Legal / Compliance:** Legal privilege, contracts, law enforcement liaison, regulatory reporting.
* **Communications / PR:** External messaging; media and customer notices.
* **HR:** People matters; staff communications and disciplinary processes.
* **Third‑Party / Vendor Manager:** Coordinates supplier notifications and support; tracks third‑party remediation.
* **All Personnel:** Report promptly; cooperate with investigations; complete training.

# 6. Incident Lifecycle & Time Targets

## 6.1 Classification & Severity (examples)

| **Severity** | **Example Impact** | **Initial Response** | **Exec Notify** | **External Notify** |
| --- | --- | --- | --- | --- |
| Critical | Org-wide outage, regulated data exfiltration, and major ransomware | ≤ 15 min | ≤ 30 min | Per law/contract |
| High | Multi-service degradation, high-risk compromise | ≤ 30 min | ≤ 1 hr | As required |
| Medium | Limited function impacted, contained malware | ≤ 4 hrs | As needed | N/A |
| Low | Minor alert, no impact | Next business day | N/A | N/A |

\*See Appendix C for jurisdictional/contractual specifics.

## 6.2 Status Codes

* **Pending:** Report received; triage in progress.
* **Confirmed:** Incident validated; response underway.
* **Resolved:** Containment/eradication/recovery complete; awaiting PIR close‑out.

## 6.3 Core Activities

1. **Triage & Assess** – validate, classify, assign lead/team.
2. **Contain** – short‑term (isolate), mid‑term (block IoCs), long‑term (hardening).
3. **Eradicate** – remove artifacts; close access; patch; reset creds.
4. **Recover** – restore services/data; validate integrity; monitored return to normal.
5. **Communicate** – internal cadence; stakeholder updates; customer/regulator comms when applicable.
6. **Close & Learn** – PIR, RCA, corrective actions, metrics update.

# 7. Communications

* **Authorised Spokespersons:** [Executive Sponsor], [Comms Lead], [Legal].
* **Cadence:** Critical/High incidents: internal updates at [every 60–120 minutes] until stable; daily thereafter.
* **Channels:** [War room tool], email templates, status page, customer notices.

**Content Principles:** factual, time-boxed, audience-appropriate, no speculation; include what happened, impact, actions, next update time.

# 8. Evidence Handling & Recordkeeping

* Maintain an **Incident Record** (ticket/case) with timeline, decisions, artifacts, and approvals.
* Use an **Evidence Register** with item IDs, description, owner, hash, storage location, and access history.
* Retention: keep records/evidence for **[X years]** or per legal hold.

# 9. Third‑Party & Regulatory Interface

* Maintain a **Notification Matrix** mapping laws, contracts, and regulators to triggers, windows, and channels.
* Vendors: require incident notice and cooperation in contracts; test contact paths.
* Law enforcement engagement requires Legal approval; preserve evidence accordingly.

# 10. Metrics & Continual Improvement

* **KPI examples:** MTTD, MTTR, % incidents by severity, repeat incidents, on‑time notifications, PIR action completion rate.
* **KRI examples:** Unpatched critical vulnerabilities, phishing click-through, and control failure rates.
* Quarterly reporting to [Risk Committee]; trend analysis feeds roadmap.

# 11. Training & Exercises

* Mandatory induction and annual refresher for all personnel; role-based training for the IR team.
* Run at least one tabletop per year and one technical simulation (e.g., ransomware), tracking findings and improvements.

# 12. Compliance, Exceptions, and Sanctions

* Violations may lead to disciplinary action up to termination; contractors are subject to contractual remedies.
* Exceptions require risk assessment, business justification, expiry, and Executive Sponsor approval.

# 13. Review & Maintenance

* Policy review at least annually or upon material changes (org, systems, regulatory landscape, or significant incidents).
* Document changes in **Document Control** and communicate updates.

# Appendix A — RACI (sample)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Task** | **Board** | **Exec** | **CISO** | **IR Mgr** | **SOC/Helpdesk** | **Sys Owner** | **Legal** | **Privacy** | **Comms** | **Vendor Mgr** |
| Maintain policy/IRP | I | A | R | C | C | C | C | C | C | C |
| Triage & classify | I | I | C | A | R | C | C | C | I | I |
| Contain/eradicate/recover | I | I | C | A | R | R | C | C | I | C |
| Regulatory notice | I | A | C | C | I | I | R | R | I | I |
| External comms | I | A | C | C | I | I | C | C | R | I |
| PIR & RCA | I | I | A | R | C | C | C | C | I | I |

# Appendix B — Severity Matrix (tailor)

| **Dimension** | **Low** | **Medium** | **High** | **Critical** |
| --- | --- | --- | --- | --- |
| Confidentiality | Limited internal data | Internal non-sensitive | Personal/Confidential data exposure | Regulated data exfiltration at scale |
| Integrity | Minor incorrect data | Limited records altered | Critical records altered | Widespread/tampering of financial or safety systems |
| Availability | Degradation | Single service outage <4h | Multi-service outage >4h | Org-wide outage; safety/critical ops impacted |
| Business Impact | Minimal | Moderate | Significant | Severe/Existential |
| Notification | None | Contractual | Contractual/Regulatory | Mandatory regulatory/customer notices |

# Appendix C — Notification Matrix (placeholders)

| **Trigger** | **Jurisdiction / Contract** | **Deadline** | **Channel** | **Owner** |
| --- | --- | --- | --- | --- |
| Personal data breach | [GDPR/Local] | 72h | DPA portal | DPO |
| Payment card data exposure | [PCI DSS] | [As required] | Acquirer/Brands | Legal |
| Critical service outage (SLA) | [Customer contract] | [e.g., 1h] | Customer portal/email | Comms |
| Law enforcement | [As needed] | N/A | Police liaison | Legal |

# Appendix D — Ticketing & Records

* **Ticket fields:** ID, reporter, timestamps, summary, assets, indicators, severity, status, actions, approvers, evidence links.
* **Statuses:** Pending → Confirmed → Resolved → Closed.
* **Retention:** [X years]; privacy redaction rules as applicable.

# Appendix E — Playbooks Index (examples)

* Phishing / Account Compromise
* Ransomware / Wiper
* Malware / EDR Detection
* BEC / Fraud Attempt
* Data Loss / Exfiltration
* DDoS / Availability Attack
* Third‑Party / SaaS Breach

**Appendix F — Related Documents & References**

* Information Security Policy; Access Control Policy; Business Continuity / DR Plans; Change Management SOP; Privacy Policy.
* Incident Response Plan (IRP) and Scenario Playbooks.
* [Local legal/regulatory references and contracts].