**Cybersecurity Templates**

**Incident Urgency Classification Checklist**

**August 2025**

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

|  |
| --- |
| **Incident Urgency Classification Checklist** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** | 1.0 | **Prepared by:** | [Name/Role] |
| **Approved by:** | [Name/Role] | **Next Review Due:** | [YYYY‑MM‑DD] |

Contents

[Incident Urgency Classification Checklist 4](#_Toc207228438)

[1. Safety & Immediate Escalation Gate 4](#_Toc207228439)

[2. Detection Context 4](#_Toc207228440)

[3. Impact Scoring (I) 5](#_Toc207228441)

[4. Threat & Spread Potential (T) 5](#_Toc207228442)

[5. Containment Status (C) 6](#_Toc207228443)

[6. Time Sensitivity Drivers (U) 6](#_Toc207228444)

[7. Compute Urgency Level 7](#_Toc207228445)

[8. Derive Priority (Impact × Urgency) 7](#_Toc207228446)

[9. Notifications & Escalation 7](#_Toc207228447)

[10. Situation Snapshot (for SITREP) 8](#_Toc207228448)

[11. Evidence & Documentation Quick‑Checks 8](#_Toc207228449)

[12. Interim Control (Workaround) Summary 8](#_Toc207228450)

[13. Hand‑offs & Next Actions 8](#_Toc207228451)

[14. Close or Re-classify 8](#_Toc207228452)

[Appendices – Ready‑to‑Use Inserts 9](#_Toc207228453)

[Appendix A — Severity & Priority Definitions (Customize) 9](#_Toc207228454)

[Appendix B — Example Thresholds (Edit to Fit) 9](#_Toc207228455)

[Appendix C — Initial Investigation Questions (Prompt Sheet) 9](#_Toc207228456)

[Appendix D — Situation Report (SITREP) Mini‑Template 9](#_Toc207228457)

[Appendix E — Evidence Register (Quick Table) 10](#_Toc207228458)

[Appendix F — Roles & Contacts (Fill‑in) 10](#_Toc207228459)

# Incident Urgency Classification Checklist

**Purpose**   
This checklist helps responders quickly and consistently determine **incident urgency** (how fast we must act) and derive the correct **priority** when combined with impact. Use at first contact and update as new facts become available.

# 1. Safety & Immediate Escalation Gate

**Goal:** Identify any life‑safety or critical‑infrastructure risk that bypasses routine scoring.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Check** | **Yes** | **No** | **N/A** | **Notes** |
| 1.1 | Threat to life/safety or public emergency? (e.g., critical healthcare/OT system degradation) | ☐ | ☐ | ☐ |  |
| 1.2 | Ongoing data destruction/encryption (ransomware, wiper) in progress? | ☐ | ☐ | ☐ |  |
| 1.3 | Active exfiltration or confirmed unauthorized access to restricted data? | ☐ | ☐ | ☐ |  |
| 1.4 | Legal/regulatory deadline within ≤ 72h triggered (e.g., breach notice)? | ☐ | ☐ | ☐ |  |

If any 1.1–1.4 = Yes → Set Urgency = Critical and trigger emergency communications/escalation. Proceed, but do not wait for full scoring.

# 2. Detection Context

**Goal:** Capture essential context for triage.

* **First Seen (UTC):**
* **Detected By:** SIEM ☐ EDR ☐ User Report ☐ Vendor ☐ Other:
* **Current State:** Ongoing ☐ Contained ☐ Eradicated ☐ Monitoring ☐ Unknown ☐
* **Affected Services/Assets (IDs/CI links):**
* **Initial Classification (type):** Phishing ☐ Malware ☐ Ransomware ☐ BEC ☐ Unauthorized Access ☐ DDoS ☐ Data Breach ☐ Other:

# 3. Impact Scoring (I)

**Goal:** Quantify business/security effect. Tick one per row; add points.

|  |  |  |
| --- | --- | --- |
| **Dimension** | **Criteria** | **Points** |
| **Service Availability** | No user impact | 0 |
|  | Degradation affecting non-critical service | 1 |
|  | Outage or severe degradation of critical service | 3 |
| **Data Sensitivity** | Public/Low sensitivity | 0 |
|  | Internal/Confidential (no regulated data) | 1 |
|  | Regulated/Restricted (PII/PHI/PCI/secrets) involved/suspected | 3 |
| **Customer/User Impact** | < 100 users / small cohort | 1 |
|  | 100–10,000 users / major cohort | 2 |
|  | > 10,000 users / external customers or multiple tenants | 3 |
| **Financial/Contractual** | Negligible | 0 |
|  | SLA/OLA risk or material operational cost | 2 |
|  | Reportable loss/exposure or revenue at risk | 3 |
| **Reputation/Media** | None likely | 0 |
|  | Elevated stakeholder concern | 1 |
|  | High public/media interest | 2 |

**Impact Score (I):** Sum points → I = [ ]  
**Impact Band:** 0–2 = Low | 3–6 = Medium | 7–11 = High

# 4. Threat & Spread Potential (T)

**Goal:** Understand adversary capability and progression risk.

| **Check** | **Yes** | **No** | **N/A** | **Notes** |
| --- | --- | --- | --- | --- |
| Evidence of lateral movement/persistence/C2 | ☐ | ☐ | ☐ |  |
| Privileged account compromise | ☐ | ☐ | ☐ |  |
| Exploitation of zero-day/novel TTP | ☐ | ☐ | ☐ |  |
| Multiple geos/tenants impacted. | ☐ | ☐ | ☐ |  |

**Threat Factor (T):** Count Yes answers → 0 = Low | 1–2 = Medium | 3–4 = High

# 5. Containment Status (C)

**Goal:** Determine the level of control in the situation now.

|  |  |  |
| --- | --- | --- |
| **Status** | **Definition** | **Points** |
| **Strong** | Contained with high confidence; controls validated; no spread in last 24h | 0 |
| **Partial** | Some controls in place; residual risk of spread remains | 1 |
| **Uncontrolled** | No effective containment; spread/impact likely | 3 |

**Containment Score (C):** [0/1/3]

# 6. Time Sensitivity Drivers (U)

**Goal:** Capture urgency factors independent of impact.

| **Driver** | **Criteria** | **Points** |
| --- | --- | --- |
| **Regulatory Clock** | No external deadline | 0 |
|  | Contractual/regulatory notice ≤ 72h | 3 |
| **Operational Window** | Off-peak; workaround viable | 0 |
|  | Near/within peak trading/operations | 2 |
| **Dependency Risk** | Isolated system | 0 |
|  | Risk to upstream/downstream critical dependencies | 2 |

**Urgency Base (U):** Sum points → U = [ ]

# 7. Compute Urgency Level

Use **T**, **C**, and **U** to derive the **Urgency Level**.

1. **Threat Modifier M(T):** Low=0, Medium=+1, High=+2
2. **Containment Modifier M(C):** Strong=0, Partial=+1, Uncontrolled=+2
3. **Raw Urgency RU = U + M(T) + M(C)**
4. **Urgency Level:** RU 0–1 = **Low**, 2–3 = **Medium**, ≥4 = **High/Critical** (if any §1 gate was Yes → **Critical**)

**Calculated Urgency:** Low ☐ Medium ☐ High ☐ Critical ☐ (RU = [ ])

# 8. Derive Priority (Impact × Urgency)

Crosswalk **Impact Band** (from §3) with **Urgency Level** (§7).

|  |  |  |  |
| --- | --- | --- | --- |
| **Impact Band** | **Urgency: Low** | **Urgency: Medium** | **Urgency: High/Critical** |
| **Impact: Low** | P4 | P3 | P2 |
| **Impact: Medium** | P3 | P2 | P1 |
| **Impact: High** | P2 | P1 | **P1** |

**Resulting Priority:** P1 ☐ P2 ☐ P3 ☐ P4 ☐  
**SLA Targets (fill from IR Plan):** P1: Response ≤ [x] min; Update cadence [y] min; Target containment [z] h.

# 9. Notifications & Escalation

|  |
| --- |

**Notifications & Escalation Triggers**

Check the actions required for the chosen **Priority**.

* **P1 (Critical/High):**
  + Notify: CIRT Lead, Exec/SEMT, Legal/Privacy, Comms ☐
  + Stand up bridge/war room; assign scribe ☐
  + Issue initial SITREP within [30] min ☐
  + Consider disaster/BC invocation if facilities/people/tech impacted ☐
* **P2 (High/Medium):**
  + Notify: CIRT + Service Owner ☐
  + SITREP within [60] min; updates [hourly] ☐
* **P3/P4 (Medium/Low):**
  + Track in ticket; notify service owner; schedule next review ☐

**External Notifications (if applicable):** Regulator ☐ Law Enforcement ☐ Insurer ☐ Customers/Partners ☐  
**Deadlines:** [entity / due / owner]

# 10. Situation Snapshot (for SITREP)

* **What we know:** [facts only, time-stamped]
* **What we’re doing:** [containment/eradication actions]
* **What we need:** [people/tools/access/approvals]
* **What’s next:** [near-term plan and time of next update]

# 11. Evidence & Documentation Quick‑Checks

* Incident log started; time‑stamps in UTC ☐
* Evidence indexed with SHA‑256; chain‑of‑custody notes ☐
* Key artifacts captured (logs, metrics, traces, configs, PCAPs, payload samples) ☐
* Decision log maintained; comms archived per policy ☐

# 12. Interim Control (Workaround) Summary

* **Objective:**
* **Steps (reversible):**
* **Risk & Side‑effects:**
* **Monitoring added:**
* **Removal criteria/expiry:**
* **Approved by:** [Incident Handler / Service Owner]

# 13. Hand‑offs & Next Actions

* Assigned **Incident Handler:**
* **Bridge/Channel:**
* Next update due: [time]
* Required approvals: [CAB/Change? yes/no]
* Owner(s) for remediation items: [names]

# 14. Close or Re-classify

* Conditions to **de-escalate** met? (containment, no spread, reduced impact)
* Conditions to **escalate** met? (new data class, wider scope, miss on SLA)
* **Re‑classification:** Priority updated to P[ ] — reason:
* **Closure** (when resolved): record final urgency/impact, lessons, and link PIR.

# Appendices – Ready‑to‑Use Inserts

## Appendix A — Severity & Priority Definitions (Customize)

* **P1 (Critical):** Immediate coordinated response; executive visibility; continuous updates; legal/comms engaged.
* **P2 (High):** Swift response; hourly updates; cross-team coordination.
* **P3 (Medium):** Business‑hours response; daily updates.
* **P4 (Low):** Planned response; backlog item.

**Impact Bands**

* **High:** Critical services down; regulated data exposure suspected/confirmed; material financial or regulatory risk.
* **Medium:** Noticeable user impact; internal/confidential data at risk; limited financial/reputation concerns.
* **Low:** Minimal user impact; no sensitive data; easily reversible.

## Appendix B — Example Thresholds (Edit to Fit)

* **Data:** Any confirmed access to *Restricted* data ⇒ Impact: High.
* **Availability:** Outage of critical service > 15 min during peak ⇒ Impact High; off‑peak ⇒ Medium.
* **Regulatory:** Any jurisdictional reporting clock started ⇒ Urgency High.

## Appendix C — Initial Investigation Questions (Prompt Sheet)

* Initial intrusion vector? Post-exploitation activity? Persistence? Lateral movement?
* Accounts or tokens compromised (privilege level)?
* Data accessed/exfiltrated? Type/volume?
* What controls failed (prevention/detection/response)?
* Which dependencies or tenants are impacted?

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

1. **Header:** Incident ID, Priority, Time (UTC), Handler, Version #
2. **Summary:** One paragraph, plain language
3. **Scope/Impact:** Services/users/data, confirmed & suspected
4. **Actions:** Done / In‑flight / Next
5. **Risks/Needs:** Decisions, resources, blockers
6. **Next update:** [time]

## Appendix E — Evidence Register (Quick Table)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Details (host/IP/serial/hash)** | **Collected by** | **Date/Time (UTC)** | **Location/Label** |
|  |  |  |  |  |

## Appendix F — Roles & Contacts (Fill‑in)

* CSIRT Lead:
* Incident Handler (Primary/Backup):
* Comms Lead:
* Legal/Privacy:
* Service Owner(s):
* Vendors/Insurer: