**Cybersecurity Templates**

**Problem Handling Checklist**

**August 2025**

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

|  |
| --- |
| **Problem Handling Checklist** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Checklist ID:** | PRB-YYYY-#### | **Owner (Problem Manager):** | [Head of Problem Management] |
| **Environment:** | ☐ Prod ☐ Staging ☐ Dev ☐ Other: | **Related Records:** | Incident(s) # / Change(s) # / Ticket(s) # / KB # |

Contents

[Problem Handling Checklist 2](#_Toc207208177)

[1. Safety & Containment 2](#_Toc207208178)

[2. Problem Definition & Verification 3](#_Toc207208179)

[3. Impact & Risk Assessment 4](#_Toc207208180)

[4. Evidence Capture & Forensics Hygiene 4](#_Toc207208181)

[5.Analysis & Root Cause Exploration 4](#_Toc207208182)

[6.Workaround / Interim Controls 5](#_Toc207208183)

[7. Permanent Fix (Remediation) Readiness 5](#_Toc207208184)

[8. Communication & Stakeholder Management 6](#_Toc207208185)

[9. Compliance & Regulatory Considerations 7](#_Toc207208186)

[10. Validation & Closure Criteria 7](#_Toc207208187)

[11. Lessons Learned & Preventive Actions 8](#_Toc207208188)

[Corrective Action Summary 8](#_Toc207208189)

[Action Log (Decisions & Evidence) 8](#_Toc207208190)

[Appendix A — Common “Gotchas” Quick Check 9](#_Toc207208191)

[Appendix B — Data to Capture (as applicable) 9](#_Toc207208192)

# Problem Handling Checklist

**Purpose:** A practical, end-to-end checklist to guide teams through handling *problems* (recurring errors, systemic defects, service degradations) from detection to closure. Use for non-urgent defects as well as follow-ups after incidents. Aligns with change, risk, and compliance requirements.

**How to Use This Checklist**

1. Work through sections in order. Use **'Yes', No / 'N/A'** and add notes.
2. If any **high-risk** items are marked **No**, pause and create a **Corrective Action** in the summary table. Assign an owner and due date.
3. Capture evidence and decisions in the **Action Log**.
4. Do not close the problem until **the Closure Criteria are satisfied and the Verification Tests** pass.

Severity Gate (select one): ☐ Low ☐ Medium ☐ High ☐ Critical  
If High/Critical, follow the **Escalation & Communication** steps immediately.

# 1. Safety & Containment

**Goal:** Prevent further harm while analysis proceeds.

| **#** | **Control** | **Yes** | **No** | **N/A** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| 1.1 | Immediate containment applied (e.g., feature toggle, throttle, blocklist, isolate node). | ☐ | ☐ | ☐ |  |
| 1.2 | Customer‑visible impact contained or acceptable under current SLA/OLA. | ☐ | ☐ | ☐ |  |
| 1.3 | Access tightened (temporary least‑privilege, token/key rotation if applicable). | ☐ | ☐ | ☐ |  |
| 1.4 | For suspected security defects: evidence preserved, no destructive changes, chain‑of‑custody started. | ☐ | ☐ | ☐ |  |

**Containment summary:**

# 2. Problem Definition & Verification

**Goal:** Make sure we are addressing a *problem* (recurrence/underlying cause) and not a one-off incident only.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Check** | **Yes** | **No** | **N/A** | **Notes** |
| 2.1 | Problem statement written (symptoms, when/where observed, scope). | ☐ | ☐ | ☐ |  |
| 2.2 | Reproduction steps confirmed (or explicit “non-repro” documented with telemetry). | ☐ | ☐ | ☐ |  |
| 2.3 | Affected components/services listed; topology/sequence diagram attached. | ☐ | ☐ | ☐ |  |
| 2.4 | Related incidents/alerts linked; duplicates merged. | ☐ | ☐ | ☐ |  |

|  |
| --- |
|  |
|  |
|  |
|  |

**Definition summary:**

# 3. Impact & Risk Assessment

**Goal:** Quantify the effect on confidentiality, integrity, availability (CIA), operations, and compliance.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Assessment** | **Yes** | **No** | **N/A** | **Notes** |
| 3.1 | User impact quantified (customers, transactions, geos, high‑risk accounts). | ☐ | ☐ | ☐ |  |
| 3.2 | Data sensitivity identified (public/internal/confidential/regulatory). | ☐ | ☐ | ☐ |  |
| 3.3 | SLA/SLO breach risk evaluated; business priority set. | ☐ | ☐ | ☐ |  |
| 3.4 | Safety/health implications considered (e.g., OT/IoT). | ☐ | ☐ | ☐ |  |

**Risk rating:** ☐ Low ☐ Medium ☐ High ☐ Critical  
**Key risks/assumptions:**

# 4. Evidence Capture & Forensics Hygiene

**Goal:** Preserve artifacts for reliable analysis and audit.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Evidence step** | **Yes** | **No** | **N/A** | **Notes** |
| 4.1 | Logs/time-series metrics snapshots saved (pre- and post-containment). | ☐ | ☐ | ☐ |  |
| 4.2 | System state captured (configs, versions, env vars, container image digests). | ☐ | ☐ | ☐ |  |
| 4.3 | Faulting inputs captured safely (PCAPs, payload samples, file hashes). | ☐ | ☐ | ☐ |  |

# 5. Analysis & Root Cause Exploration

**Goal:** Identify contributing and root causes; prioritize the vital few.

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Technique** | **Done** | **Notes/Findings** |
| 5.1 | 5‑Whys or Fishbone (People/Process/Tech/External) completed. | ☐ |  |
| 5.2 | Pareto of error categories drawn from telemetry/cases. | ☐ |  |
| 5.3 | Fault‑tree or sequence timeline drafted. | ☐ |  |
| 5.4 | Hypotheses tested (A/B toggles, canaries, chaos/rollback). | ☐ |  |
| 5.5 | “Could it be…?” checklist (time skew, config drift, cert expiry, capacity, permissions, DNS, dependencies). | ☐ |  |

**Suspected root cause(s):**  
**Contributing factor(s):**

# 6. Workaround / Interim Controls

**Goal:** Reduce impact now, safely.

| **#** | **Control** | **Yes** | **No** | **N/A** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| 6.1 | Workaround documented, risk‑assessed, and approved. | ☐ | ☐ | ☐ |  |
| 6.2 | Rollback/backout plan defined and tested (table‑top ok). | ☐ | ☐ | ☐ |  |
| 6.3 | Monitoring/alerts updated to watch the workaround. | ☐ | ☐ | ☐ |  |

# 7. Permanent Fix (Remediation) Readiness

**Goal:** Implement a robust, auditable fix.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Readiness item** | **Yes** | **No** | **N/A** | **Notes** |
| 7.1 | Change/RFC raised with description, risk, and test evidence. | ☐ | ☐ | ☐ |  |
| 7.2 | Security review completed (static/dynamic tests as applicable). | ☐ | ☐ | ☐ |  |
| 7.3 | Regression tests updated; negative tests added. | ☐ | ☐ | ☐ |  |
| 7.4 | Capacity/performance validated under peak scenarios. | ☐ | ☐ | ☐ |  |
| 7.5 | Rollout plan: order, waves, and maintenance window defined. | ☐ | ☐ | ☐ |  |

# 8. Communication & Stakeholder Management

**Goal:** Keep the right people informed at the right cadence.

| **#** | **Audience / Channel** | **When** | **Owner** | **Notes** |
| --- | --- | --- | --- | --- |
| 8.1 | Internal: on‑call/engineering leaders |  |  |  |
| 8.2 | Cross-functional: support, ops, legal, privacy |  |  |  |
| 8.3 | External: customers/partners (if needed) |  |  |  |
| 8.4 | Exec updates/escalation (if High/Critical) |  |  |  |

# 9. Compliance & Regulatory Considerations

**Goal:** Ensure obligations are met.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Check** | **Yes** | **No** | **N/A** | **Notes** |
| 9.1 | Data classification confirms whether breach/reporting rules apply. | ☐ | ☐ | ☐ |  |
| 9.2 | Statutory notifications assessed (sectoral, cross-border, contractual). | ☐ | ☐ | ☐ |  |
| 9.3 | Evidence retention period set; legal hold applied if required. | ☐ | ☐ | ☐ |  |

# 10. Validation & Closure Criteria

**Goal:** Verify the problem is truly resolved and won’t regress.

| **#** | **Closure test** | **Pass** | **Fail** | **N/A** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| 10.1 | Reproduction test now passes (no symptoms). | ☐ | ☐ | ☐ |  |
| 10.2 | Monitoring indicates normal baselines over the past **X** days. | ☐ | ☐ | ☐ |  |
| 10.3 | No new related incidents for **X** days/releases. | ☐ | ☐ | ☐ |  |
| 10.4 | Security, performance, and reliability checks are green. | ☐ | ☐ | ☐ |  |

**Closure decision:** ☐ Close ☐ Re‑open  
**Approver (name/sign/date):**

# 11. Lessons Learned & Preventive Actions

**Goal:** Make it more complicated for this to happen again.

* What detection failed or was late?
* What automation can prevent recurrence? (guardrails, limits, auto‑rotation, self-healing)
* What documentation or runbooks need updates?
* What training/guidance is required?
* Product/UX changes to reduce user‑error?

**KB/Runbook updates completed:** ☐ Yes ☐ No (link):  
**Backlog items created:** ☐ Yes ☐ No (IDs):

# Corrective Action Summary

Use this table to track all **No** or **High‑risk** findings. Prioritize and assign.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item No. | Risk (L/M/H) | Corrective Action | Owner | Target Date (YYYY‑MM‑DD) | Status |
|  |  |  |  |  |  |

# Action Log (Decisions & Evidence)

Record the most relevant actions and decisions, including links to evidence.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date/Time | Action/Decision | Reference (ticket/change/doc) | Owner | Notes |
|  |  |  |  |  |

**Reviews & Sign‑off**

* **Prepared by:** (name/sign/date)
* **Problem Manager:** (name/sign/date)
* **Technical Reviewer:** (name/sign/date)
* **Service Owner:** (name/sign/date)

**Next review cycle (if left open):** ☐ Weekly ☐ Bi‑weekly ☐ Monthly  
**Archive location for this checklist:**

# Appendix A — Common “Gotchas” Quick Check

* Time sync/drift across components
* Certificate and key expiry
* DNS, routing, firewall, or proxy changes
* Config drift/feature flags/environment mismatch
* Capacity limits (threads, file descriptors, storage, queue depth)
* Permission/role changes
* Third-party dependency degradation

# Appendix B — Data to Capture (as applicable)

* Relevant logs with timestamps/timezone, metric charts, traces
* Build/commit IDs, package, and container versions
* Config diffs before/after
* Screenshots/PCAPs/sample payloads (sanitised)
* Hashes for critical artifacts, storage location, and retention policy