**Cybersecurity Templates**

**Problem Handling Procedure**

**August 2025**

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

|  |
| --- |
| **Problem Handling Procedure** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document ID:** | SOP‑PH‑SEC‑[####] | **Owner:** | [Head of Problem Management] |
| **Approved by:** | [Operations Governance Board Chair] | **Effective date:** | [YYYY‑MM‑DD] |

Contents

[Problem Handling Procedure 3](#_Toc207217999)

[1. Scope & Applicability 3](#_Toc207218000)

[2. Definitions & Abbreviations 3](#_Toc207218001)

[3. Roles & Responsibilities (RASCI) 4](#_Toc207218002)

[4. Triggers & Inputs 5](#_Toc207218003)

[5. Process Overview 5](#_Toc207218004)

[6. Procedure (Step‑by‑Step) 5](#_Toc207218005)

[6.1 Intake & Triage (within one business day) 5](#_Toc207218006)

[6.2 Immediate Containment (as needed) 6](#_Toc207218007)

[6.3 Analysis & Root Cause 6](#_Toc207218008)

[6.4 Known Error (optional but recommended) 6](#_Toc207218009)

[6.5 Permanent Fix (via Change) 7](#_Toc207218010)

[6.6 Verification & Closure 7](#_Toc207218011)

[7. Communication & Escalation 7](#_Toc207218012)

[8. Records, Evidence & Retention 7](#_Toc207218013)

[9. Tools & Techniques 8](#_Toc207218014)

[10. Compliance, Privacy & Security 8](#_Toc207218015)

[11. KPIs & Monitoring 8](#_Toc207218016)

[12. Training & Adoption 8](#_Toc207218017)

[13. Version Control & Change History 9](#_Toc207218018)

[Appendices — Working Aids 9](#_Toc207218019)

[Appendix A — Problem / KE / WA Forms (copy into ITSM or use as intake sheets) 9](#_Toc207218020)

[Appendix B — Communication Templates 10](#_Toc207218021)

[Appendix C — Escalation Matrix (example) 11](#_Toc207218022)

[Appendix D — Checklists (quick use) 11](#_Toc207218023)

# Problem Handling Procedure

**Purpose**  
Establish a consistent, auditable procedure for identifying, analysing, resolving, and preventing **problems** (recurring faults, underlying causes of incidents, systemic security/control failures) across all technology and cybersecurity domains. This procedure integrates with Incident, Change, Risk and Knowledge processes and ensures learning is captured and reused.

**Problem Handling Procedure**

# 1. Scope & Applicability

* **In scope:** All services/systems under [Org] operational control (on-prem, cloud, third-party operated where [Org] retains accountability). Applies to security problems (e.g., misconfigurations, detection gaps, recurring vulnerabilities), reliability problems (availability/performance), and data integrity problems.
* **Out of scope:** One-off incidents resolved without underlying cause; service requests; planned changes; HR/disciplinary matters (refer to HR). When personal data or suspected criminal acts are identified, follow legal/HR guidance in parallel.
* **Interfaces:** Incident Mgmt (inputs); Change Mgmt (permanent fixes); Risk Mgmt (residual risk); Vulnerability Mgmt (CVE/campaign linkage); Knowledge Mgmt (Known Errors/Workarounds).

# 2. Definitions & Abbreviations

* **Problem:** A significant or repeating service/security defect with an identifiable or suspected underlying cause.
* **Known Error (KE):** A problem with a confirmed root cause and a documented workaround; may await a permanent fix.
* **Workaround (WA):** A temporary, risk-assessed measure that reduces impact until a fix is implemented.
* **RCA:** Root Cause Analysis (5‑Whys, Fishbone, Fault Tree, timeline analysis, log/trace correlation).
* **CI:** Configuration Item in CMDB/asset inventory.
* **ATT&CK:** MITRE ATT&CK technique mapping for adversary behaviours (if applicable).
* **MTTPF/MTTR:** Mean Time to Permanent Fix / Mean Time to Resolve.

# 3. Roles & Responsibilities (RASCI)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Role** | **Responsibilities (excerpt)** | **R** | **A** | **S** | **C** | **I** |
| **Problem Manager** | Owns end-to-end process, triage, prioritisation, quality gates, and KPI reporting | **R** | **A** |  | Change, Risk, Legal | Execs |
| **Service Owner** | Accepts impact/priority; funds/approves workaround & fix; owns service outcomes | **R** |  |  | Problem, Change | Stakeholders |
| **CIRT Lead** | Links incidents/evidence; provides threat context and ATT&CK mapping | **R** |  |  | Problem |  |
| **Engineers/SMEs** | RCA, implement workaround/fix, testing, validation | **R** |  |  | Problem |  |
| **Change Manager/CAB** | Approves permanent fix deployments; ensures safe rollout/rollback |  |  | **S** | Problem |  |
| **Knowledge Manager** | Publishes KE/WA; maintains findability/KB quality | **R** |  |  | Problem |  |
| **Records/Legal** | Retention, classification, legal holds, privacy checks |  |  |  | Problem |  |

RASCI: Responsible, Accountable, Support, Consulted, Informed.

# 4. Triggers & Inputs

Open or update a **Problem** when any of the following occur:

* Incident repeat pattern (≥2 occurrences in [30] days) or high business/security impact.
* Confirmed control gap (e.g., missing detection, misconfigured policy) with recurrence risk.
* Vendor defect causing repeated service/security degradation.
* Major incident follow-up reveals unresolved root cause.
* Audit/compliance finding that indicates systemic weakness.

**Inputs:** Incident records, SIEM/SOAR cases, vulnerability findings, audit reports, availability/performance dashboards, and user/customer complaints.

# 5. Process Overview

**Goal:** Contain impact quickly, confirm problem definition, find and fix the root cause safely, and embed learning.

**States:** New → Triage → Analysis → Known Error (optional) → Fix in Progress → Validation → Closed → Archived

**Controls:** Classification at creation; access by role; artifact hashing; mandatory linkages (incidents, changes, CIs/Risks); time-boxed workarounds with removal criteria.

# 6. Procedure (Step‑by‑Step)

## 6.1 Intake & Triage (within one business day)

1. **Create/Update Problem Record** with: title, summary (≤5 lines), owner, service/CI, environment, classification, related incidents/changes/risks, initial severity.
2. **Deduplicate**: search directory/KB; merge if existing problem/KE covers the issue.
3. **Initial Assessment**: rate **Impact/Urgency/Size** (Very High → Very Low); estimate scope (users, regions, versions).
4. **Decide Containment Need**: if immediate risk exists, proceed to 6.2; otherwise, move to Analysis (6.3).

**Outputs:** Problem ID; triage notes; decision on containment; stakeholder notification if High/Critical.

## 6.2 Immediate Containment (as needed)

1. Apply safe interim controls (e.g., feature flag, throttle, access revocation, network block, isolation).
2. Preserve evidence (don’t destroy logs/artifacts); start chain‑of‑custody if potential forensic value.
3. Document **Workaround Draft** (purpose, steps, risk notes, rollback, monitoring additions).
4. Obtain **Problem Manager and Service Owner approval for the interim control; record the** expiry/removal criteria.

**Outputs:** Workaround entry; monitoring/tuning updates; comms to affected teams/customers where applicable.

## 6.3 Analysis & Root Cause

1. **Evidence collection**: logs, metrics snapshots, traces, PCAPs, configs, build numbers, dependency versions.
2. **Reproduce** or characterise symptoms; attach a timeline with UTC timestamps.
3. **RCA method**: 5‑Whys/Fishbone/Fault Tree; corroborate with data. Map to ATT&CK techniques if adversarial.
4. **Scope confirmation**: list affected CIs/services; note data sensitivity and regulatory exposure.
5. **Detection gap** (if any): document why existing controls missed it and propose detection improvements.

**Outputs:** Confirmed/likely root cause(s); contributing factors; ATT&CK mapping; updated risk assessment.

## 6.4 Known Error (optional but recommended)

1. When the cause is confirmed and a safe workaround exists, publish **Known Error (KE)** referencing the Problem ID.
2. Ensure KE is discoverable (search terms, tags), access-controlled, and contains **removal criteria** and **monitoring**.
3. Communicate KE to support/operations and affected engineering teams.

**Outputs:** KE ID; Workaround(s) linked; publication and review dates.

## 6.5 Permanent Fix (via Change)

1. Draft **Fix Strategy** (options, risk analysis, test plan); raise **RFC** with back-out plan and stakeholder impact.
2. Validate in non-prod; gather performance and security test evidence; update runbooks.
3. Execute controlled rollout (waves/canary/blue‑green) within maintenance window if needed.
4. Update documentation, training materials, and monitoring rules.

**Outputs:** Implemented change; updated docs/runbooks; rollback logs (if invoked).

## 6.6 Verification & Closure

1. **Verification tests**: repeat reproduction cases; confirm symptom no longer present.
2. **Telemetry review**: baselines stable for **[X] days/releases**; no related incidents.
3. **Residual risk**: record remaining risk (if any) and acceptance/expiry.
4. **Closure**: mark Problem/KE/WA closed; archive evidence per retention; capture **Lessons Learned**.

**Outputs:** Closure record; lessons learned; detection/rule updates.

# 7. Communication & Escalation

* **Severity gate:** High/Critical problems trigger immediate notification to Service Owner, CIRT Lead, and Operations Leadership.
* **Cadence:** Weekly Problem Review Board (PRB) for open items, risk/ageing, and approvals; monthly trend read‑out to leadership.
* **Stakeholders:** Support, Ops, Product, Legal/Privacy, Communications. External messaging to customers/partners is handled via Communications and Legal/Privacy.

**Templates:** Status update email; KE publication notice; closure note (Appendix B).

# 8. Records, Evidence & Retention

* **Mandatory metadata:** Problem/KE/WA ID, title, owner, service/CI, environment, classification, summary, related records (Incidents/Changes/Risks/KB), created/updated (UTC), status/state dates.
* **Assessment fields:** Impact, Urgency, Size/Effort, Frequency, Data Sensitivity, affected users/customers.
* **Evidence index:** Each artifact with SHA‑256 hash and storage location; chain‑of‑custody where relevant.
* **Retention:** Problem/KE/WA: Active + 3 years; evidence packs aligned; legal hold on request.

# 9. Tools & Techniques

* **Techniques:** 5‑Whys, Fishbone, Fault Tree, Pareto charts, timeline analysis, chaos/experimentation, canary toggles.
* **Tooling:** ITSM (Problem/Change/KB), CMDB/asset inventory, SIEM/SOAR/EDR, APM/metrics, ticketing/ALM, document repository.

# 10. Compliance, Privacy & Security

* Classify records at creation; restrict access to need‑to‑know.
* For data incidents or suspected criminal activity, coordinate with Legal/Privacy and follow incident & notification requirements.
* Ensure fixes do not degrade security posture; perform security tests (static/dynamic) where applicable.

# 11. KPIs & Monitoring

| **KPI** | **Definition** | **Target** |
| --- | --- | --- |
| **Time to Publish KE** | Problem created → KE published (median) | ≤ 2 business days |
| **MTTPF** | KE published → fix validated (median) | ≤ 30 days |
| **Workaround Age** | Active WAs older than threshold | < 10% > 45 days |
| **Recurrence Rate** | Incidents referencing existing KE | ≤ 5% per month |
| **Completeness** | Problem records with mandatory fields | ≥ 98% |

Dashboards will display heat maps by domain, ageing buckets, and top repeaters.

# 12. Training & Adoption

* Onboard engineers/analysts on creating Problems/KEs/WAs and using evidence/indexing standards.
* Publish authoring style guides and classification cheat‑sheets.
* Quarterly RCA clinics featuring best/worst examples; refresh KE library at least quarterly.

# 13. 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 |

# Appendices — Working Aids

## Appendix A — Problem / KE / WA Forms (copy into ITSM or use as intake sheets)

**A1. Problem Record (PR) — Intake Form**

* **PR‑ID:**
* **Title:**
* **Service/CI:**
* **Environment:** Prod / Pre‑Prod / DR
* **Owner:**
* **Classification:** Public / Internal / Confidential / Restricted
* **Summary (≤ 5 lines):**
* **Related:** Incidents [IDs] / Changes [IDs] / Risks [IDs] / KB [IDs]
* **Impact:** Very High / High / Medium / Low / Very Low
* **Urgency:** Immediate / High / Normal / Low
* **Size/Effort:** Very High / High / Medium / Low / Very Low
* **Frequency:** Frequent / Occasional / Rare
* **Data Sensitivity:** None / PII / PHI / PCI / Secrets
* **Symptoms & Indicators:**
* **Scope (assets/regions/versions):**
* **ATT&CK Techniques (if applicable):**
* **RCA Method & Findings:**
* **Detection Gap & Fix:**
* **Fix Strategy & RFC:**
* **Verification & Closure Notes:**

**A2. Known Error (KE) — Publication Form**

* **KE‑ID:** (linked PR‑ID)
* **Title:**
* **Cause Summary:**
* **Workarounds (IDs):**
* **Preconditions:**
* **Steps (reversible):**
* **Risk Notes:**
* **Monitoring Added:**
* **Removal Criteria (date/metric):**
* **Audience/Channels:**
* **Owner / Review Date:**

**A3. Workaround (WA) — Approval Card**

* **WA‑ID:** (linked KE/PR)
* **Purpose:**
* **Steps:**
* **Rollback:**
* **Risk Assessment:**
* **Monitoring:**
* **Owner:**
* **Effective:**
* **Expires/Removal Criteria:**
* **Approved by:** Problem Manager + Service Owner

## Appendix B — Communication Templates

1. **Status Update (Internal)**  
   Subject: [Problem ID] — Status [State] — [Service]  
   Body: Summary (3‑5 lines); Current risk; Next actions & owners; Key dates; Links.
2. **KE Publication Notice**  
   Subject: [KE‑ID] Published — [Service]  
   Body: Cause summary; Workaround; Monitoring; Removal criteria; Who is affected; Contact.
3. **Closure Note**  
   Subject: [Problem ID] Closed — [Service]  
   Body: What happened; Fix deployed; Verification evidence; Lessons learned; Links.

## Appendix C — Escalation Matrix (example)

| **Severity** | **Examples** | **Notify within** | **Approvers** |
| --- | --- | --- | --- |
| Critical | Data exfil suspected; national outage; regulatory deadline risk | 1 hr | CISO, Ops Dir, CAB Chair |
| High | Major customer impact; repeated P1 incidents | 4 hrs | Service Owner, Problem Manager |
| Medium | Limited user impact; a viable workaround exists | 1 day | Service Owner |
| Low | Minimal impact; no SLA risk | PRB | Problem Manager |

## Appendix D — Checklists (quick use)

**E1. Safety & Containment**

* Interim control applied and approved
* Evidence preserved (hash/index)
* Customer/partner impact assessed
* Monitoring updated

**E2. Analysis & RCA**

* Reproduction steps confirmed
* ATT&CK mapping (if applicable)
* Contributing factors listed
* Detection gap documented

**E3. Fix & Validation**

* RFC raised with rollback
* Non‑prod test evidence attached
* Security/regression tests passed.
* Verification complete; residual risk recorded

**Appendix E — Data Dictionary (extract)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Field** | **Description** | **Type** | **Example** |
| Problem ID | Immutable identifier | String | PR‑2025‑00123 |
| Classification | Sensitivity of record | Enum | Confidential |
| Impact | Business effect | Enum(5..1) | High |
| Evidence Hash | Integrity of artifact | String | 9f86d081… |
| ATT&CK | Technique IDs | List | T1059, T1190 |

**Contact:** [Problem Management Office] — [group email]  
**Archive Location:** [ECM/Share path or KB link]