SOP Template: Initial Troubleshooting and Triage Protocols

This SOP defines the **initial troubleshooting and triage protocols** designed to quickly identify, assess, and prioritize issues based on urgency and impact. It includes systematic steps for problem detection, immediate evaluation, categorization of incidents, and the appropriate initial response to ensure efficient resolution and minimize disruption. The goal is to establish a clear framework for frontline personnel to effectively manage incoming problems and escalate them as necessary.

1. Scope

This protocol applies to all frontline personnel responsible for handling initial reports of incidents, problems, or service disruptions.

2. Definitions

- **Incident:** Any unplanned interruption or reduction in the quality of a service.
- **Triage:** The process of prioritizing incoming issues based on urgency and impact.
- **Initial Response:** The set of actions taken before escalation or resolution.

3. Roles & Responsibilities

Role	Responsibilities
Frontline Personnel	Receive, assess, and triage incident reports; perform documented troubleshooting steps.
Supervisor/Lead	Support escalation decisions; review triage accuracy.
Escalation Team	Handle advanced troubleshooting and unresolved critical incidents.

4. Protocol Steps

1. **Detection & Initial Intake**
   - Log all incoming issues with timestamp and reporter details.
   - Confirm receipt with reporter and clarify critical information (who, what, when, where, impact).
2. **Immediate Evaluation**
   - Assess urgency and impact using standard criteria.
   - Determine affected services or systems.
   - Check for related past incidents or known issues.
3. **Categorization & Prioritization**
   - Classify the incident (e.g., hardware, software, network, security).
   - Assign priority (Critical, High, Medium, Low) based on business impact and urgency (see table below).
4. **Initial Troubleshooting**
   - Follow predefined checklists for each incident type.
   - Document all actions and findings in the incident log.
   - If resolved, record resolution and close the incident.
5. **Escalation**
   - If unresolved after initial steps, escalate according to escalation matrix.
   - Ensure all documentation is complete for handoff.
6. **Communication**
   - Update affected stakeholders/customers as per communication guidelines.
   - Record all communications.

5. Prioritization Table

Priority	Description	Response Time	Example
Critical	System-wide outage or severe business impact	15 minutes	Entire network down
High	Major function impaired, many users affected	1 hour	Department unable to access core software

Medium	Limited functions impaired, some users affected	4 hours	Single user unable to print
Low	Minor impact, workarounds available	Next business day	Non-essential software update request

6. Documentation & Record-Keeping

- Log all steps, decisions, and communications in incident management system.
- Use consistent templates for accuracy and traceability.

7. Review & Continuous Improvement

- Regularly review incidents and triage effectiveness.
- Identify trends and update procedures as needed.
- Provide training refreshers to frontline staff.

8. References

- Incident/Problem Management Policy
- Escalation Matrix & Contact List
- Troubleshooting Checklists by System Type