

SOP Template: Incident Ticketing and Resolution Workflow

This SOP describes the **incident ticketing and resolution workflow**, detailing the process for logging, categorizing, prioritizing, and resolving incidents. It ensures efficient tracking and management of issues by defining roles and responsibilities, escalation procedures, communication protocols, and documentation requirements to maintain system reliability and enhance user satisfaction.

1. Purpose

To outline the standardized process for the effective management, tracking, escalation, and resolution of incidents to minimize disruption and ensure continual service improvement.

2. Scope

This SOP applies to all personnel responsible for logging, managing, and resolving incidents within the organization's IT systems and services.

3. Definitions

Term	Definition
Incident	An unplanned interruption or reduction in the quality of an IT service.
Ticket	A record in the incident management system representing the reported issue or request.
Escalation	Process of involving higher-level support personnel or management to address unresolved incidents.
Priority	The level of urgency assigned to an incident based on its impact and urgency.

4. Roles and Responsibilities

Role	Responsibilities
Service Desk Agent	<ul style="list-style-type: none">Log incident tickets with accurate and complete informationPerform initial categorization and prioritizationResolve or escalate incidents as necessaryUpdate users and maintain documentation
Tier 2/3 Support	<ul style="list-style-type: none">Investigate and resolve escalated incidentsCommunicate with Service Desk and usersDocument root cause and resolution steps
Incident Manager	<ul style="list-style-type: none">Monitor incident trends and high-impact issuesCoordinate major incident responseEnsure compliance with SLA and SOP

5. Workflow

1. Incident Detection & Reporting

- Users report incidents via the service portal, email, or phone.
- Automated monitoring tools may also generate tickets.
- 2. Logging**
 - Service Desk logs the incident in the ticketing system, capturing all relevant details.
- 3. Categorization & Prioritization**
 - Apply appropriate category, sub-category, and priority level based on impact/urgency matrix.
- 4. Initial Diagnosis & Resolution**
 - Service Desk performs basic troubleshooting and attempts resolution.
 - If resolved, document solution and close ticket; otherwise, escalate.
- 5. Escalation**
 - Unresolved or high-priority incidents are escalated to Tier 2/3 or Incident Manager as per escalation matrix.
- 6. Resolution & Recovery**
 - Assigned teams investigate root cause, implement the fix, and restore service.
- 7. Communication**
 - Update users and stakeholders on status and resolution progress as per communication protocols.
- 8. Closure**
 - Verify resolution with user, add final documentation, and formally close the ticket.

6. Escalation Procedures

1. Incidents must be escalated to the next support level if not resolved within SLA timelines.
2. High-impact or widespread issues are immediately escalated to the Incident Manager.
3. Escalation matrix must be referenced for contact details and paths.

7. Communication Protocols

- Acknowledge incident receipt to users within 15 minutes of submission.
- Provide status updates per SLA or on request.
- Notify stakeholders of major incidents or delays immediately.

8. Documentation Requirements

- Complete and accurate ticket data including description, categorization, priority, and actions taken.
- All communication and resolution steps must be recorded.
- Root cause analysis for critical or recurring incidents.

9. Review and Continuous Improvement

- Regularly review incident trends and update SOP as necessary.
- Conduct post-incident reviews for major incidents to identify improvements.

10. References

- Incident Management Policy
- Service Level Agreements (SLAs)
- ITIL Best Practices