

SOP Template: Incident Ticket Logging and Categorization Procedures

This SOP details the **incident ticket logging and categorization procedures**, encompassing the systematic recording of incidents, assigning appropriate priority levels, categorizing incidents based on type and severity, and ensuring timely communication with relevant stakeholders. The objective is to streamline incident management, improve resolution efficiency, and maintain accurate records for analysis and reporting.

1. Purpose

To define the process for logging and categorizing incident tickets to ensure consistency, traceability, and effective incident management throughout the organization.

2. Scope

This procedure applies to all employees and contractors responsible for reporting, recording, and managing incidents within the organization's ticketing system.

3. Definitions

- **Incident:** Any unplanned interruption or reduction in the quality of an IT service.
- **Ticket:** A record in the incident management system used to capture details about an incident.
- **Priority:** The level of urgency and impact associated with an incident.
- **Category:** The classification of an incident by type (e.g., hardware, software, network).
- **Stakeholder:** Anyone with an interest in the resolution or progress of the incident.

4. Responsibilities

- **Service Desk Staff:** Initial ticket logging, assignment, and communication.
- **Incident Manager:** Oversight, categorization validation, escalation, and reporting.
- **Technical Teams:** Incident resolution and status updates.

5. Procedure

1. **Incident Detection & Reporting**
 - Incidents can be reported via email, phone, self-service portal, or automatically generated alerts.
2. **Ticket Logging**
 - Enter all relevant incident details into the ticketing system, including:
 - Reporter details (name, contact)
 - Date and time of report
 - Description of the incident
 - Affected systems or services
3. **Prioritization**
 - Assign a priority level based on urgency and impact as per the prioritization matrix:

Priority	Description	Response Time (SLA)
Critical (P1)	Service/application is down or business operations severely impacted	15 minutes
High (P2)	Major functionality affected, workaround unavailable	1 hour
Medium (P3)	Limited impact, users can perform their tasks	4 hours
Low (P4)	Minor issue, does not affect business operations	24 hours

4. **Incident Categorization**
 - Select the most appropriate category and sub-category for the incident (e.g., Network → VPN, Application → Email).

- Assign the incident severity based on its business impact.

5. **Stakeholder Notification**

- Notify relevant parties (e.g., affected users, IT support teams, management) based on incident priority and impact.

6. **Record Keeping**

- Ensure all actions, communications, and updates are logged in the ticket for future reference and reporting.

6. **Related Documents**

- Incident Management Policy
- Service Level Agreement (SLA) Documentation
- Escalation Matrix

7. **Revision History**

Version	Date	Description	Author
1.0	2024-06-01	Initial SOP Template	ITSM Team