

SOP Template: Incident Identification and Ticket Logging Procedures

This SOP details the **incident identification and ticket logging procedures**, outlining the systematic approach for recognizing, documenting, and reporting incidents within an organization. It includes steps for incident detection, initial assessment, accurate ticket creation, prioritization, and assignment, ensuring efficient tracking and resolution. The process aims to enhance communication, maintain incident records, and support timely response to minimize operational disruptions and improve overall incident management.

1. Purpose

To define standardized procedures for the identification, documentation, and logging of incidents to ensure timely and effective response and resolution.

2. Scope

This SOP applies to all employees, contractors, and service providers involved in incident detection and reporting within the organization.

3. Definitions

Term	Definition
Incident	An unplanned interruption to an IT service or a reduction in the quality of an IT service.
Ticket	A record created to document an incident, service request, or problem within the IT Service Management (ITSM) tool.

4. Roles and Responsibilities

Role	Responsibilities
Incident Reporter	Identifies and reports potential incidents.
Service Desk	Receives incident reports, logs tickets, performs initial assessment, and assigns priority/ownership.
Incident Owner	Manages and oversees the progress and resolution of the assigned incident ticket.

5. Procedure

- Incident Identification**
 - Incidents may be reported by users, detected automatically by monitoring tools, or identified by IT staff.
 - All employees are encouraged to report any unplanned service interruptions or quality issues observed.
- Initial Assessment**
 - Service Desk evaluates the reported issue to confirm if it qualifies as an incident.
 - Gather necessary information: affected service, user details, symptoms, and time of occurrence.
- Ticket Logging**
 - Create a new incident ticket in the ITSM/ticketing system immediately after confirming the incident.
 - Include the following details:
 - Date and time of incident
 - Reporter's name and contact information
 - Incident description and impact
 - Status, categorization, and relevant attachments/screenshots
- Prioritization and Assignment**
 - Categorize and assign a priority level based on impact and urgency (see table below).
 - Assign the ticket to the appropriate resolver group or incident owner for investigation.
- Notification and Communication**
 - Notify affected stakeholders as per organizational protocol.
 - Maintain communication and update the ticket with investigation progress and status changes.

Incident Priority Classification Example

Priority	Impact	Urgency	Response Time
Critical	Business-wide	Immediate	15 minutes
High	Departmental	High	1 hour
Medium	User group	Moderate	4 hours
Low	Individual	Low	1 business day

6. Documentation and Record Keeping

- All incident tickets must be stored and tracked within the approved ITSM tool.
- Maintain clear and up-to-date records for auditing, trend analysis, and reporting purposes.

7. Review and Continuous Improvement

- Periodically review incident logs for process improvement opportunities.
- Update this SOP as required to align with new tools, regulations, or lessons learned from past incidents.

Note: Adherence to this SOP ensures consistent incident handling, minimizes response times, and improves organizational resilience.