SOP Template: Incident Escalation and Resolution Workflow

This SOP defines the **incident escalation and resolution workflow**, detailing the systematic process for identifying, reporting, escalating, and resolving incidents within an organization. It includes guidelines for initial incident detection, assessment of severity, escalation pathways, roles and responsibilities of involved personnel, communication protocols, resolution strategies, and documentation requirements. The aim is to ensure timely and effective handling of incidents to minimize impact, improve response efficiency, and prevent recurrence through continuous monitoring and follow-up.

1. Purpose

To establish a systematic approach for identifying, reporting, escalating, and resolving incidents, ensuring prompt mitigation and continuous improvement.

2. Scope

This SOP applies to all staff, contractors, and relevant personnel involved in incident management within the organization.

3. Definitions

- **Incident:** Any event that disrupts normal operations, services, or security.
- **Escalation:** The process of involving higher-level authority or specialized personnel to resolve an incident.
- **Resolution:** Actions taken to restore normal operations and eliminate the root cause.

4. Roles and Responsibilities

Role	Responsibility
Incident Reporter	Identify and report incidents following the defined process.
Incident Manager	Assess, categorize, and coordinate incident management activities.
Support Team	Investigate, troubleshoot, and provide resolution.
Escalation Manager	Oversee escalations, allocate resources, and communicate with stakeholders.
Documentation Officer	Ensure accurate record-keeping and post-incident documentation.

5. Incident Management Workflow

1. **Detection**
    - Incident is detected by monitoring systems, employees, or users.
2. **Reporting**
    - Report incident via designated channels (helpdesk, ticketing system, direct supervisor).
    - Record basic incident details (time, nature, affected systems).
3. **Assessment & Categorization**
    - Assess incident severity (low, medium, high, critical).
    - Categorize incident type and assign priority.
4. **Initial Response**
    - Implement immediate containment actions, if necessary.
    - Notify impacted stakeholders.
5. **Escalation**
    - Escalate incident based on severity and escalation matrix.
      E.g., High/Critical incidents escalated to senior management or specialized teams.
6. **Investigation & Resolution**
    - Diagnose root cause and implement resolution strategies.
    - Document all actions taken during the process.
7. **Communication**
    - Update stakeholders at key milestones and upon resolution.
8. **Closure**
    - Verify successful resolution and restore normal operations.
    - Log incident as closed and conduct post-incident review.

9. **Post-Incident Activities**
    - Document lessons learned, update SOPs or controls as needed.
    - Continuous monitoring for recurrence and improvement opportunities.

6. Escalation Matrix Example

Severity Level	Escalation Path	Response Time
Low	Support Team	Within 8 hours
Medium	Incident Manager	Within 4 hours
High	Escalation Manager & Department Head	Within 1 hour
Critical	Senior Management & Emergency Response Team	Immediate (â‰¤30 minutes)

7. Documentation Requirements

- Maintain incident log with timestamps and actions.
- Record root cause analysis, decision points, and communications.
- Archive supporting evidence and reports.

8. Communication Protocols

- Notify affected parties immediately upon incident detection and at resolution.
- Maintain regular updates for ongoing high/critical incidents.
- Use predefined templates for consistent communication.

9. Review and Continuous Improvement

- Conduct periodic reviews of incident management performance.
- Implement improvements based on lessons learned and feedback.
- Update SOP annually or as needed.

10. References

- Incident Reporting Policy
- Business Continuity Plan
- Risk Management Framework