SOP: Incident Management and Escalation Protocol

This SOP establishes the **incident management and escalation protocol**, detailing the procedures for identifying, reporting, assessing, and responding to incidents in a timely and effective manner. It defines roles and responsibilities, communication channels, severity levels, and escalation paths to ensure incidents are managed efficiently, minimizing impact and facilitating continuous improvement through proper documentation and follow-up actions.

1. Purpose

To ensure effective and timely management of incidents by establishing clear procedures for identification, assessment, communication, escalation, resolution, and documentation.

2. Scope

This protocol applies to all employees, contractors, and relevant parties involved in incident management within the organization.

3. Definitions

- **Incident:** Any unplanned event that disrupts normal operations, services, or security, or has the potential to do so.
- **Escalation:** The process of involving higher levels of management or specialized teams when an incident cannot be resolved at the current level.
- **Severity Level:** A categorization of the impact and urgency of an incident, determining prioritization and escalation path.

4. Roles and Responsibilities

- **Incident Reporter:** Identifies and reports incidents promptly.
- **Incident Manager:** Assesses, classifies, coordinates, and assigns incidents to responders.
- **Response Team:** Investigates, resolves, and documents actions taken for each incident.
- **Management:** Receives escalated incidents, oversees critical incidents, and approves external communications.

5. Incident Lifecycle & Procedure

1. **Identification:**
    - Recognize potential incidents through monitoring, alerts, or user reports.
2. **Reporting:**
    - Report incidents via designated channels (email, hotline, ticketing system).
    - Document all relevant details (time, location, description, impact).
3. **Assessment & Classification:**
    - Incident Manager evaluates the incident and assigns a severity level.
4. **Response & Containment:**
    - Initiate appropriate response based on severity and impact.
5. **Communication:**
    - Inform affected stakeholders and management as required by severity level.
6. **Resolution:**
    - Implement corrective actions and monitor until incident is resolved.
7. **Documentation:**
    - Record all actions, communications, and root cause analysis.

8. **Review & Closure:**
    - Hold post-incident review to identify lessons learned and preventive measures.
    - Formally close the incident record after management approval.

6. Severity Level Matrix

Level	Description	Examples	Initial Response Time	Escalation Path
1 â€“ Critical	Major disruption impacting critical systems or large user base	System outage, data breach, safety threat	15 min	Immediate to senior management and response team
2 â€“ High	Significant impact, but limited in scope; partial system failure	Partial downtime, security incident	30 min	Response team and management within 1 hr
3 â€“ Medium	Moderate impact, workaround available	Performance degradation, minor vulnerabilities	2 hrs	Response team as scheduled
4 â€“ Low	Minor impact, no immediate effect on operations	User inconvenience, cosmetic issues	4 hrs	Track for routine resolution

7. Escalation Process

1. Incident Manager monitors incident progress and triggers escalation according to severity and status.
2. If no resolution within defined time, escalate to the next management level.
3. Critical incidents require immediate involvement of executive management and relevant departments.
4. All escalations must be logged for audit and review purposes.

8. Communication

- Use pre-defined communication channels (email, phone, messaging apps).
- Provide regular status updates to stakeholders according to severity and policy.
- For high/critical incidents, schedule incident conference calls or war rooms as needed.

9. Documentation & Continuous Improvement

- Maintain detailed incident records, including time stamps and actions taken.
- Perform root cause analysis and document lessons learned.
- Implement corrective actions and update SOP as needed.

10. Review and Approval

- This SOP will be reviewed annually or following major incidents.
- All updates require management approval.