Standard Operating Procedure (SOP)

Incident Notification and Escalation Guidelines

This SOP defines **incident notification and escalation guidelines** to ensure timely and effective communication during emergencies or operational disruptions. It covers the identification of incidents, notification procedures, roles and responsibilities for reporting, escalation protocols based on incident severity, communication channels, and documentation requirements. The objective is to minimize impact by enabling prompt response, coordination, and resolution of incidents within the organization.

1. Purpose

To establish a standardized approach for incident notification, reporting, and escalation to ensure effective management and accountability during incidents.

2. Scope

This SOP applies to all employees, contractors, and third-parties involved in supporting the organization's operations and IT systems.

3. Definitions

- **Incident:** Any unplanned event that disrupts or could disrupt normal operations.
- **Severity Levels:**
    - **Level 1 (Critical):** Major disruption affecting multiple users/services, regulatory impact, or safety implications.
    - **Level 2 (High):** Significant disruption to some users/services, potential risk of widespread impact.
    - **Level 3 (Medium):** Minor or localized disruption, little or no impact on service delivery.
    - **Level 4 (Low):** No impact to services, informational or potential issues only.

4. Roles and Responsibilities

Role	Responsibility
Incident Reporter	Identify and report incidents according to the notification procedure.
Incident Manager	Assess, classify, and initiate escalation as necessary; coordinate response efforts.
Escalation Team	Participate in resolution and provide expertise as required by the escalation level.
Communications Team	Ensure timely and clear updates to stakeholders and affected parties.

5. Incident Identification

1. Identify potential or actual incidents through observation, automated monitoring, or reports from users or third-parties.
2. Gather relevant details: date/time, location, impacted services/systems, observed symptoms.

6. Notification Procedures

- Report all suspected or confirmed incidents immediately via designated communication channels (e.g., ticketing system, phone, email, instant messenger).
- Provide essential details (Who, What, When, Where, and Impact).
- For critical incidents, use direct phone calls/SMS to ensure rapid response.

7. Escalation Protocols

Severity Level	Escalation Timeline	Responsible Parties
Critical (Level 1)	Immediate (within 15 minutes)	Incident Manager, Senior Management, IT, Communications
High (Level 2)	Within 1 hour	Incident Manager, Relevant Support Teams
Medium (Level 3)	Within 4 hours	Support Team Lead

Low (Level 4)	Next business day	Support Team

8. Communication Channels

- Primary: Incident ticketing system, official email.
- Secondary: Phone, SMS, instant messenger (for urgent or out-of-hours issues).
- Escalation distribution lists for Level 1 and 2 incidents.

9. Documentation Requirements

- All incidents shall be recorded in the incident management system.
- Document full incident lifecycle: detection, notification, escalation, resolution, communication, and post-incident review.
- Attach all relevant communication logs, evidence, and reports.

10. Review and Continuous Improvement

- Conduct post-incident reviews within 5 business days for Level 1 and 2 incidents.
- Update this SOP annually or following a major incident to incorporate lessons learned.

11. References

- Incident Management Policy
- Business Continuity Plan
- Disaster Recovery Procedures