Standard Operating Procedure (SOP): Incident Escalation and Communication Protocols

This SOP details **incident escalation and communication protocols**, focusing on timely reporting, clear communication channels, roles and responsibilities during incidents, escalation procedures based on severity levels, notification of key stakeholders, documentation requirements, and continuous monitoring. The objective is to ensure effective management of incidents through structured communication and prompt escalation to mitigate risks and facilitate resolution.

1. Purpose

To establish a standardized process for escalating incidents and communicating effectively to ensure rapid response, risk mitigation, and timely resolution.

2. Scope

This SOP applies to all employees, contractors, and stakeholders involved in incident detection, response, and management within the organization.

3. Definitions

- **Incident:** Any event that disrupts normal operations, poses a risk, or requires immediate response.
- **Escalation:** The process of notifying higher-level personnel or management based on incident severity.
- **Severity Levels:** Predefined categories that determine the criticality and response priority of incidents.

4. Roles and Responsibilities

Role	Responsibilities
Incident Reporter	Identify and report incidents promptly using the designated reporting channels.
Incident Manager	Assess incident severity, coordinate response, manage escalation, and ensure communication flow.
Stakeholders	Provide support and resources as required; receive notifications relevant to their domain.
Communication Lead	Draft and disseminate internal/external communications related to the incident.

5. Communication Channels

- Email distribution lists (e.g., *incident@company.com*)
- Incident management system/ticketing tools
- Designated messaging groups (Slack, Teams, etc.)
- Direct phone contacts for urgent escalation

6. Incident Severity Levels & Escalation Procedure

Severity Level	Description	Escalation/Notification Requirement
Critical (Level 1)	Widespread service disruption, data breach, or significant business impact	Immediate notification to executive management, IT, and relevant stakeholders
High (Level 2)	Major functionality impact, not widespread	Notify department management and impacted teams within 30 minutes
Medium (Level 3)	Minor service impact, workaround available	Notify support teams and log in incident tracker within 2 hours

Low (Level 4)	No immediate impact, informational	Document and review during regular team meetings

7. Notification of Key Stakeholders

- Identify impacted stakeholders based on incident type and severity.
- Send incident notification using predefined templates.
- Schedule updates at regular intervals until resolution.
- Escalate to senior management for unresolved or escalated incidents.

8. Documentation Requirements

- Log all incidents in the incident management system.
- Document actions taken, communications sent, and escalation steps.
- Maintain records of timelines and decisions for audit and review.

9. Continuous Monitoring & Review

- Monitor incident progress and update documentation regularly.
- Conduct post-incident reviews to identify improvements.
- Update this SOP as necessary based on lessons learned and changes in organizational structure or technology.

10. References

- Incident Management Policy
- Communication Plan Template
- Business Continuity Procedures

11. Revision History

Date	Version	Description	Author
2024-06-10	1.0	Initial Release	[Your Name]