SOP Template: Downtime Event Categorization and Escalation Guidelines

This SOP defines **downtime event categorization and escalation guidelines**, detailing the process for identifying, classifying, and prioritizing downtime incidents to ensure timely and effective resolution. It includes criteria for event severity levels, roles and responsibilities for escalation, communication protocols, response time targets, and documentation requirements. The objective is to minimize operational disruption by establishing a structured approach to managing downtime events and ensuring appropriate stakeholder involvement based on event impact and urgency.

1. Scope

This SOP applies to all staff involved in incident management for IT systems, critical business applications, and production environments.

2. Definitions

- **Downtime Event:** Any unplanned interruption or degradation of standard service operations.
- **Severity Level:** A rating that indicates the impact and urgency of an incident.
- **Escalation:** The process of involving higher-level personnel or management based on defined triggers.

3. Downtime Event Categorization

Severity Level	Description	Examples
Critical (P1)	Total business outage or loss of critical functions; severe operational impact.	System-wide outage, production line halt, security breach in live systems
High (P2)	Significant reduction in service; notable impact to operations, but partial functionality remains.	Multiple users unable to access core services; major module failure
Medium (P3)	Limited impact; functionality degraded, but workaround is available.	Intermittent issues; minor subsystem failure
Low (P4)	Minimal impact; cosmetic or non-urgent.	Report formatting issue; single non-critical user affected

4. Roles and Responsibilities

- **Incident Owner:** Initial triage, categorization, coordination of resolution, and updating stakeholders.
- **Support Teams:** Troubleshoot, resolve, and communicate the technical aspects of the incident.
- **Management:** Approve escalations, support resource allocation, and communicate with affected business units.
- **Communications Lead:** Distribute timely updates and maintain communication channels.

5. Escalation Guidelines

Severity	Initial Response Time	Escalation Trigger	Escalation Path

Critical (P1)	Within 10 minutes	Immediate upon detection	Notify Incident Owner, Support Team, and Management; escalate to external/vendor support if unresolved after 30 mins
High (P2)	Within 30 minutes	Escalate if unresolved after 1 hour	Notify Incident Owner and Support Team; escalate to Management if unresolved
Medium (P3)	Within 2 hours	Escalate if unresolved after 4 hours	Notify Support Team; escalate to Management if required
Low (P4)	Within 4 hours	Escalate if unresolved after 1 business day	Notify Support Team

6. Communication Protocols

- Initial notification via designated incident management system.
- Stakeholder updates at defined intervals (e.g., every 30 mins for P1, every hour for P2).
- Post-resolution incident summary and root cause analysis shared with stakeholders.

7. Documentation Requirements

- Log all events, actions taken, timestamps, and communications in the incident management system.
- Maintain records for audit and continuous improvement purposes.
- Update knowledge base articles as necessary after resolution.

8. Review and Continuous Improvement

- Conduct post-incident reviews for all P1 and P2 events.
- Update SOP annually or after major incidents to address gaps and improve processes.