SOP Template: Post-Incident Review and Restoration of Operations

This SOP details the **post-incident review and restoration of operations**, focusing on the systematic evaluation of incidents to identify root causes, implement corrective actions, and restore normal business functions efficiently. It includes procedures for incident documentation, team debriefing, assessment of operational impacts, communication protocols, restoration planning, and continuous improvement to enhance organizational resilience and prevent recurrence.

1. Purpose

To ensure a systematic approach to reviewing incidents, identifying lessons learned, restoring operations, and strengthening organizational resilience.

2. Scope

This procedure applies to all staff involved in incident response and recovery, across all business units affected by the incident.

3. Responsibilities

Role	Responsibility
Incident Response Team Lead	Facilitate post-incident review, oversee documentation, and lead restoration efforts.
Department Managers	Report incident impacts, contribute to assessments, implement corrective actions.
IT Support	Restore technical services, validate system integrity, support documentation.
Communications Officer	Coordinate internal and external communications, notifications, and status updates.

4. Procedures

1. **Incident Documentation**
   - Complete incident report capturing timeline, description, actions taken, and personnel involved.
   - Collect logs, screenshots, and relevant evidence for recordkeeping.
2. **Team Debriefing**
   - Assemble incident response team and stakeholders within 24-48 hours post-incident.
   - Discuss incident timeline, decisions made, and challenges encountered.
3. **Assessment of Operational Impacts**
   - Identify affected systems, services, and business functions.
   - Document extent, severity, and ongoing risks.
4. **Root Cause Analysis**
   - Perform structured analysis (e.g., Five Whys, Fishbone Diagram) to determine the root cause.
   - Document findings and evidence supporting conclusions.
5. **Corrective and Preventive Actions**
   - Identify actions to address root causes and prevent recurrence.
   - Assign action items with clear timelines and responsibilities.
6. **Communication Protocols**
   - Update stakeholders on incident status, recovery progress, and restoration plans.
   - Issue internal and (if required) external notifications as per communication guidelines.
7. **Restoration Planning and Execution**
   - Develop and execute step-by-step restoration plan for affected operations or services.
   - Validate restoration and confirm system or service integrity before resuming normal operations.
8. **Continuous Improvement**
   - Update policies, procedures, and training based on lessons learned.
   - Track open action items to closure and review effectiveness of improvements.

5. Documentation and Reporting

- Maintain records of incident reports, meeting minutes, analysis results, and action logs.
- Distribute post-incident report to relevant management and stakeholders.

- Archive records securely according to organizational policy.

6. Review and Update

- SOP to be reviewed annually or after significant incidents.
- Update procedures to reflect improvements and organizational changes.