SOP Template: Remediation and Recovery Procedures

This SOP details **remediation and recovery procedures**, focusing on identifying issues, implementing corrective actions, restoring systems to normal operation, monitoring progress, and preventing recurrence. It ensures a structured approach to addressing problems effectively and minimizing downtime or impact on operations.

1. Purpose

To provide a standardized process for identifying, containing, remedying, and recovering from system issues or incidents with the goal of minimizing business disruption and preventing future occurrences.

2. Scope

This SOP applies to all incidents, issues, or failures affecting critical systems, applications, or infrastructure within the organization.

3. Responsibilities

Role	Responsibilities
Incident Response Team	Coordinate remediation and recovery activities, lead root cause analysis, communicate status updates.
System/Application Owners	Provide technical input, assist in system restoration, validate recovery.
IT Management	Review incident reports, approve corrective actions, and support organizational changes.

4. Procedures

1. **Identification**
   - Detect and document the issue or incident, noting time, scope, and affected systems.
   - Notify relevant stakeholders according to escalation procedures.
2. **Containment**
   - Isolate affected systems as needed to prevent further impact.
   - Implement temporary controls if required.
3. **Remediation**
   - Determine root cause through analysis.
   - Develop and execute corrective action plan (e.g., patching, configuration changes, removal of malicious components).
   - Document all steps taken.
4. **Recovery**
   - Restore affected systems and services to normal operation.
   - Verify system integrity and data consistency.
   - Communicate restoration to stakeholders and users.
5. **Monitoring**
   - Monitor affected systems for signs of recurrence or continued issues.
   - Collect logs and metrics as evidence of successful remediation.
6. **Review & Prevention**
   - Conduct post-incident review (Lessons Learned meeting).
   - Update procedures, controls, or training to prevent recurrence.
   - Document outcomes and recommendations.

5. Documentation

- Maintain detailed records of incidents, actions taken, and communications.
- Store incident reports and related documentation in the designated repository.

6. References

- Incident Response Policy
- Business Continuity Plan
- Change Management Procedure

7. Revision History

Version	Date	Description	Author
1.0	2024-06-10	Initial template release	Admin