SOP Template: Remote Monitoring and Management (RMM) Protocols

This SOP details the **Remote Monitoring and Management (RMM) Protocols**, encompassing procedures for continuous system monitoring, proactive issue detection, automated maintenance tasks, security management, and incident response. The protocols aim to ensure optimal performance, security, and reliability of IT assets through remote access and control, minimizing downtime and enhancing operational efficiency.

1. Purpose

To establish standardized procedures for remote monitoring, maintenance, security management, and incident response for all IT assets utilizing RMM platforms.

2. Scope

Applies to all IT personnel managing company endpoints, servers, and network devices via RMM solutions.

3. Responsibilities

- **IT Administrators:** Oversee implementation and configuration of RMM protocols.
- **Technicians:** Execute routine monitoring, respond to alerts/incidents, and perform maintenance tasks.
- **Security Team:** Review alerts related to security and ensure compliance with security protocols.
- **RMM Platform Vendor:** Provide support and platform updates as required.

4. Procedures

4.1 Continuous System Monitoring

- Deploy RMM agents to all designated assets.
- Configure asset monitoring for CPU, memory, disk, network utilization, and key services.
- Establish and document alert thresholds for all monitored metrics.
- Verify agent communication status at least once daily.

4.2 Proactive Issue Detection

- Enable automated alerts for performance degradation or failure events.
- Review and classify alerts within 30 minutes of receipt during business hours.
- Utilize trend analysis to predict potential hardware and software issues.

4.3 Automated Maintenance

- Schedule and automate patch updates, disk cleanup, and antivirus scans per documented maintenance windows.
- Regularly review automation scripts for efficiency and security.

4.4 Security Management

- Deploy and update endpoint protection via RMM platforms.
- Monitor for vulnerabilities and compliance with security baselines.
- Review RMM access logs weekly for unauthorized access attempts.

4.5 Incident Response

- Escalate critical alerts as per the Incident Management SOP.
- Document incidents with time of detection, actions taken, resolution, and root cause analysis.
- Restore affected systems from backup if required and verify functionality.

5. Documentation and Reporting

- Log all maintenance activities, detected incidents, and RMM changes in the centralized ticketing system.
- Generate and review weekly reports on system health, alert statistics, and resolved issues.

6. Compliance & Review

- Ensure adherence to organizational IT and security policies.
- Review this SOP annually or upon significant changes to the RMM platform or security landscape.

7. Revision History

Version	Date	Description	Author
1.0	2024-06-11	Initial draft	[Author Name]