SOP: Patch Management and Software Updates Schedule

This SOP defines the **patch management and software updates schedule** to ensure all systems and applications are regularly updated with the latest patches and security fixes. It includes identification, testing, deployment, and documentation of patches, aiming to reduce vulnerabilities, enhance system performance, and maintain compliance with organizational security policies. Regular updates are scheduled to minimize disruption and protect IT infrastructure from potential threats.

1. Purpose

To establish a consistent and effective process for managing software updates and patch deployments in order to mitigate security vulnerabilities and maintain operational integrity.

2. Scope

This SOP applies to all servers, desktops, laptops, network devices, and applications owned or managed by the organization.

3. Responsibilities

- **IT Security Team:** Oversight of patch management processes and security compliance.
- **System Administrators:** Identification, testing, deployment, and documentation of patches.
- **Application Owners:** Coordination and validation of updates for proprietary and third-party software.

4. Patch Management Process

1. **Identification**
   - Subscribe to vendor security bulletins and update notifications.
   - Perform weekly scans to detect missing patches and updates.
2. **Assessment and Prioritization**
   - Evaluate the criticality and risk of each patch.
   - Prioritize security patches addressing critical or high-severity vulnerabilities.
3. **Testing**
   - Test patches in a controlled, non-production environment.
   - Document any compatibility or deployment issues encountered during testing.
4. **Deployment**
   - Schedule patch deployment based on criticality and system usage.
   - Notify end-users prior to deployment to minimize disruptions.
   - Deploy patches to production systems per the approved schedule.
5. **Verification**
   - Confirm successful patch installation through automated tools or manual checks.
6. **Documentation**
   - Record all applied patches, issues, and resolutions in the patch management log.
7. **Reporting**
   - Generate and review patch status and compliance reports monthly.

5. Patch Management and Software Updates Schedule

System/Software Type	Frequency	Window	Responsible
Operating Systems (Servers)	Monthly	Second Saturday 10pmâ€“2am	System Administrators
Operating Systems (Workstations)	Monthly	Second Sunday 12amâ€“4am	Desktop Support
Critical Security Patches	As Needed	Within 48 hours of release	System Administrators
Applications (Business Critical)	Quarterly	Third Saturday 9pmâ€“3am	Application Owners/IT
Network Devices (Firmware)	Semi-Annually	As Scheduled	Network Engineers

6. Exception Handling

Exceptions to the patch management schedule must be documented, reviewed, and approved by the IT Security Team. Systems pending updates due to business impact or technical constraints must be reported and mitigated via compensating controls until patched.

7. Records and Documentation

- Maintain a patch management log with installation dates, system details, patch descriptions, and verification status.
- Documentation must be retained for a minimum period in accordance with the organization's compliance requirements.

8. Review and Continuous Improvement

This SOP and associated schedules must be reviewed at least annually or following major security incidents, vendor advisories, or changes in organizational policy. Feedback and lessons learned will be incorporated to strengthen the process.

9. References

- Vendor Patch Documentation
- IT Security Policy
- Regulatory Compliance Requirements (e.g., ISO 27001, NIST 800-53)

10. Approval

Prepared by: _____

Reviewed by: _____
Approved by: _____
Date: _____