SOP: Software Updates and Patch Management

This SOP provides comprehensive **guidelines for software updates and patch management**, covering the identification, evaluation, testing, and deployment of software patches and updates. It aims to ensure systems are securely maintained by minimizing vulnerabilities, reducing downtime, and enhancing overall IT infrastructure reliability. The procedure includes scheduling updates, backup protocols, change management approval, and documentation to maintain compliance and operational stability.

1. Purpose

To establish procedures for the timely identification, evaluation, testing, approval, deployment, and documentation of software updates and patches in order to protect IT systems and maintain compliance.

2. Scope

This SOP applies to all organizational systems, servers, workstations, applications, and network appliances where software updates and patches are applicable.

3. Responsibilities

- **IT Team:** Responsible for implementing this SOP and executing updates and patching activities.
- **System Owners:** Ensure systems comply with update requirements and collaborate in scheduling.
- **Change Management:** Review and approve high-impact changes.
- **Security Team:** Monitor vulnerabilities and verify patch effectiveness.

4. Procedure

1. **Identification**
    - Monitor vendor announcements, security advisories, and vulnerability databases for new patches or updates.
    - Maintain an inventory of all systems and software versions in use.
2. **Evaluation**
    - Assess the criticality and relevance of available patches and updates.
    - Prioritize security and critical updates.
3. **Testing**
    - Test patches and updates in a controlled, non-production environment.
    - Evaluate compatibility and impact on system performance.
4. **Backup Protocols**
    - Ensure recent backups of affected systems/data are available before deployment.
5. **Change Management Approval**
    - Submit change requests for high-risk or critical systems.
    - Obtain necessary approvals and notify relevant stakeholders.
6. **Deployment**
    - Schedule patch deployments during maintenance windows to minimize disruption.
    - Apply updates in accordance with vendor guidelines.
    - Monitor systems post-deployment for any issues.
7. **Documentation**
    - Record patch/update details, dates, affected systems, and outcomes.
    - Maintain records for compliance and audit purposes.

5. Scheduling and Frequency

- Critical updates: Deploy within 48 hours of release.
- Regular (non-critical) updates: Deploy monthly or as recommended by vendors.
- Emergency patches: Deploy immediately following expedited risk assessment and approval.

6. Compliance and Review

- Regularly review and update this SOP to reflect changes in technology and compliance requirements.
- Conduct periodic audits to ensure adherence to the SOP.

7. References

- Vendor patch advisory bulletins
- Company IT Security Policy
- NIST SP 800-40 Revision 4: Guide to Enterprise Patch Management Technologies

8. Revision History

Date	Version	Description	Author
2024-06-15	1.0	Initial Template Creation	IT Department