**Document Title:** Script Update Frequency and Compliance Procedure  
**Version:** 1.0  
**Effective Date:** [Insert Date]  
**Prepared by:** [Name/Team]  
**Reviewed by:** [Compliance Officer/Team]  
**Approved by:** [Manager/Director]

**1. Purpose**

The purpose of this document is to define the procedure and frequency for updating all scripts to ensure they comply with the latest technology specifications and security hardening requirements. It outlines the responsibilities, compliance requirements, and steps for a standardized update process.

**2. Scope**

This procedure applies to all automation scripts used within [Company/Department Name], including but not limited to configuration management, monitoring, data processing, and system integration scripts. The process is relevant for scripts interacting with network devices, servers, databases, and third-party applications.

**3. Roles and Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| **Script Owner** | Owns and maintains the scripts. Responsible for updating scripts as per the latest tech specs. |
| **Tech Lead** | Verifies that scripts are compliant with latest hardening and technical standards. |
| **Compliance Team** | Reviews the updates for security, regulatory, and policy adherence. Approves the updates. |
| **Operations Team** | Schedules and applies the approved updates in production environments. |
| **Security Team** | Validates security hardening measures as per latest guidelines. |

**4. Script Update Frequency**

* **Regular Updates:** Scripts must be updated every **90 days** to ensure alignment with the latest technology specifications and security hardening standards.
* **Critical Updates:** Immediate updates must be applied in case of:
  + Security vulnerabilities identified by the Security team.
  + Major software releases affecting functionality or compliance.
  + Critical bugs discovered in the scripts affecting production systems.

**Note:** Exceptions to this schedule must be justified and approved by the Compliance team.

**5. Update Procedure**

**5.1 Review Latest Tech Specs and Hardening Guidelines**

* **Responsibility:** Script Owner
* **Description:** Script Owners must regularly review the latest technical specifications and security hardening requirements published by:
  + Hardware/software vendors.
  + Internal security policies.
  + Industry standards (e.g., CIS benchmarks, ISO standards).

**5.2 Script Modification**

* **Responsibility:** Script Owner
* **Description:** Modify scripts based on the latest guidelines. Ensure that:
  + Code is optimized for performance and security.
  + Compliance requirements are adhered to.
  + Updates align with functional and operational needs.

**5.3 Internal Review**

* **Responsibility:** Tech Lead
* **Description:** Conduct a peer review of the updated script to ensure technical accuracy and compliance with the latest specifications.

**5.4 Submission to Compliance Team**

* **Responsibility:** Script Owner
* **Description:** Submit the updated script, along with a change log, to the Compliance Team for review and approval.

**5.5 Compliance Review**

* **Responsibility:** Compliance Team
* **Description:** The Compliance Team will review the script to ensure it adheres to:
  + Internal security policies.
  + Industry regulations (e.g., GDPR, HIPAA).
  + Company standards for system hardening.

**5.6 Security Validation**

* **Responsibility:** Security Team
* **Description:** Validate the script for any security risks or vulnerabilities that might arise from the changes. Ensure adherence to security hardening benchmarks.

**5.7 Approval**

* **Responsibility:** Compliance Team
* **Description:** Once the compliance and security reviews are successful, the script update is approved for production deployment.

**5.8 Deployment**

* **Responsibility:** Operations Team
* **Description:** Deploy the updated script in the production environment, ensuring minimal disruption to ongoing operations.

**6. Post-Deployment Monitoring and Reporting**

* **Responsibility:** Script Owner and Operations Team
* **Description:**
  + Monitor the performance of the updated script for any unexpected behavior or issues.
  + Prepare a report summarizing the outcome of the update, including any incidents or lessons learned.
  + Submit the report to the Compliance Team.

**7. Documentation and Change Management**

* **Version Control:** Each script update must be tracked through version control systems (e.g., Git), and all changes must be documented in the change log.
* **Change Log:** The following details must be recorded:
  + Update description.
  + Date of modification.
  + Approvals and reviewers.
  + Compliance check results.

**8. Compliance and Audit**

* **Audit Frequency:** The Compliance Team will conduct an audit every **6 months** to verify that scripts are updated in accordance with this procedure.
* **Non-Compliance:** Any instances of non-compliance will be escalated to senior management for review, and corrective actions will be implemented as needed.

**9. Exception Handling**

Any deviation from the defined update schedule or process must be documented and approved by the Compliance Team, including a justification for the delay and a proposed action plan for rectifying the situation.

**10. References**

* [Company Name] Security Policy
* [Industry Standard/Regulatory Guidelines]
* [Vendor Tech Specifications]
* [Internal Change Management Policy]

**Signatures**

| **Name** | **Role** | **Signature** | **Date** |
| --- | --- | --- | --- |
| **[Name]** | Script Owner |  |  |
| **[Name]** | Tech Lead |  |  |
| **[Name]** | Compliance Officer |  |  |
| **[Name]** | Security Lead |  |  |

**Document Control**

| **Version** | **Date** | **Description** | **Author** |
| --- | --- | --- | --- |
| 1.0 | [Insert Date] | Initial Document Creation | [Name] |