Configuration Management Procedure

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>October 02, 2023</td>
<td>Chief Technology Officer</td>
</tr>
</tbody>
</table>

Purpose of Procedure

The purpose of this Configuration Management Policy is to ensure consistent and controlled management of IT server and application configurations throughout their lifecycle. This policy aims to minimize disruptions, enhance stability, improve security, and facilitate effective change management.

Procedure Scope

This procedure applies to all virtual servers and applications, across the organization. It encompasses server hardware configurations, operating systems, software applications, patches, configurations, and related documentation.

This procedure shall be reviewed periodically for any potential advancement in best practices or impact of any environmental changes.

Procedure

1. Configuration Identification
   a. Define naming conventions, labeling, and tagging standards for identifying server configurations.
   b. Maintain an inventory of all servers, including hardware specifications, installed software, configurations, and dependencies.

2. Configuration Control
   a. Establish a formal process for submitting change requests for server configurations.
   b. Conduct impact assessments to evaluate the effects of proposed changes on system performance, security, and functionality.
   c. Obtain approval from the Change Management Team before implementing changes to server configurations.
3. Configuration Status Accounting
   a. Maintain accurate records of server configurations, including version history, change logs, and baselines.
   b. Implement version control mechanisms to track changes and revert to previous configurations if necessary.

4. Configuration Audits
   a. Conduct regular audits of server configurations to verify compliance with standards, policies, and regulatory requirements.
   b. Document audit findings, recommendations, and corrective actions taken to address identified issues.

5. Configuration Documentation
   a. Create and maintain detailed documentation for each server configuration, including configuration baselines, architecture diagrams, network configurations, and security settings.
   b. Ensure documentation is kept up-to-date with any changes or updates to server configurations.

6. Training and Awareness
   a. Provide training and awareness programs for DevOps Engineers, IT staff, and users on configuration management policies, procedures, and tools.
   b. Promote a culture of accountability and responsibility for maintaining accurate and secure server configurations.

7. Tools and Infrastructure
   a. Utilize configuration management tools and software to automate and streamline configuration processes.
   b. Implement monitoring and alerting mechanisms to detect unauthorized changes or deviations from approved configurations.

8. Compliance and Review
   a. Conduct regular reviews of configuration management processes and procedures to identify areas for improvement and ensure ongoing compliance.
   b. Monitor key performance indicators related to configuration management, such as change request turnaround time, configuration accuracy, and security posture.

9. Roles and Responsibilities
   a. Clearly define the roles and responsibilities of DevOps Engineers, Director of IT, Change Management Team members, CISO/IT Security Team, and users in the configuration management process.
   b. Establish communication channels and escalation procedures for addressing configuration-related issues and concerns.

10. Enforcement and Consequences
a. Enforce adherence to configuration management policies and procedures through regular audits, assessments, and performance evaluations.

b. Define consequences for non-compliance, which may include disciplinary actions, training requirements, or corrective measures to mitigate risks associated with improper configuration management practices.

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>Chief Technology Officer</th>
<th>Contact: email</th>
<th><a href="mailto:Brian.Wells@healthshareexchange.org">Brian.Wells@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Brian Wells</td>
<td>Version #</td>
<td>1.0</td>
</tr>
<tr>
<td>Current Approval Date:</td>
<td>October 2, 2023</td>
<td>Last Reviewed</td>
<td></td>
</tr>
<tr>
<td>Date Procedure to go into Effect:</td>
<td>October 2, 2023</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>