New AWS Server Setup Procedure

1. Purpose of Procedure

The purpose of this procedure is to ensure that any new AWS server that is deployed has the necessary configurations to stay compliant with HSX’s security policies.

2. Procedure Scope

This procedure applies to all new AWS servers configured and deployed by HSX employees and 3rd party vendors.

3. Procedure

1. Gather the use case and server specifications
2. Log in to HSX's AWS Console (https://aws.amazon.com/)
3. Open the Amazon EC2 console
4. From the navigation bar, select the US East (N. Virginia) region.

Create a Security Group

5. In the navigation pane, choose Security Groups.
6. Choose Create security group.
7. In the Basic details section, do the following:
   a. Enter the name for the new security group and a description
   b. In the VPC, select the appropriate VPC. Avoid assigning a public IP, if possible, especially for systems storing sensitive PHI data.
8. In the Inbound rules section, create the following rules:
a. Choose SSH from the Type list. In the Source box, choose Custom and specify the port and bastion security groups needed. Set the security group rules to be as restrictive as possible.

9. Choose **Create security group**.

**Launch an Instance**

10. From the console dashboard, choose **Launch Instance**.
11. On the **Quick Start** tab, select the most up to date Ubuntu IAM
12. Choose **Review and Launch** to let the wizard complete the other configuration settings
13. On the **Review Instance Launch** page, under **Security Groups**, select the security group created prior.
14. Choose **Launch**
15. When prompted for a key pair, select **Choose an existing key pair** and select **HSX_Master SSH key** (unless requirements dictate otherwise)
16. Select the acknowledge check box, and then choose **Launch Instances** which will return you to the console
17. On the Instances screen, monitor the status of the launch.
18. Connect to the instance using SSH to verify and validate the instance is up and running.

**Instance Management**

19. Tag the instance with “Patch Group”:”Security Updates” to ensure SSM Fleet Manager will both manage the instance and apply security updates.
20. Setup Duo for two-factor authentication.

**Vulnerability Scanning**

- Perform vulnerability port scanning on the new server, if applicable.
- Perform scan for patch compliance and configuration inconsistencies.
4. **Enforcement**

- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.

5. **Definitions**

For a complete list of definitions, refer to the *Glossary*.

6. **References**

Regulatory References:

- HIPAA Regulatory Reference: <from HITRUST>
- HITRUST Reference: <from HITRUST>
- PA eHealth Reference: <from PDF>

<table>
<thead>
<tr>
<th><strong>Policy Owner</strong></th>
<th>Brian Wells</th>
<th><strong>Contact</strong></th>
<th><a href="mailto:Brian.Wells@healthshreexchange.org">Brian.Wells@healthshreexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approved By</strong></td>
<td>Brian Wells</td>
<td><strong>Approval Date</strong></td>
<td>12-31-21</td>
</tr>
<tr>
<td><strong>Date Policy In Effect</strong></td>
<td>1-1-22</td>
<td><strong>Version #</strong></td>
<td>1.1</td>
</tr>
<tr>
<td><strong>Original Issue Date</strong></td>
<td>4-13-21</td>
<td><strong>Last Review Date</strong></td>
<td>October 28, 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 5, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 30, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>April 13, 2021</td>
</tr>
<tr>
<td><strong>Related Documents</strong></td>
<td>Glossary</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>