Change Management Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4</td>
<td>December 21, 2021</td>
<td>CTO</td>
</tr>
</tbody>
</table>

1. Purpose

The purpose of this policy is to provide the internal structure for the HealthShare Exchange’s (HSX’s) IT Change Management Process.

IT Change Management is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The Change Management Process begins with the creation of a Change Request within the company’s selected technology platform. It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

2. Scope

This policy applies to all HSX employees, contractors, members, participants, users, and third parties

3. Policy

All changes to IT services must follow a standard process to ensure appropriate planning and execution.

Changes will be categorized as a Standard change, a Significant change, or an Emergency change. Appropriate processes and levels of renewal shall be applied to each type of change commensurate with the potential of the change to disrupt operations.

Changes shall formally define and address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management.
It is the responsibility of the Change Control Manager to ensure that all areas under their direction have document processes that meet minimum standards, are reviewed annually, and are communicated to staff. The Change Control Manager serves as Change Authority by default and is ultimately responsible for ensuring that changes are made in a manner appropriate to their impact on operations.

Only authorized administrators are allowed to implement approved upgrades to software, applications and program libraries based on business requirements and the security implications of the release.

The change management procedures shall:

- ensure changes are submitted by authorized users.
- maintain a record of agreed authorization levels.
- review controls and integrity procedures to ensure that they will not be compromised by the changes.
- identify all software, information, database entities, and hardware that require amendment.
- obtain formal approval for detailed proposals requesting changes before work commences.
- document unit, system, and user acceptance testing procedures in an environment segregated from development and production.
- ensure all system components are tested and approved prior to promotion to production.
- document rollback procedures for failed changes.
- ensure authorized users accept changes prior to implementation based on the results on the completion of each change of testing the changes.
- ensure that the system documentation set is updated, and that old documentation is archived or disposed.
- maintain a version control for all software updates.
- maintain all change requests and approvals with Jira.
- testing for mobile device, operating system, and application compatibility issues via a documented application validation process.
- ensure that operating documentation and user procedures are changed as necessary to remain appropriate.
- Ensure that automated updates are not used on critical systems, as some updates may cause critical applications to fail.
• Ensure that there is control over operational software such that HSX shall not allow for HSX development executable code or compilers to be added to operational systems and that they only hold approved programs or executable code.

• **Configuration Management**: Written procedures for configuration management will be assessed and whether or not the procedure(s) address(es) each element of the policy/control requirement(s). The configuration management plan must:
  o Address roles, responsibilities, and configuration management processes and procedures.
  o Define the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management.
  o establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; and protect the configuration

4. **Procedures**

The following procedures apply to HSX internal operations only

• Change Management Procedure

5. **Enforcement**

• HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
• Each member, participant and third party shall be responsible for ensuring that their respective physicians, care managers and other staff follow this policy.
• The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the President.
• The results and recommendations of the reviews are documented and approved by management.

6. **Definitions**

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

<table>
<thead>
<tr>
<th>Policy Owner</th>
<th>Technical Operations</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By</td>
<td>Privacy and Security Workgroup</td>
<td><a href="mailto:Brian.Wells@healthshareexchange.org">Brian.Wells@healthshareexchange.org</a></td>
</tr>
<tr>
<td>Date Policy In Effect</td>
<td>February 24, 2022</td>
<td>Approval Date: February 24, 2022</td>
</tr>
<tr>
<td>Original Issue Date</td>
<td>October 2, 2014</td>
<td>Version #: 1.4</td>
</tr>
<tr>
<td>Related Documents</td>
<td>Glossary</td>
<td>Last Review Date:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>October 23, 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td>December 5, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td>February 24, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td>December 21, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td>September 29, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td>September 16, 2020</td>
</tr>
<tr>
<td></td>
<td></td>
<td>November 29, 2018</td>
</tr>
</tbody>
</table>