1. Purpose of Procedure

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 interest parties.

2. Procedure Scope

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX information assets are required to comply with this process.

3. Procedures

The primary goal of the IT change management organization is to accomplish IT changes in the most efficient manner while minimizing the business impact, costs, and risks. All IT changes within the company will be documented in the company’s selected technology platform. Changes shall formally define and address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management.

To achieve this, the change management process includes the following primary steps:

- **Formally Request a Change** - All requests for change will be documented within the company’s selected technology platform by creating a new change record. The completion of a new request for change will be completed by the change coordinator with input from the Change Requester. The requestor must be required
to document rollback procedures for failed changes. Additionally, in the event of an unforeseen event, the requestor must provide documentation for aborting the change and recovery.

- **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:
  - Address roles, responsibilities, and configuration management processes and procedures.
  - Define the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management.
  - 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 management plan from unauthorized disclosure and modification.

- **Categorize and Prioritize the Change**: The Change Management Advisory Committee will assess the urgency and the impact of the change on the infrastructure, end user productivity, and budget.

- **Analyze and Justify the Change**: The Change Coordinator works with the change requester and the change initiator to develop specific justification specifically in regard to usability and security issues for the change and to identify how the change may impact the infrastructure, business operations, and budget. The Change Coordinators use this information to further research and develop an extensive risk and impact analysis. When completing the analysis of the change, the Change Coordinator must ensure they consider the business as well as the technical impacts and risks.

- **Review Each Change** to ensure the compliance of information processing as part of a formal risk assessment process. The review shall include a determination if there is a new or retired authorized software. In these cases, HSX shall maintain an up-to-date list of authorized software that is required in the enterprise for any business purpose on any business system. The approver for a specific change shall determine if such change adds authorized software to the authorized software list or removes or retires software from the authorized list. Maintained within the Application Risk Assessment documentation.
• **Validate Test Results.** To **ensure** appropriate separation between production and non-production (development, test/quality assurance) environments, separate change requests tickets are required for testing vs promotion to production. This separation of approvals is designed to prevent operational issues. To ensure that all system components are tested and approved prior to promotion to production. Such testing includes checking the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. Once the testing change ticket has been approved for closure, a change request to promote the changes to production may be submitted for approval.

• Ensure for in-house developed software that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

• **Source Code Management** - All new and revised source code shall be managed through a source code management service called Bitbucket. All source code versions will be archived and will never be purged.

• **Control of operational software** – 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.

Ensure that automated updates are not used on critical systems, as some updates may cause critical applications to fail.

**Approval**

• **Approve and Schedule the Change** - The Change Coordinator uses the company’s selected technology platform to record an efficient process for routing the Request for Change (RFC) to the Change Coordinator, technical approvers, business approvers and, in the event of a major or significant change, to the Change Advisory Board for approval or rejection of the change.

• **Plan and Complete the Implementation of the Change** - This process includes developing the technical requirements, reviewing the specific implementation steps and then completing the change in a manner that will minimize impact on the infrastructure and end users.

• **Post-Implementation Review** - A post-implementation review is conducted to ensure whether the change has achieved the desired goals. Post-implementation actions include deciding to accept, modify or back-out the change; contacting the end user to validate success; and finalizing the change documentation within the company’s selected technology platform.

• **Requirements and criteria for acceptance of new systems** must be clearly defined, agreed, documented, and tested. HSX ensures that new system upgrades
and new versions are only migrated into production after obtaining formal acceptance from management.

- HSX shall review and update authorization authority (approvals) annually or when circumstances require an earlier review.

1. **Standard Changes (What are they?)**
   a. A Standard Change is a relatively low-risk change with well-understood outcomes that is regularly made during the course of business. A Standard change follows pre-determined processes, is pre-approved by change management processes and may be made at the discretion of an individual employee, provided it has been defined as Standard per the Change Management assessment process.

2. **Normal/ Significant Changes**
   a. A significant change is one that has medium to high risk for critical services, involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during the course of business. Because of the ability to affect downstream or upstream services, any proposed significant change must be reviewed by the Change Advisory Board and authorized by the Change Authority. Significant changes are reviewed weekly after submission.

3. **Emergency/Urgent Changes**
   a. Occasionally, critical nature or “emergency” changes may be required to quickly mitigate outages or production issues. Emergency changes may enter the Change Management process by request from the change requester. In the case of an emergency change, while maintaining integrity of the formal process, a streamlined process is used to allow the most rapid response possible. All Emergency RFCs will be reviewed within one hour after submittal. Before implementation, a text message must be sent to the Advisor/Change Advisory Board.

4. **Salesforce Changes**
   a. Subcommittee will make decisions for RFC to the Salesforce environment.
   b. Subcommittee will meet based on the number of requests submitted each week.

**Third Party Change Management**

1. All changes from a Third Party Vendor will be relayed to HSX via a Change Management ticket.
   a. All proposed changes are evaluated and potential impacts identified before implementation.
   b. All new code going into production is reviewed and signed off by HSX before the Change Management Ticket. The review team examines security flaws, potential issues, and efficiency in particular.
II. Ensure that vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions in the application. Also, maintain information systems according to the current baseline configuration and configure available system security parameters to prevent misuse. Also, checklists and configuration management processes and procedures for vulnerability port scans are performed in accordance with the Vulnerability Management Plan.

III. In the event that systems or system components in production are no longer supported by the developer, vendor, or manufacturer, HSX shall develop a formal migration plan approved by management to upgrade or replace the system or system components.

IV. The above general Change Management procedures are implemented subsequently.

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 shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
   • The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
   • The Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
   • The results and recommendations of the reviews are documented and approved by management.

Documentation
   • All documentation and all prior changes shall be maintained within Salesforce within the appropriate location per the change.

4. Definitions

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

   • Change control – A formal planning process to make sure only necessary changes are authorized, made, and recorded.
   • RFC – A request for change is a declarative document containing the details of an emergency or non-emergency call to an adjustment of a system. HealthShare
Exchange of Southeastern Pennsylvania, Inc. requires an online form to be completed in order make a request for change.

- **Requester** – Individual, team, or entity seeking a change pertaining to the existing system.

### 5. References

Regulatory References:
- HITRUST References: XX.y CSF Control Reference, XX.y Another CSF Control Reference

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>CISO</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>1.3</td>
</tr>
<tr>
<td>Current Approval Date:</td>
<td>January 10, 2022</td>
<td>Review Dates:</td>
<td>November 9, 2023 December 6, 2022 January 9, 2022 October 2, 2021 October 19, 2020 December 16, 2020 September 15, 2020 April 1, 2017</td>
</tr>
<tr>
<td>Date Procedure to go into Effect:</td>
<td>December 16, 2019 April 1, 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Documents:</td>
<td>Glossary Change Management Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>