Third Party Access Procedures

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>January 11, 2022</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

Purpose of Procedure

The purpose of this procedure is to define the steps necessary to grant access to HSX’s information assets, specifically to ensure that due diligence has been conducted, appropriate controls have been implemented, and a written contract defining the terms of access have been assigned.

Procedure Scope

This procedure applies to all third-party arrangements, including those with Business Associates.

Procedures

A. For the third party to obtain access to the HSX system the following procedure must be followed:

1. The third party must execute a BAA prior to access procedures being started. In the event that the third party is a member then they are also required to execute a Participation Agreement.
2. The third party must complete or provide HIPAA training before any access is granted. If the third party does not have HIPAA training, the CISO conducts on an account-by-account basis.
3. After training has been completed, a ticket to change management in the form of a change request is submitted which includes an authorization for the level of access and privileges to be granted based upon contracted services,
4. The Change Management procedure is followed.
5. If the Change Request is accepted, unique user names (IDs) are created for the third party members. Such access shall include temporary passwords that must be reset by the end-user and meet HSX minimum password standards. See Create a New User Procedure.
6. All access that is not explicitly authorized is forbidden.
7. The change management procedures will be utilized for authorization to revoke access rights or interrupting the connection between systems;
8. Third party support vendors will only receive physical or logical access for support and diagnostic purposes when necessary, and with management approval by either the HSX CISO or the HSX Director of IT. Such approval shall require written requests from support vendor’s management for named resources prior to granting access to covered information.
Access will be granted with strong credentials consistent with privileged access credential requirements. Access will be monitored by the Director of IT. Change management tickets will be created to document support and diagnostic activities, Credentials will be disabled once the required services are completed.

9. Contracts with third party subcontractors in an arrangement with a business associate, and requiring access to PHI for a business associate, shall include the same contractual requirements that apply to other arrangements between an organization, acting as a covered entity, and the business associate. Such arrangements shall be governed by the Business Associate Privacy Policy.

B. After the Third Party gains access, the Technical Operations Team will monitor the vendor’s activity per the following procedure:

1. On a monthly basis, the Technical Operations Team will gather all the metrics provided by the vendor for the last 30 days and measure them against the established critical success factors and SLAs with the specific vendor.
2. The referenced metrics are the established specifications for the underpinning contracts between HSX and its membership (the HSX Service Level Objectives or SLOs). The metrics are compared to the HSX SLOs and reported to the HSX membership via the HSX Implementation workgroup monthly.
3. For any infractions or breach of the SLA within the previous month, Technical Operations reports the issues to the account manager of the vendor with a ticket raised to enforce any policies that have been previously agreed upon within contract.
4. Once penalties have been agreed upon and are credited to HSX, Technical operations reports to the HSX Leadership Team to be accounted for within the next billing cycle.

C. Access to HSX Privacy Policies:

1. All externally facing services that are configured to provide connections that allow customers to access HSX’s computing assets will provide appropriate text or a link to HSX’s privacy policy for data use and protection as well as the customer’s responsibilities when accessing the data.

Definitions

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

References
<table>
<thead>
<tr>
<th><strong>Responsible Owner:</strong></th>
<th>Chief Information Security Officer</th>
<th><strong>Contact:</strong> email</th>
<th><a href="mailto:Brian.Wells@healthshareexchange.org">Brian.Wells@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approved By:</strong></td>
<td>Brian Wells</td>
<td><strong>Version #</strong></td>
<td>1.2</td>
</tr>
</tbody>
</table>
| **Current Approval Date:** | January 11, 2022                   | **Review Dates:**  | October 28, 2023  
December 18, 2023  
October 9, 2021  
October 18, 2020  
March 19, 2019  
May 13, 2015 |
| **Date Procedure to go into Effect:** | March 19, 2019 | **Related Documents:** | Change Management Policy  
Third Party Risk Management Policy  
Change Management Procedure  
Create a New User Procedure |