Third Party Vendor Selection Process

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>March 19, 2019</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

1. Purpose of Procedure

The purpose of this procedure is to provide guidelines for due diligence required during third party vendor selection.

2. Procedure Scope

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

3. Procedures

A. Preparation for Third Party Vendor Selection:
   1. An initiative is approved by the HSX Board or the HSX Leadership team.
   2. A project manager (PM) is assigned to the initiative.
   3. A PMO Project Request Form is prepared by the PM and submitted to the Project Review Committee for review.
   4. If approved by the Project Review Committee, an HSX evaluation team (ET) is assigned to the project.
   5. HSX Preferences for third party vendor selection are established by the ET.
   6. Outreach to potential third party vendors is completed by the PM.
   7. An initial demonstration of the product(s) or service(s) by the third party vendor is scheduled with the ET and all pertinent HSX personnel present.
   8. The ET, with support from pertinent HSX personnel develops the Request for Quote (RFQ) and gains internal approval.
   9. The ET determines the timeline for distribution, vendor response, ET team evaluations and the remainder of the selection process through to negotiations.
   10. All vendors are sent a Request for Quote (RFQ) with appropriate instructions.

B. Vendors are evaluated per the following process:
   1. The HSX ET has primary responsibility for evaluating and rating the proposals.
2. The PM develops a side-by-side comparison of the ET members RFQ ratings along with a cost side-by-side comparison.
3. The ET and relevant HSX leadership preliminary ET team review findings and discuss differences in perspectives.
4. Based upon the RFQ response ratings and cost-analysis, a shortlist of third party vendors is agreed upon.
5. Checkpoint meeting is held with relevant requesting members as needed to share high-level findings and determine a go or no go position to proceed with the due diligence components below.
6. Additional Information is obtained through the following means to validate vendor capabilities and refine evaluations:
   - Third Party Vendor client reference calls are completed.
   - A budget analysis is performed and shared with the pertinent HSX members.
   - Formal demonstrations of the service/product with the shortlist of third party vendors is performed during which testing of compatibility with HSX functionality occurs. Particular attention is devoted to the establishment of encrypted remote access connections between HSX and the external parties.
   - Interviews are conducted with the third party vendor’s pertinent personnel, including and highlighting the third party’s security compliance officer.
   - An analysis of the Third-Party Vendor’s security measures is performed during which their most recent security audit is examined and their response to the gap assessment is evaluated.
      1. If an analysis is unavailable, HSX will allow for the Third-Party Vendor to provide evidence as to their security capabilities.
      2. This information will be taken into account in the final processes and evaluation detailed below.
      3. HITRUST certification is required for vendors who process or store PHI.
   - During which, HSX ensures all data is encrypted when stored. If the data is not to be encrypted, the rationale for this decision is documented and submitted to HSX before any formalization of contracts occurs.
   - The evaluation process shall validate that specifications for related security controls have been incorporated in the system. If any non-essential security controls are absent from the system, supplemental manual controls will be developed as needed.

C. Final Processes
1. ET presents findings and vendor selection recommendations to HSX leadership.
2. HSX leadership and PM meet with relevant members to present final recommendation.
3. On approval:
   - A Master Service Agreement (MSA) is drafted by the third party vendor which will include and cover all HSX security priorities.
The MSA is reviewed by the HSX legal department to ensure that all HSX security policies are met and that access is granted minimally and for only the duration required.

If software development is necessary for functionality, discussions pertaining to ownership of the source code is established during the contracting process.

Any penalties exacted in the event of any failure will be in accordance with the MSA.

D. The Vendors are evaluated by the following criteria (a nonexclusive list):

<table>
<thead>
<tr>
<th>Third Party Vendor Evaluation Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Proposal</strong></td>
</tr>
<tr>
<td>Vendors proposed solution fully meets HSX in-scope services and does not require additional features to be licensed.</td>
</tr>
<tr>
<td>Vendors proposed solution fully meets HSX in-scope services and does not require additional features to be licensed.</td>
</tr>
<tr>
<td>Vendor proposed high-level timeline meets objectives</td>
</tr>
<tr>
<td>Vendors proposed team has the expected qualifications and experience with like implementations</td>
</tr>
<tr>
<td><strong>Vendor Business Information</strong></td>
</tr>
<tr>
<td>Organizational commitment to proposed products</td>
</tr>
<tr>
<td>Vendors experience with &amp; delivering quality software components similar to HSX scope to customers</td>
</tr>
<tr>
<td>Vendor has documented acceptable certifications for and / or other related components of their offering</td>
</tr>
<tr>
<td>Vendor complies with federal and state laws and regulations and meets HSX requirements</td>
</tr>
<tr>
<td>Vendor has supplied an acceptable customer install base consistent with our RFQ requirements such that it is clear that the offering is operational...and has supplied an acceptable client reference list for same</td>
</tr>
<tr>
<td>Vendor long term offering strategy meets expectations and any leveraged third party for components or delivery are acceptable.</td>
</tr>
<tr>
<td>Vendors leadership structure and organization supporting their offering to HSX is satisfactory</td>
</tr>
<tr>
<td>Vendors Commitment to the HIE software marketplace makes it clear of their intent to continue</td>
</tr>
<tr>
<td>Vendors account management model and engagement with HSX is at HSX’s optimal level given learnings from current HSX vendor account management protocols</td>
</tr>
</tbody>
</table>
Vendor has not disclosed any pending organizational changes such as mergers or divestitures that are of a concern to HSX

Vendor has provided 3 specific references for each proposed solution relevant to this RFQ with required contact information.

**Privacy and Security Framework**

Vendors description of their application security meets or exceeds industry best practices for the protection of their systems.

Vendor has provided HITRUST certification or other Security specific certifications that meet HSX requirements and vendor agrees to provide HITRUST certification letters throughout the contract period.

**Vendor Licensing and Support**

- Value of Quote for professional services and other one-time implementation costs is within HSX budget
- Value of Quote for licensing costs are within HSX budget
- Value of Quote for support model costs are within HSX budget

Vendors approach to upgrades and releases for the proposed solution is well organized, reflects QA procedures, shows a reasonable frequency and meets HSX requirements.

Vendors cost model for tiered pricing for growth provides adequate discounts within HSX expected likely range

**Vendor Financials**

Vendors provided consolidated financials that attest to their financial viability to enter into a long-term relationship with HSX

**Future Potential Interest**

Variable based on goals

---

E. When onboarding a new vendor, before the service in which the vendor is providing goes live, the SLA or OLA will be discussed and agreed upon by service level. Discussion topics that will be communicated to both parties beforehand include the following:

- Contract duration (with start and end dates)
- Agreements shall include requirements to address the information security risks associated with information and communications technology services consistent with HSX policies and procedures
- Rules regarding renewal and termination of the agreement (if applicable, also rules regarding early termination of the agreement)
• Description/ desired customer outcome
• Business justification and benefits
• Business processes/ activities on the HSX side supported by the service
• Desired outcome in terms of utility
• Desired outcome in terms of warranty
• Communication between HSX and service provider
• Responsible contact person on HSX side with contact details
• Designated Business Relationship Manager on service provider side with contact details
• Service Reporting (contents and intervals of service reports to be produced by the service provider)
• Procedure for handling exceptions and complaints (e.g. details to be included in formal complaints, agreed response times, escalation procedure)
• Satisfaction surveys (description of the procedure for measuring customer satisfaction on a regular basis)
• Service Reviews (description of the procedure for reviewing the service with the customer on a regular basis)
• Service and asset criticality
• Identification of business-critical assets connected with the service
• Vital Business Functions (VBFs) supported by the service
• Other critical assets used within the service (e.g. certain types of business data)
• Estimation of the business impact caused by a loss of the service or assets (in monetary terms, or using a classification scheme)
• Service times, including times when the service is required to be available and exceptions
• Required types and levels of support (e.g.  
  ▪ on-site support  
    • area/ locations  
    • Types of users  
    • Types of infrastructure to be supported  
    • Reaction and resolution times (according to priorities, definition of priorities e.g. for the classification of Incidents)  
  ▪ Remote support  
    • Area/ locations  
    • Types of users (user groups granted access to the service)  
    • Types of infrastructure to be supported  
    • Reaction and resolution times (according to priorities, definition of priorities e.g. for the classification of Incidents)
• Service level requirements/ targets
• Availability targets and commitments
• Conditions under which the service is considered to be unavailable (e.g. if the service is offered at several locations)
• Availability targets (exact definition of how the agreed availability levels will be calculated, based on agreed service time and downtime)
• Reliability targets (required by some customers, usually defined as MTBF (Mean Time Between Failures) or MTBSI (Mean Time Between Service Incidents))
• Maintainability targets (required by some customers, usually defined as MTRS (Mean Time to Restore Service))
• Down times for maintenance (number of allowed down times, pre-notification periods)
• Restrictions on maintenance, e.g. allowed maintenance windows, seasonal restrictions on maintenance, and procedures to announce planned service interruptions
• Definitions of Major Incidents as well as Emergency Changes and Releases to resolve urgent issues, including procedures to announce unplanned service interruptions
• Requirements regarding availability reporting
• Capacity/ performance targets and commitments
• Required capacity (lower/upper limit) for the service, e.g.
• Numbers and types of transactions
• Numbers and types of users
• Business cycles (daily, weekly) and seasonal variations
• Response times from applications
• Requirements for scalability (assumptions for the medium and long-term increase in workload and service utilization)
• Requirements regarding capacity and performance reporting
• Service Continuity commitments (availability of the service in the event of a disaster)
• Time within which a defined level of service must be re-established
• Time within which normal service levels must be restored
• Technical standards/ specification of the service interface
• Mandated technical standards and specification of the technical service interface
• Responsibilities
  ▪ Duties of the service provider
  ▪ Duties of the customer (contract partner for the service)
  ▪ Responsibilities of service users (e.g. with respect to IT security)
• IT Security aspects to be observed when using the service (if applicable, references to relevant IT Security Policies)
• Pricing model
  ▪ Cost for the service provision
  ▪ Rules for penalties/ charge backs

4. Definitions

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

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>Technical Operations</th>
<th>Contact: email</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Board</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSX Management Team</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Approval Date:</td>
<td>March 19, 2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review Dates:</td>
<td>October 28, 2023</td>
<td>December 20, 2022</td>
<td></td>
</tr>
<tr>
<td></td>
<td>October 9, 2021</td>
<td>October 16, 2020</td>
<td></td>
</tr>
<tr>
<td></td>
<td>March 19, 2019</td>
<td>January 19, 2017</td>
<td></td>
</tr>
<tr>
<td>Date Procedure to go into Effect:</td>
<td>January 19, 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Documents:</td>
<td>Third Party Risk Management Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>