Information Systems Acquisition, Development & Maintenance Security Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>December 16, 2015</td>
<td>Daniel Wilt</td>
</tr>
</tbody>
</table>

1. Purpose
To ensure that security is an integral part of HealthShare Exchange of Southeastern Pennsylvania, Inc. (HSX) information systems throughout all phases of the acquisition, development, and maintenance lifecycle.

Security must be considered at every stage of an information system’s life cycle (e.g., feasibility, planning, development, implementation, maintenance, retirement, and disposal) in order to:

- Ensure conformance with all appropriate security requirements
- Protect enterprise data throughout its life cycle
- Facilitate efficient implementation of security controls
- Prevent the introduction of new risks when the system is modified
- Ensure proper removal of data when the system is retired

2. Scope
This policy applies to all enterprise information systems or systems that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein.

3. Policy
Information Systems Acquisition, Development and Maintenance Policy:

- HSX shall ensure that security is an integral part of its information systems throughout all phases of the acquisition, development, and maintenance lifecycle.
• HSX shall maintain cyber liability insurance in accordance with industry standards and as required by the Founding Members Participation Agreement.
• In accordance with the HSX Audit, Logging and Monitoring Policy, HSX regularly monitors and assesses security risks as part of proactive and ongoing maintenance.
• HSX will mitigate risks that are identified during the regular auditing process.

Capacity Management:
• The use of information resources shall be planned, prepared, and monitored, and projections shall be made of future capacity requirements to ensure adequate performance.
• Procedures shall be developed to respond to audit log storage capacity issues according to the Audit Logging and Monitoring policy.

Information System Acceptance:
• HSX shall establish acceptance criteria for new information systems, upgrades, and new versions.
• HSX shall conduct suitable tests of each information system during development and prior to acceptance to ensure security controls are in place.
• New information systems, upgrades, and new versions shall only be released into production after obtaining formal acceptance from senior leadership.

Business Requirements for New Information Systems:
• Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems, shall specify requirements for security controls.
• In acquiring new information systems and/or contracting with new vendors, HSX will ensure that the systems/entities are of high reputation and at least similar caliber to the current health information exchange vendors and that all such relationships comply with the terms of the Founding Member Participation Agreement and HSX Policies.
• Security controls in business requirements shall include:
  o Consideration of business value and legal-regulatory-certificatory standards for information assets affected by the new/changed system.
  o Consideration of administrative, technical, and physical controls available to support security for the information system.
  o Integration of security controls early in requirements specification and system design.
  o A formal plan for testing and acceptance, including independent evaluation where appropriate.

Input Data Validation:
• Data input to applications and databases shall be validated to ensure that the data is correct and appropriate. Both automatic and manual methods of data input validation testing shall be used as appropriate.
• HSX shall define data input validation procedures.
• HSX shall define secure coding guidelines to prevent common vulnerabilities during software development.
• HSX shall develop system and information integrity procedures.
• HSX shall include data input validation checks in testing methodologies. Where possible data input validation testing shall be automated through use of tools or other non-manual methods.
• Applications developed by HSX or third parties shall be based on secure coding guidelines and shall undergo testing.
• Applications that store, process, or transmit confidential data shall undergo application vulnerability testing by a qualified third party at least annually.
• Third party vendors shall comply with vulnerability testing requirement and provide HSX reports in accordance with the *HSX Audit Logging and Monitoring Policy*.

Control of Internal Processing:

• Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
• HSX shall define integrity controls and develop a validation checklist.

Message Integrity:

• Requirements for ensuring authenticity and protecting message integrity in applications shall be identified.
• Message integrity controls shall be identified and implemented.

Output Data Validation:

• Data output from applications and databases shall be validated to ensure that the processing of stored information is correct and appropriate. Both automatic and manual methods of output data validation testing shall be used as appropriate.
• HSX shall define output data validation procedures.

Control of Production Software:

• HSX shall implement procedures to control the installation of software on production/operating systems to minimize the risk of interruptions to, or corruption of those systems.
• To minimize the risk of corruption to operational systems, the following procedures shall be implemented:
Only authorized System Administrators shall be allowed to implement approved upgrades to software, applications and program libraries. Production systems shall only hold approved programs or executable code (i.e., no development code or compilers).

- Third party software used in production systems shall be maintained at a level supported by the vendor.
- If systems in production are no longer supported by the vendor, HSX must provide evidence of a formal migration plan and obtain senior leadership approval to implement the plan.
- Applications and production/operating systems shall be tested for usability, security, and impact prior to release in production.
- Production software must comply with the Change Management Policy and Configuration Management Policy.
- Physical or logical access shall be given to a third party for support purposes only when necessary, and only with senior leadership approval. The vendor’s activities shall be monitored.

Protection of Test Data:

- Test data shall be selected carefully, and appropriately logged, protected and controlled.
- The use of operational databases containing confidential data for non-production (e.g., testing) purposes shall be avoided. If confidential data or internal use only data must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (de-identified) before use.
- HSX shall establish controls and procedures to protect test data, test systems, and testing environments.

Access Control to Program Source Code:

- Access to program source code and associated items (e.g., designs, specifications, verification plans, validation plans, etc.) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

Outsourced Software Development:

- The development of software by third parties shall be done under the supervision of HSX.
- The development of software by third parties shall be governed by a contract or a Service Level Agreement (SLA) that includes security requirements.
- Independent security and code reviews shall be conducted by an individual with certified security training before bringing new services into production.
4. Enforcement

- The CISO 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: HIPAA § 164.312(b), HIPAA § 164.312(c)(1), HIPAA § 164.312(c)(2), HIPAA § 164.312(e)(2)(i), HIPAA § 164.314(a)(2)(i)
- HITRUST Reference: 09.h Capacity Management, 09.i System Acceptance, 10.a Security Requirements Analysis and Specification, 10.b Input Data Validation, 10.c Control of Internal Processing, 10.d Message Integrity, 10.e Output Data Validation, 10.h Control of Operational Software, 10.i Protection of System Test Data, 10.j Access Control to Program Source Code, 10.l Outsourced Software Development
- PCI DSS v3 2.2, PCI DSS v3 2.2.4, PCI DSS v3 6.5, PCI DSS v3 6.5.1, PCI DSS v3 6.5.2, PCI DSS v3 6.5.3, PCI DSS v3 6.5.4, PCI DSS v3 6.5.5, PCI DSS v3 6.5.6, PCI DSS v3 6.5.7, PCI DSS v3 6.5.8, PCI DSS v3 6.5.9, PCI DSS v3 6.5.10, PCI DSS v3 6.6
- PA eHealth Reference: 11.0. Service Level Agreements (SLAs)
<table>
<thead>
<tr>
<th>Related Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Logging and Monitoring Policy</td>
</tr>
<tr>
<td>Change Management Policy</td>
</tr>
<tr>
<td>Configuration Management Policy</td>
</tr>
<tr>
<td>Founding Member Participation Agreement</td>
</tr>
<tr>
<td>Glossary</td>
</tr>
</tbody>
</table>