Vulnerability Management Plan

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>November 22, 2022</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

Purpose of Procedure

This procedure states the actions HealthShare Exchange (HSX) will take to manage risk related to technical vulnerabilities in an effective, systematic, and repeatable way, and to confirm the effectiveness of those actions.

Procedure Scope

This procedure applies to all information assets connected to the HSX network including but not limited to computer workstations, laptops, tablets, smartphones, servers, appliances, network switches and routers, etc.

The Chief Information Security Officer (CISO) has the authority to conduct vulnerability assessments on any information asset, product, or service within HSX.

Procedures

A. Vulnerability Management Plan Evaluation Procedure:

1. On a quarterly basis, the Technical Operations lead, the Privacy Officer, and the Security Officer review the Vulnerability Management Plan and the Vulnerability Management Policy.
2. If any changes are deemed necessary per Section B, they are discussed, prioritized and finalized with the Privacy and Security Workgroup,
3. The revised Vulnerability Management Plan is presented to the Executive Board.
4. Recommendations from the Executive Board are included in the organizational goals for next year.
5. The TechSecOps group will review information from its tools and vulnerability mailing lists/other information sources to identify relevant technical vulnerabilities and/or to maintain awareness about them, identified for software and other technology based on the asset inventory. TechSecOps will update these sources based on changes in the inventory, or when other new or useful resources are found.
6. HSX shall have "Cross-Region copy" set to on to ensure that patches are installed in the organization's disaster recovery environment.
7. HSX shall use the CVSS score to determine the risk ranking, classification of the vendor supplied patch, and/or the classification and criticality of the affected system.
B. Risk Monitoring and Review:

1. Risks shall be continually evaluated and assessed.
2. HSX CISO shall subscribe to automated notifications from DHHS Office of critical Infrastructure Protection (CIP) automated notification services, as well as HPH Sector Highlights – Cybersecurity Editor. HSX CISO shall promptly advise management and share appropriate notifications with HSX staff via email and/or through direct meetings.
3. HSX’s CISO shall maintain membership in special interest groups or forums/services as a means to: improve knowledge of best practices and stay up to date with relevant security information; ensure that its understanding of the information security environment is current and complete (e.g., threat monitoring/intelligence services); receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; gain access to specialist information security advice; share and exchange information about new technologies, products, threats, or vulnerabilities; and provide suitable liaison points when dealing with information security incidents.
4. 
5. Risks and their factors (asset value, impacts, threats, vulnerabilities, and likelihood) shall be monitored and reviewed regularly to identify any changes.
6. Review incidents of non-compliance and determine whether to waive compliance to the policy and accept the risks.
7. HSX shall regularly review the compliance of information processing as part of a formal risk assessment process. Records of the compliance results (e.g., shall be maintained in order to better track security trends within the organization, respond to the results of correlation and analysis, and to address longer term areas of concern.
8. HSX shall review and update policies on an annual basis.
9. HSX shall review any proposed changes to policies and procedures, non-compliant situations, and exceptions to policies at least annually.

Internal and external vulnerability assessments of covered information systems and networked environments, including both network and application-layer tests are performed by a qualified individual on an annual basis or after significant changes

10. HSX shall contract with one or more third-party vendors to perform a full-scale security and risk assessment as well as penetration and vulnerability testing with industry standard tools. Internal and external vulnerability assessments of systems with confidential data will be in-scope for the third-party evaluating vendor which includes a thorough risk assessment, internal and external penetration testing, and phishing test.
   I. The HSX CISO shall accept the risk ratings from the contracted expert third party assessments and develop a remediation and risk mitigation plan...
   II. The HSX CISO shall ensure that tickets in Jira are created to allow for assigning responsibilities and tracking progress, remediation approach along with evidence of such remediation through to completion of the risk.
III. The CISO reviews the report and consults with HSX leadership. The HSX CISO will perform a cost/benefit analysis for identified countermeasures and present risk treatment summary reports to management.

IV. The CISO will document planned implementations (current and future) in the organization’s security improvement plan; based upon findings of Security Risk Assessments and other contracted security related analysis.

V. HSX shall have identified risks mapping decisions taken against the list of HITRUST CSF controls through Security Risk Assessments.

VI. If needed, the COO is consulted for approval of any new solutions in need of financing.

VII. The HSX CISO shall continually assess the capability of technology needed to sustain an appropriate level of information security based on the size, complexity, and risk appetite of the organization.

C. Application developed by HSX are based on secure coding guidelines to prevent common vulnerabilities and undergo the appropriate testing by the following procedure:

1. HSX mainly depends on its vendors to develop applications for HSX operations. HSX only works with HIPAA compliant applications familiar with secure coding guidelines.

2. Once applications are completed, a change request to Go Live is submitted, and the HSX Change Management Procedures followed.

3. HSX internally reviews all source code in alignment with OWASP (Open Web Application Security Project) and makes any recommendations needed.
   i. HSX uses OWASP for a foundation for secure coding guidelines

4. Before the application is approved to move forward, the application undergoes specific penetration testing on all endpoints.

5. After review of testing, and seeing no vulnerabilities, the application is submitted to Change Management for the final approval to Go Live.

Secure Coding Guidelines

In the event that HSX internally develops applications, they will be based on secure coding guidelines to prevent:

1. common coding vulnerabilities in software development processes;
2. injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.);
3. buffer overflow (Validate buffer boundaries and truncate input strings);
4. insecure cryptographic storage (Prevent cryptographic flaws);
5. insecure communications (Properly encrypt all authenticated and sensitive communications);

6. improper error handling (Do not leak information via error messages);

7. broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user);

8. cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.);

9. improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users);

10. cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers

Applications that store, process or transmit covered information undergo automated application vulnerability testing by a qualified party on an annual basis.

1. All HSX applications used by HSX undergo full vulnerability testing once a year performed by a third-party qualified security vendor.

2. Vulnerability scanning tools used by the third party include those with the capability to readily update the information system vulnerabilities.

3. Every endpoint (both external and internal) is given to the security vendor for assessment; the security group performs testing on all of those endpoints.

4. The test results are submitted to HSX for remediation implementation.

5. If a critical vulnerability is found, the remediation plan is immediately created and performed.

6. HSX schedules and performs a follow up testing on the endpoints to ensure successful remediation has occurred.

7. HSX also performs internal vulnerability checks once every 30 days using AWS Inspector, which provides a list of HSX recommendations for any vulnerabilities found on a specific service or server.

8. HSX also uses Darktrace which performs real time evaluation on all network traffic servers and services and provides real time recommendations over vulnerabilities or potential vulnerabilities within the HSX network.

9. HSX also reviews compliance of office 365 every 30 days, looking for critical suggestions made to become more aligned with their security requirements.
10. If any of the above assessments identify new vulnerabilities within the HSX systems or networked environments, remediation occurs and additional testing is performed to ensure the risk is mediated.

11. All of the internal vulnerabilities testing results are compiled within a documented list and reported, assessed, and monitored accordingly.

**Recommendations from the above review process are created and approved by the following process:**

1. After the above receive process, the third-party evaluating vendor would provide a report of findings.
2. The CISO and Technical operations discuss with the third-party evaluating vendor concerning any threats and issues where the threats and issues are categorized by urgency.
3. Any findings are shared with the pertinent vendor.
4. The Vulnerability Management plan is presented to leadership and recommendations are included in the organizational goals for the next year.
   i. If needed, the COO is consulted for approval of any new solutions in need of financing.
5. The goals are tracked through presentations to the Executive Board.

**A hardened configuration standard exists for all system components**

1. HSX maintains documentation in which a copy of all configurations are maintained for all services, servers, and networks.
2. During a change or upgrade to an application, the application undergoes a review of the settings compared to the documentation, with any discrepancies opened up as support tickets to be addressed. The HSX Support Process is followed.
3. During review, if a change to the system is needed for the documentation to be accurate or resort change in system back to hardened configuration, the HSX Change Management Process is followed.
4. The review occurs on an annual basis of all systems to ensure accuracy.

Where software development is outsourced, the development process is monitored by HSX and includes independent security and code reviews. Additionally, change control procedures to address security must be included in the contract(s). Furthermore, the developer of the information system, system component, or information system service shall be required to track security flaws and flaw resolution and report findings to HSX CISO.
Network services are periodically audited to ensure that providers implement the required security features and meet the requirements agreed with management, including new and existing regulations.

Roles and Responsibilities for technical vulnerability management (from policy)

Processes and procedures for monitoring, assessing, ranking and remediating vulnerabilities identified in systems (from policy)

Processes and procedures proving a timely response to technical vulnerabilities presenting a risk to any information assets, including a timeline based on level of risk (from policy)

Processes and procedures proving a timely response to technical vulnerabilities presenting a risk to any information assets, including a timeline based on level of risk (from policy)

Systems are appropriately hardened (e.g., configured with only necessary and secure services, ports and protocols enabled).

1. HSX provides a VPN or SSL configuration template to the HSX member/participant.
2. The HSX Member/Participant fills out the respective components (requesting specific security and networking configurations e.g. IPs, security protocols, ports, etc.)
3. On AWS
   i. HSX sets up a networking configuration (providing HSX template)
4. On Mirth
   i. Mirth will set up networking configuration (provide Mirth template)

Each sets up agreed upon configuration and testing proceeds

HSX maintains change control of all implemented software and system documentation and archive prior versions of implemented software and system documentation

4. Application in need of upgrade are processed through the upgrade plan coordinated with the application. The process is tracked through the Change Management Procedure throughout the duration of the update.
5. The upgrade is processed within the development environment to identify any severe negative impacts on the HSX infrastructure. During which, statistics are taken concerning the process of the upgrade (e.g. how long the process should take, if any warnings or alarms are observed).
6. If the application upgrade is successful (as observed by the HSX Technical Operations and the vendor support), a change management ticket is opened to upgrade to the HSX test environment.
7. The full testing plan is executed and significant review of all outputs and operations are completed by the HSX Technical Operations team.
8. A Change Management ticket is then submitted by the vendor and the HSX team with the full installation plan and the process for production.
10. Prior to the upgrade, a back-up of the previous version of the application is taken and will act as the restore environment if regression to the prior version is needed.

11. All previous application versions are recorded by the vendor and kept until the vendor no longer supports the version.

**Insider Threat**

HSX maintains a very strong set of policies and procedures that help to minimize the potential for security threats including those from insiders. However, the presence of these controls is just one part of the insider threat program. HSX insider threat monitoring and response must be coordinated by the HSX CISO with the aid of the TechSecOps team or other selected resources at the CISO’s discretion. Early detection and response if critical to minimizing adverse impacts.

**Examples of insider threat classifications include:**

1. Malicious insiders – intentionally use their access to sensitive data and systems to harm the company or misusing or sabotaging HSX assets for personal gain
2. Careless insiders – pose an unintentional threat due to human error or security policy violations
3. Compromised insiders – whose accounts are compromised by cyber criminals

**Insider threat detection and mitigation strategies include:**

1. Limiting access privileges to minimal required (e.g., role-based)
2. Disallow use of BYOD devices to access sensitive data and systems
3. Ensure all installed software is approved
4. Review logs per HSX policy for privileged user access
5. Set automatic alerts from log systems
6. Look for potential indicators of behavioral issues:
   a. Unprofessional behavior
   b. Personality conflicts
   c. Misuses of time or expenses
   d. Conflicts with coworkers
7. Look for indicators of IT sabotage
   a. Creation of backdoor accounts
   b. Disabling system logs
   c. Installing malware
   d. Accessing systems or equipment of other staff
8. Look for indicators of data theft:
   a. Massive downloads
   b. Sending sensitive data to a non-corporate address
   c. Sending emails with large attachments
   d. Extensive use of corporate printers
When HSX outsources software development, the process and implementation is monitored by the following procedure:

1. All software development that is outsourced proceeds through two separate change management processes.
2. The first is an internal process by the vendor in which the code is reviewed by senior membership and senior development to ensure that there are no downstream affects any of the HSX systems. If approved, the request is reviewed by Change Management, which reviewed for any efficiency improvements, errors, or potential negative impacts (including independent security and code reviews).
3. The output of the HSX Change Management Team is sent to the original software development team for final approval.
4. If approved by both change management teams, the final product is dropped into production.

Vulnerability scanning tools used by the third-party risk assessor include the capability to readily update the information system vulnerabilities scanned.

The above procedures will be evaluated annually through the following procedure:

All risks identified through the above procedures which persist for a period greater than one (1) year will be added to the HSX Risk Management Plan (per the Risk Management Policy).

**Definitions**

For a complete list of definitions, refer to the *Glossary*.
| Current Approval Date: | November 22, 2022 | Review Dates: | October 28, 2023  
December 24, 2022  
December 21, 2021  
October 9, 2021  
April 6, 2021  
October 19, 2020  
March 19, 2019  
January 19, 2017 |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Procedure to go into Effect:</td>
<td>November 22, 2022</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Related Documents: | Risk Management Policy  
Risk Management Plan  
Third Party Risk Management Policy  
Vulnerability Management Policy |