HealthShare Exchange

190 N. Independence Mall West | Suite 701 | Philadelphia, PA 19106 | www.healthshareexchange.org | 215-391-4905

Vulnerability Management Policy

Version	Approval Date	Owner
1.2	February 4, 2022	Chief Information Security Officer

1. Purpose

This policy 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.

2. Scope

This policy 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.

3. Policy

HSX shall take deliberate actions to ensure risks to HSX systems resulting from exploitation of published technical vulnerabilities are reduced and mitigated.

Control of Technical Vulnerabilities:

- Timely information about technical vulnerabilities shall be obtained, HSX's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk
- HSX shall follow the *Information Asset Management Policy* and maintain an inventory of information assets with sufficient detail to identify systems at risk by a particular technical vulnerability.
- HSX shall develop, implement, test, and maintain a Vulnerability Management Plan that facilitates the reduction of risk from published technical vulnerabilities. The Vulnerability Management Plan shall include, at a minimum:
    - Roles and responsibilities for technical vulnerability management

  - Processes and procedures for monitoring, assessing, ranking, and remediating vulnerabilities identified in systems.
  - Processes and procedures that provide a timely response to technical vulnerabilities that present a risk to any information assets, including a timeline based on the level of risk.

- HSX shall evaluate the Vulnerability Management Plan at least annually.
- Risks identified in the Vulnerability Management Plan which persist for a period of greater than one (1) year shall be added to the HSX Risk Management Plan according to the *Risk Management Policy*.
- Information resources (including tools and vulnerability mailing lists/other information sources), shall be used to identify relevant technical vulnerabilities and/or to maintain awareness about them, identified for software and other technology (based on the asset inventory list) and shall be updated based on changes in the inventory, or when other new or useful resources are found.
- A prioritization process is implemented to determine which patches are applied across the organizations systems. HSX will accept the severity level of the patches as set by the software vendors' determination.
- Critical security patches shall be applied by the HSX engineering team within one month of release and all other patches shall be applied within 90 days of release. Patches shall be tested and evaluated before they are installed on production systems according to the *Change Management Policy*.
- Updates flagged as Security for the respective underlying operating system shall be automatically installed when a patch operation is run.
- Patches installed in the production environment shall also be installed in the disaster recovery environments in a timely manner.
- Systems shall be appropriately hardened (e.g., configured with only necessary and secure services, ports and protocols enabled) according to the *Configuration Management Policy*. A hardened configuration standard shall exist for all system components and be documented.
- HSX shall engage industry experts to conduct annual technical compliance checks through industry standard automated means to include vulnerability scans, penetration testing, and security risk assessments. Such assessments shall include both Internal and External vulnerability assessments of systems with confidential data.
  - The HSX CISO shall accept the risk ratings from the contracted expert third party assessments and develop a remediation ad risk mitigation plan.
  - 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.
- Semi-annual system scans shall be performed to detect vulnerabilities (e.g., unauthorized software).

- Technical tests of the external and internal network shall be performed annually.
- Applications that store, process or transmit covered information shall undergo automated application vulnerability testing by a qualified party on an annual basis. The qualified party shall be chosen based on the CISO's discretion.
- Exploitable vulnerabilities found during technical testing shall be corrected and testing shall be repeated to verify the corrections.
- Vulnerability remediation processes shall be centrally managed whenever possible.
- The technical vulnerability management program shall be evaluated on a quarterly basis by the Technical Operations Team and CISO.
- Annual compliance reviews shall be conducted by security or audit individuals using manual or automated tools and, if non-compliance is found, appropriate action is taken. These will include:
    - Internal and external vulnerability assessments of systems with confidential data shall be performed on at least an annual basis by a qualified individual or third-party.
    - Semi-annual system scans shall be performed to detect vulnerabilities (e.g., unauthorized software).
- The results and recommendations of the annual compliance reviews must be documented and approved by management.
- Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.1 or later, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).

Configuration Requirements:

- All user systems must have the most up to date version of the following operating systems: Linux, Windows, Apple OS, and Android.
- The Technical Operations Team shall be responsible for alerting staff members when a new and acceptable update is available for download.
- At the Technical Operations Team discretion, staff members shall have up to 30 days to complete critical updates and up to 90 days to complete all other updates.
- The Technical Operations Team shall be responsible for archiving acceptable versions of software.

4. Procedures

The following procedures apply to HSX internal operations only:

- HSX Patch Management
- Incidence Response Plan
- Network Protection Procedures

- Risk Management Plan
- Vulnerability Management Plan

5. Enforcement

- The CISO shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.

6. Definitions

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

7. References

Regulatory References

- HITRUST Reference: 10.m Control of Technical Vulnerabilities
- PCI Reference: PCI DSS v3 2.2, PCI DSS v3 6.1, PCI DSS v3 6.2, PCI DSS v3 6.4.5, PCI DSS v3 6.4.5.1, PCI DSS v3 6.4.5.2, PCI DSS v3 6.4.5.3, PCI DSS v3 6.4.5.4, PCI DSS v3 11.2, PCI DSS v3 11.2.1, PCI DSS v3 11.2.2, PCI DSS v3 11.2.3, PCI DSS v3 11.3, PCI DSS v3 11.3.1, PCI DSS v3 11.3.2, PCI DSS v3 11.3.3., PCI DSS v3 11.3.4

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Board	**Approval Date**	February 4, 2022
Date Policy In Effect	February 4, 2022	**Version #**	1.2

Original Issue Date	July 28, 2015	**Last Review Date**	October 25, 2023 December 5, 2022 February 4, 2022 October 2, 2021 April 6, 2021 September 15, 2020 December 1, 2018 September 20, 2017
Related Documents	Change Management Policy Configuration Management Policy Glossary Information Asset Management Policy Risk Management Policy		