1801 Market Street, Suite 750 Philadelphia PA, 19103 www.healthshareexchange.org

Endpoint Protection Policy

Version	Approval Date	Owner
1.1	September 20, 2017	Daniel Wilt

1. Purpose

To establish effective security configuration, malware detection, and malware prevention methods for all endpoints in the HealthShare Exchange (HSX) computing environment.

2. Scope

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX data are required to comply with this policy.

All HSX employees, interns, contractors and third parties must take responsibility for minimizing the risk of their computing device of infecting other systems or shared files on a server.

3. Policy

Controls Against Malicious Code:

- Detection, prevention, and recovery controls shall be implemented to protect against malicious code.
- Awareness and training on malicious code detection and prevention shall be provided on a regular basis.
- All computing devices that connect to the HSX network shall have anti-malware software installed and running at all times.
- Anti-malware software shall ensure that updates are applied within 24 hours of availability.
- Anti-malware software shall automatically conduct scans of computing devices on boot and every 24 hours.
- Where automatic updates and scans are not possible, users shall be responsible for regularly initiating the scan and updating the software to protect against the latest threats.

- Anti-malware software shall be configured to scan downloads from external sources as they are downloaded and prevent infected files from opening or executing.
- Anti-malware software shall maintain logs of all scans according to the *Audit, Logging, and Monitoring Policy*.
- Anti-malware software shall automatically clean and remove or quarantine malicious code. Infected computing devices shall be removed from the HSX network until they are verified as safe.
- All third-party laptops must have up-to-date anti-malware software installed and verified prior to connecting to the HSX network.
- All employees and contractors must take reasonable measures to protect against the installation of unlicensed or malicious software and must scan media before use, in accordance with the *Acceptable Use Policy*.
- Any activities with the intention of creating and/or distributing malicious programs using HSX's network (e.g., viruses, worms, Trojan Horses, etc.) are strictly prohibited, in accordance with the *Acceptable Use Policy*.

Operating Systems:

- Unmanaged computing devices which become a security risk to the HSX environment shall be disconnected from the HSX network.
- Operating Systems must be maintained by applying any service packs, patches, or security updates that are subsequently released.
- Operating System updates shall be provided automatically. Employees and contractors must follow directions from the Chief Information Security Officer (CISO) when Operating System updates are distributed.
- The CISO must ensure, insofar as possible, that all users apply Operating System updates to their computing devices within a reasonable timeframe.
- Operating Systems which are no longer secure due to obsolescence and therefore no longer have security updates available to fix vulnerabilities, must be upgraded to a currently supported Operating System. If this is not possible for regulatory reasons, the risk shall be documented, and measures taken to reduce and mitigate that risk. The CISO shall determine the risk level and shall issue a waiver in cases where such a waiver is warranted.

4. Procedure

The following procedures apply to HSX internal operations only:

- Virus and Malware Protection Procedure

5. Enforcement

- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.
- The Member, Participant and Third-Party Service Provider shall be responsible for enforcing compliance with this policy at minimum within their organization.

6. Definitions

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

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.308(a)(5)(ii)(B)
- HITRUST Reference: 09.j Controls Against Malicious Code
- PCI Reference: PCI DSS v3 5.1, PCI DSS v3 5.1.1, PCI DSS v3 5.2, PCI DSS v3 5.3

Policy Owner	Security Officer	**Contact**	Daniel.wilt@healthshareexchange.org
Approved By	HSX Management Team HSX Board	**Approval Date**	September 20, 2017
Date Policy In Effect	May 13, 2015	**Version #**	1.1
Original Issue Date	May 13, 2015	**Last Review Date**	December 1, 2018
Related Documents	Acceptable Use Policy Audit, Logging, and Monitoring Policy Glossary Virus and Malware Protection Policy		