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

Virus and Malware Protection Policy

Version	Approval Date	Owner
1.1	September 20, 2017	Chief Information Security Officer

1. Purpose

To establish the requirements for the protection of HealthShare Exchange (HSX) information assets against intrusion by viruses and other malware.

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.

3. Policy

Virus and Malware Protection Policy:

- HSX shall protect its information assets by taking active measures to detect, prevent, and manage malware and virus intrusions and to recover from their effects.
- HSX shall actively monitor traffic on the HSX network and computing devices connected to the network, including remote activity and traffic, in order to maintain the integrity, reliability and performance of IT Systems. This includes (but is not limited to) monitoring for computer viruses and other malware, attempts to access HSX systems without appropriate authorization, systems performance, and compliance with HSX policies.
    - HSX uses technical tools (e.g. IDS) are implemented and operated on the network perimeter and other key points to identify vulnerabilities and mitigate threats and are updated on a regular basis.
- HSX shall reserve the right to intercept and/or quarantine any network traffic or computing resources that may pose a threat to HSX infrastructure, systems or data. This includes but is not limited to files, messages, network traffic and devices.

Controls Against Malicious Code:

- Detection, prevention, and recovery controls shall be implemented to protect against malicious code.
- Protection against malicious code shall be based on security awareness, appropriate system access controls, and change management controls.
- Anti-malware software shall be installed and operating on all HSX computing devices.
- Anti-malware software shall ensure that updates are applied within 24 hours of availability.
- Anti-malware software shall conduct scans of critical computing devices on boot and every 24 hours.
- HSX shall develop procedures that address the receipt of false positives during malicious code detection and eradication and the potential impact on the availability of the information system.
- Anti-malware software shall be configured to automatically scan the following:
    - Downloads from external sources
    - Files received over the HSX network
    - Inbound email and attachments
    - Web traffic, such as HTML, JavaScript, and HTTP
- Anti-malware software shall create audit logs of all scans according to the *Audit, Logging, and Monitoring Policy*.
- Anti-malware software shall block or quarantine malicious code and send an alert to the System Administrator. Infected computing devices shall be removed from the HSX network until they are verified as safe by the Chief Information Security Officer (CISO).
- Anti-spam software shall be implemented at the entry/exit points of the network and at computing devices connected to the HSX network.
- Anti-spam software shall be updated when new releases are available in accordance with the *Configuration Management Policy*.
- HSX shall periodically scan information systems to identify and, where possible, remove any unauthorized software.
- Procedures for responding to detections of malicious code and unauthorized software shall be developed.
- User functionality shall be separated from information system management functionality.
- Each entity shall attempt to identify computing devices that have been compromised and appropriately remediate.
- Once computing devices have been identified as compromised, security actions shall be initiated under the *Incident Management Policy* for affected computing devices.

- For systems not commonly affected by malicious software, each entity shall perform periodic assessments to confirm whether such systems continue to not require anti-virus software.
- External web sites, specific non-critical ports, and Internet Protocol (IP) addresses and ranges that are known sources of malware shall be blocked.

4. Procedures

The following procedures apply to HSX internal operations only:

- HSX Laptop Check
- Incidence Response Plan
- Technical Operations Security Check
- Virus and Malware Protection Procedure

5. Enforcement

- The CISO 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; 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	Audit, Logging, and Monitoring Policy Change Management Policy Configuration Management Policy Endpoint Protection Policy Glossary Incident Management Policy		