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

Network Protection Policy

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

1. Purpose

To ensure the protection of HealthShare Exchange (HSX) enterprise data, especially confidential data in HSX networks, and protection of the supporting HSX network infrastructure.

The secure management of the HSX network, which spans organizational boundaries, requires careful consideration of the flow of information and the regulatory requirements regarding monitoring and protection of its networks.

2. Scope

This policy applies to all employees, interns, contractors, members, participants, users, third parties, and computing devices connecting to any HSX information systems network.

3. Policy

Network Protection Policy:

- HSX shall manage and control its networks in order to protect HSX enterprise data and other information assets that access, traverse, or reside within the HSX networks.
- Network traffic shall be denied by default and allowed by exception (i.e., deny all, permit by exception).
- Network traffic shall be controlled through firewall and other network-related restrictions.

Network Architecture:

- HSX confidential data shall be logically and/or physically partitioned by means of network architecture design and connectivity except where the risk of not doing so is accepted by the HSX Board.
- Changes that affect the security posture shall be approved by the Chief Information Security Officer (CISO) and shall be documented in the network diagram in accordance with the *Change Management Policy*.
- Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. Routing controls shall also be based on positive source and destination address checking mechanisms.
- HSX's network shall be logically and physically segmented by a defined security perimeter and traffic shall be controlled based on functionality required and classification of the associated data, applications, or systems.
- Exceptions to the traffic flow policy shall be documented and shall be reviewed annually.

Network Segregation:

- Groups of information services, users, and information systems shall be segregated on networks.
- Firewalls shall be used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet) shall enforce access control policies for each of the domains.
- Network segregation architecture and security design logic shall be documented and reviewed annually.
- All HSX Servers are virtualized servers.

Network Devices:

- All network devices shall be identified and authenticated prior to establishing a connection.
- Firewalls shall be configured to deny by default (deny all, permit by exception) or control any traffic from a wireless environment into the confidential data (e.g., PHI, SSN, PII) environment.
- Servers hosting HSX internal business confidential data shall not be visible to the Internet, other external networks, nor to unprotected internal subnets.
- Internal directory services and internal IP addresses shall be protected and hidden from any external access.
- Firewalls shall validate source and destination addresses.
- Firewalls shall restrict inbound and outbound traffic to the minimum necessary.
- HSX shall utilize firewalls from at least two different vendors that employ stateful packet inspection.

- Firewall and router baseline configuration standards shall be defined and implemented and shall be reviewed every 6 months.
- The firewall rule set shall be reviewed periodically.
- Firewall, router, and network connection changes shall be approved and tested prior to implementing the changes. Changes shall be documented in accordance with the *Configuration Management Policy*.
- The domain name system (DNS) shall provide additional authentication and integrity verification assurances.
- Information systems shall perform data origin authentication and data integrity verification on the DNS responses they receive.
- MAC address authentication and static IP addresses authentication shall be implemented.
- Quarterly network scans shall be performed to identify unauthorized components and devices.

Network Routing and Connection Controls:

- Transmitted information shall be secured and, at a minimum, encrypted over open, public networks.
- Remote devices that have established a non-remote connection shall be prevented from communicating outside of that communication path (i.e., with resources in external Networks).
- Audit, logging, and monitoring capabilities shall be enabled at all managed interfaces in accordance with the *Audit, Logging, and Monitoring Policy*.

Network Diagram:

- A current network diagram shall exist and shall be updated whenever there are network changes and no less than every 6 months.
- The network diagram shall be made immediately and continuously available for HSX official operational, planning, and coordination purposes. The network diagram shall be classified as internal-use-only in accordance with the *Data Classification Policy* and shall be handled in accordance with the *Data Handling, Labeling, and Storage Policy*.

Security of Network Services:

- Security features, service levels, and management requirements for all network services shall be identified and shall be included in any network services agreement, whether these services are provided in-house or outsourced.
- The risk and impacts of the loss of network services shall be defined and documented.

- Business Associate agreements with third party service providers shall include specific obligations for security and privacy.
- Services provided by a third party service provider shall be formally managed and regularly monitored to ensure they are in accordance with the terms of the formal agreements.
- HSX shall formally authorize and document the characteristics of each connection from an information system to other information systems that are outside of the organization.
- Technical tools such as an IDS are implemented and operating on the network perimeter and other key points to identify vulnerabilities and mitigate threats and are updated on a regular basis.
- HSX uses at least 2 DNS servers located on different subnets, which are geographically separated and perform different roles (internal and external) to eliminate single points of failure and enhance redundancy.

4. Procedure

The following procedures apply to HSX internal operations only:

- Data Transfer Procedure
- Incidence Response Plan
- Information Exchange Procedures
- Network Protection Procedures

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:

- HIPAA Regulatory Reference: HIPAA §164.308(b)(1), HIPAA §164.308(b)(3), HIPAA §164.312(a)(2)(i), HIPAA §164.312(c)(1), HIPAA §164.312(c)(2), HIPAA

§164.312(d), HIPAA §164.312(e)(1), HIPAA §164.312(e)(2)(i), HIPAA §164.312(e)(2)(ii), HIPAA §164.314(a)(1), HIPAA §164.314(a)(2)(ii)

- HITRUST Reference: 09.m Network Controls, 09.n Security of Network Services
- PCI Reference: PCI DSS v3 1.1.1, PCI DSS v3 1.1.2, PCI DSS v3 1.1.3, PCI DSS v3 1.1.4, PCI DSS v3 1.1.5, PCI DSS v3 1.1.6, PCI DSS v3 1.1.7, PCI DSS v3 1.2, PCI DSS v3 1.2.1, PCI DSS v3 1.2.2, PCI DSS v3 1.2.3, PCI DSS v3 1.3, PCI DSS v3 1.3.1, PCI DSS v3 1.3.2, PCI DSS v3 1.3.3, PCI DSS v3 1.3.4, PCI DSS v3 1.3.5, PCI DSS v3 1.3.6, PCI DSS v3 1.3.7, PCI DSS v3 1.3.8, PCI DSS v3 2.1.1, PCI DSS v3 4.1.1, PCI DSS v3 11.1, PCI DSS v3 11.4

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Board HSX Management Privacy and Security Workgroup Executive Committee	**Approval Date**	September 20, 2017
Date Policy In Effect	June 3, 2015	**Version #**	1.1
Original Issue Date	June 3, 2015	**Last Review Date**	September 15, 2020 December 1, 2018 September 20, 2017
Related Documents	Access Control Policy Change Management Policy Configuration Management Policy Data Classification Policy Data Handling, Labeling and Storage Policy Encryption Glossary		