Network Protection Processes

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>December 28, 2021</td>
<td>Technical Operations</td>
</tr>
</tbody>
</table>

1. Purpose of Procedure

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. Procedure Scope

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

3. Procedures

A. The ability of users to connect to the internal network is restricted using a deny-by-default and allow-by-exception policy at managed interfaces according to the access control policy and the requirements of clinical and business applications.

   1. The user submits a request to the HSX Support Desk for internal network access.
   2. The user submits their MAC address within the ticket request
   3. The HSX Support Desk will add the MAC address within the wireless endpoint management system.
   4. The HSX Support Desk will notify the user of the change of access.

B. HSX specifies the networks and network services to which users are authorized access by the following procedure:

   1. The user submits an access request for the pertinent network to the HSX Support Desk.
   2. The request will contain access to one/more of the following HSX networks:
      - AWS: Subnet A, Subnet B, Subnet C, Subnet D
      - HSX's Internal network
      - Mirth's Network
   3. The request will proceed through the Change Management Process if the network request is to AWS or Mirth's network.
4. During the Change Management Process, the particular parts of the network of which the user will have permitted access will be defined including the specific ports, protocols, security group and/or server.

5. Upon approval, the user will be gain a user account (see Access Control Procedures) and the IP address requested.

6. In lieu of deploying IDS and IPDS on the wireless side of the firewall (WIDS), HX shall utilize MAC address filtering. With this approach there is no way to get to the wireless network and therefore IDS and IPDS are unnecessary.

C. HSX identifies and manages the external information systems that may be used by employees and other workforce members by the following procedure:

1. The HSX Technical Operations Team meets annually to identify permitted and H SX sponsored external information systems during which an owner/administrator is assigned to a particular application.

2. The permitted list is distributed to the HSX Staff as an approved list for allowed applications.

D. The HSX Participatory Agreement categorizes the necessary security controls and connections permitted for authorization. Authorized individuals are prohibited from using external information systems unless an agreement is in place beforehand.

E. Segregation between internal wired, internal wireless and external network segments is maintained through the following procedure:

1. By default, HSX segregates internal wired versus internal wireless networks.

2. The wired network is for internal phone systems only with only the MAC addresses on the allowed list permitted. The wired network is a secondary network ISP service provider separate from the wireless network.

3. The wireless network is the main network HSX staff has access to. This is separate from all other networks (any internal/external network).

4. HSX does not need to use DMZs as the networks they have are isolated to each other and any connection we make to outside networks is done externally (remote into those networks through allowed secure connections).

F. HSX logically and physically segments its networks by the following procedures:

1. By default, HSX has four separate subnetworks in four different availability zones. Thus, each network is separated logically and physically as each is hosted in a separate data center.

2. In order to access or deploy any server tickets on these networks, the HSX Change Management Process is completed.
3. During the Change Management Process, each subnet is decided upon the traffic and functionality required.
4. A security group is placed in front of subnet and/or application, defining the specification of what traffic is permitted to interact with each subnet and/or application.

G. For each network access point or external telecommunication service's managed interface, network traffic is controlled in accordance with the HSX's access control policy through firewall and other network-related restrictions through the following procedure:

1. For all HSX networks, HSX has a deny-by-default and allow-by-exception policy.
2. For all external telecommunication services, the Change Management Process is completed for any network level changes to the firewall and/or security groups.
3. Changes are evaluated by a case-by-case scenario based on access control policy and other network related restrictions.

H. Exceptions to the traffic flow policy are documented with a supporting mission/business need and duration of that need, reviewed annually, and the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

I. Remote devices establishing a non-remote connection are not allowed to communicate with external (remote) resources by the following.

1. Any HSX devices working from remote home are considered as remote device establishing a non-remote connection such as live channels, movie sites, porn sites etc. or any HSX unauthorized sites.
2. Procedures for the above should be:
   - Reviewing all unauthorized sites in Sophos
   - Adding or removing sites based on the management decisions on what sites should be allowed to access from HSX devices
   - Blacklisting or white listing those sites in Sophos
   - Enforcing them to block in HSX devices etc.
3. Servers, buckets, databases, and storage compartments that handle covered information do not allow connections from a remote IP addresses or sites.
4. A user must SSH or RDP into a separate server or instant in the network and then access the database, server or data from machine inside the network.
J. Routing controls are implemented through security gateways (e.g., firewalls) used between internal and external networks (e.g., the Internet and 3rd party networks) by the following:

1. HSX shall implement a managed interface for each external telecommunication service, i.e., transmissions of data to or from other entities external to the secure site, including to other secure sites using networks or any other communications resources outside of the physical control of the secure site to transmit information; establish a traffic flow policy for each managed interface; employ security controls as needed to protect the confidentiality and integrity of the information being transmitted.

2. Firewall rules for controlling network traffic and network traffic shall be controlled by implicit rules that are set for internal network and also globally.

3. When creating a connection with an external network, the change management committee will evaluate what security roles get in placed (ports and protocols)

4. The Change Management Committee will evaluate the routing necessary for external system to communication with internal network at minimum necessary level.

5. A global route table is used to communicate all traffic and their destinations.

K. Requirements for network routing control is based on the access control policy, including positive source and destination checking mechanisms, such as firewall validation of source/destination addresses, and the hiding of internal directory services and IP addresses by the following:

1. Every new connection or network HSX makes complies with the access control policy (and review)

2. By default, HSX firewall is deny all policy we open up a specific port for a specific IP address provided by the client. once the firewall is configured HSX will perform a connectivity test with the client to ensure that the connection is bidirectional.

3. Clients can connect to one of two destinations (1) to vendor mirth. The IP they connect to will be a public IP address NATed (network area translation) to internal addresses which are only known by the vendor. (2) to AWS. HSX provides client DNS address which is then publicly resolved to the dynamic internal IP.

L. The sensitivity of applications/systems is explicitly identified and documented by the application/system owner by the following:

1. When a new application/service is created and deployed, it is determined if the application will host or read sensitive information.
2. If the application needs to be HIPAA/HITRUST compliant, the application owner must document the services and controls the application uses and must fall underneath the BAA agreement with the underpinning vendor.

M. Unless the risk is identified and accepted by the data owner; sensitive systems shall be isolated (physically or logically) from non-sensitive applications/systems by the following:

1. HSX has a designated IP range/subnets that are used for servers or applications hosting sensitive information. Each application is hosted on its own instance inside the subnet which is both separated physically and logically
2. The data owner is required to only use HIPAA compliant services and only use services under BAA agreement with the underpinning vendor
3. All servers have individual security groups which are isolated/controlled independently.

N. Shared system resources (e.g., registers, main memory, secondary storage) are released back to the system, protected from disclosure to other systems/applications/users, and users cannot intentionally or unintentionally access information remnants by the following:

1. Mirth physically and logically separates their appliances to prevent shared resources from accessing information remnants.
2. AWS is HITRUST certified when instances are terminated or shut down, the memory will be released back into the overall system. And is protected from other services applications or systems.

O. A current network diagram (including wireless networks) exists and is updated whenever there are network changes and no less than every 6 months by the following:

1. The technical operations team meets once a quarter to review the network diagram to confirm that it is fully up to date and includes all changes which may have occurred.
2. The technical operations lead is responsible for keeping the diagram up to date whenever a change is made.
3. The final diagram is distributed out to technical team and changes communicated.

P. HSX uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection that, at a minimum, use shared
information (i.e., MAC or IP address) and access controls lists to control remote network access by the following:

1. The HSX wired network is a deny by default and will not allow network devices to communicate with the network unless the device has an approved mac address and an assigned IP address.
2. The HSX wireless network requires authentication with an SSID and a WPA2 encrypted password.
3. The wireless network is also a deny by default and will not let network devices communicate with the network unless device has approved MAC address.
4. A support ticket must be submitted with device mac address the HSX service desk will validate the device and whitelist the mac address if approved.

Q. In the event that HSX requires the implementation of a network, HSX Shall:
   a. determine who is allowed to access which network and networked services;
   b. specify the means that can be used to access networks and network services (e.g., the conditions for allowing access to a remote system);
   c. at a minimum, manages all enterprise devices remotely logging into the internal network, with remote control of their configuration;
   d. at a minimum, manages all enterprise devices remotely logging into the internal network, with installed software;
   e. at a minimum, manages all enterprise devices remotely logging into the internal network, with patch levels;
   f. publish minimum security standards for access to the enterprise network by third-party devices (e.g., subcontractors/vendors);
   g. perform a security scan before allowing access;
   h. identify the ports necessary for business and provides the rationale—or identifies compensating controls implemented—for those protocols to be non-secure;
   i. identify the services necessary for business and provides the rationale—or identifies compensating controls implemented—for those protocols to be non-secure; and
   j. identify the similar applications (e.g., protocols) necessary for business and provides the rationale—or identifies compensating controls implemented—for those protocols to be non-secure.

R. Firewall, router and network connection changes are approved and tested prior to implementing the changes by the following:

1. Network changes are documented at the setting and process level needed to be approved by change management.
2. All changes are made during off hours or maintenance windows. Changes applied and regression testing performed if passes, changes committed and then in production.
3. change
4. Tested during off hours or maintenance windows where outage times are expected to occur. Once the change is tested, the configuration can be committed and the change is considered in production.

S. Firewall and router configuration standards are defined and implemented and are reviewed every 6 months by the following:

1. On a monthly basis, the Technical Operations Team logs into the firewall, reviews and applies for any updates available for the device.
2. The Technical Operations Team identifies and reviews any alerts inside the firewall or the IDS system (firehose).
3. The Technical Operations Team reviews the statistics of usage for firewall and investigate any anomalies within the monitoring metrics.
4. The Technical Operations Team reviews the DHCP server, confirming enough leased IP addresses are available.
5. The Technical Operations Team logs into WIFI access points and identities and reviews any alerts/upgrades and applies/manages if found.
6. For all of the above, the Technical Operations Team confirms all settings are configured properly to meet the HSX hardened configuration standards.

T. Firewalls restrict inbound and outbound traffic to the minimum necessary by the following:

1. By default, HSX firewalls have deny-by default policy. In order to open up the firewalls, a change management ticket needs to be placed and approved. Traffic is limited by IP address and import.

U. Organizations shall use secured and encrypted communication channels when migrating physical servers, applications or data to virtualized servers by the following:

1. HSX has controls around only implementing virtualized servers. HSX's policies state that no physical servers should be used at any time.

V. MAC address authentication and static IP addresses are implemented by the following:

1. HSX support desk manages the network configuration and firewalls. HSX uses static ip addresses for all network devices that are stationary within the HSX office.
2. All other mobile devices are used on a 200 IP range DHCP server in which IP addresses are leased at time of connection.
3. In order to connect to the network and retrieve an IP address, you must authenticate through mac address filtering which is a whitelisted allow list.
4. Copy and paste top part (service desk)
W. HSX scans the HSX network monthly to ensure no authorized components are on the network or devices attached to it.

X. HSX utilizes firewalls from at least 2 different vendors that employ stateful packet inspection (also known as dynamic packet filtering) by the following:

1. AWS is HITRUST certified. HSX followed AWS BAA agreement which is HIPAA and HITRUST certified.
3. Ai unknown (TBD).

Y. A DMZ is established with all database(s), servers and other system components storing or processing covered information placed behind it to limit external network traffic to the internal network (08.29).

a. HSX does not host any servers on the internal network that can be accessible to the public and reviews on a regular basis that this does not happen.
b. HSX servers are hosted in the AWS infrastructure
c. Any databases, containers, buckets or other methods of storing covered information are required to be stored in a private subset. This is amazon's equivalent for setting up a DMZ zone in the server.

Z. Information systems performs data origin authentication and data integrity verification on DNS responses it receives.

1. Every external access points that HSX uses that gives the potential of a user or member to log into or to send to is required to have DNS SEC enabled to validate and monitor the authenticity of the IP address requesting.
2. HSX also requires that all external endpoints when data is being sent is encrypted using message authentication codes to assist authenticate and validate that the data being received is from the source and that there is data integrity verification.

AA. 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 by the following:

1. Currently, HSX uses the default ISPs DNS servers which are co-located and have redundancy built in in case of single point of failure.
2. HSX must receive change management approval is chose to use a different DNS server than default.
BB. HSX formally authorizes and documents the characteristics of each connection from an information system to other information systems outside the organization by the following:

1. HSX maintains a secure list of all external connections and unique data traffic flows coming into HSX.
2. HSX uses this list to manage VPNs client internal IPS and assigned ports.

CC. HSX has a business associate agreement with all providers which includes specific obligations for security and privacy, which establishes a formal agreement with external information system providers that includes specific obligations for security and privacy.

DD. For any public-facing Web applications, HSX addresses new threats and vulnerabilities on an ongoing basis and ensures these applications are protected against known attacks by one of two methods:

1. HSX implements multiple levels of security for web-facing applications for every external IP address exposed, HSX implements an IDS solution which automatically updates with new vulnerability threats pushed from the vendor.
2. HSX also uses a firewall and router with strict rules and polices with deny by default policies. HSX also uses built in technologies such as AWS shield, WAF, Cloudfront, DDOS mitigation monitoring.

EE. 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.

1. On a monthly basis, HSX Technical Operations hosts a HSX Service Desk Meeting in which network services are reviewed.
2. HSX audits its vendors to ensure that all security requirements are implemented and agreed upon by management.
3. If any discrepancies are found, they are reported during the Technical Operations Team Meeting and reported to the HSX CISO.
4. It is the responsibility of the CISO the ensure that issues/discrepancies are sent and/or escalated to the vendor.

FF. Requirements for Service Provider Management Service Agreements

MSA must:
1. require providers to comply with organizational information security requirements;
2. employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance;
3. define and document organizational oversight and user roles and responsibilities with regard to external information system services;
4. provide for organizational monitoring of security control compliance by external service providers;
5. require the use of FIPS-validated cryptographic mechanisms during transmission to protect the confidentiality and integrity of information unless otherwise protected by alternative physical measures; and
6. state the provider is responsible for the protection of covered information

**GG. VoIP Service**

Microsoft TEAMS is the only authorized VoIP service. Any new VoIP services will require authorization by the CISO via the Change Management P&P.

**4. Definitions**

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

**5. References**

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>Technical Operations</th>
<th>Contact: email</th>
<th>Version #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Board H SX Management Privacy and Security Workgroup Executive Committee</td>
<td></td>
<td>1.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current Approval Date:</th>
<th>Review Dates:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 28, 2021</td>
<td>October 28, 2023</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date Procedure to go into Effect:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>June 3, 2015</td>
<td></td>
</tr>
</tbody>
</table>
| Related Documents: | Glossary  
Network Protection Policy |