Physical Security and Access Procedures

Version	Approval Date	Owner
1.3	September 26, 2022	Chief Information Security Officer

1. Purpose of Procedure

To ensure the physical safety of all HSX employees, consultants, interns, and subcontractors as well as maintaining the physical safety of all health information contained within the HSX Suite. The organization shall train workforce members on how to properly respond to perimeter security alarms through this procedure.

2. Procedure Scope

This procedure applies to all HSX employees, consultants, interns, and subcontractors of HSX and to the 10 Penn Center Building Staff. This procedure will be reviewed as part of the onboarding process.

3. Procedures

A. When not explicitly stated below, HSX refers to the American College of Physicians (ACP) Tenant Handbook for the appropriate procedures.

B. Access Procedures

HSX uses all cloud services and relies upon AWS who is responsible to develop, approve and maintain a list of individuals with authorized access to the facility where the information system resides and issues authorization credentials for facility access.

1. HSX Staff
   - Once a new member to the HSX staff has completed the onboarding training, they will be given an access card to the building and the HSX suite.
   - Access cards will be given to consultants as well and all cards will include a picture of the individual and the HSX logo.
   - Areas containing sensitive information are controlled and restricted to authorized personnel. Authorization is obtained directly through the pertinent HSX supervisor and ultimately through the Chief Information Security Officer and Chief Policy Officer.
   - HSX employees and contractors shall only be aware of the existence of, or activities within, a secure area on a need-to-know basis.

-

2. Access Review Processes
   - A log of the visitors to the HSX Suite is reviewed monthly and maintained for at least 2 years.
     - The Operations Manager requests the ACP Staff to maintain the visitor log for at least 2 years and provide monthly updates.
     - The updates are reviewed monthly by the HSX Privacy and Security Officer.
   - An audit trail of all physical access is maintained both by ACP (entrance to the building) and by HSX (entrance to the HSX Suite) and reviewed monthly.
     - The Operations Manager requests the ACP Staff to submit a monthly update of all previous physical access to the HSX Suite.
     - The updates are reviewed monthly by the HSX Privacy and Security Officer.
   - Physical access rights and devices used for physical access to the HSX suite are reviewed every 90 days and updated accordingly.
     - Every 90 days the current access card inventory is obtained by the Operations Manager from The American College of Physicians and is matched to the current employee rosters obtained by Operational Staff. Individuals will be removed from the facility access list and access card recovered when access is no longer required.
   - HSX staff will immediately notify building security personnel if they encounter unescorted visitors and anyone not wearing visible identification

C. Maintenance Request Procedures

1. Maintenance and service operations are controlled by the HSX Operations Manager
   - The HSX Operations Manager will field all requests to the Building Management Office by phone or through ACP. Building Management would reach out to their vendorJor their contractor, for any physical changes to the HSX Suite for a quote to be passed along to HSX.
   - Records of maintenance are maintained through the ACP portal by the HSX Operations Manager and retained for a suggested 7 years (not a substitute for counsel's own research and determination as to the appropriate periods).
2. Maintenance procedures are conducted by authorized personnel fielded by the HSX Operations Manager and ACP Staff and are in accordance with the supplier-recommended intervals, insurance policies.
3. Covered information is cleared from equipment as per the Data and Media Sanitization Policy prior to maintenance unless explicitly authorized.
4. Following maintenance, security controls are checked and verified both by ACP Staff and, when applicable, HSX Staff.

5. Tools for maintenance are approved, controlled, monitored and periodically checked by ACP Staff.

D. Fire Protection Procedures

1. Fire extinguishers and detectors are installed according to current laws and regulations by ACP Staff.
2. Fire prevention and suppression mechanisms, including workforce training, are provided. The Office Manager completes Floor Warden training through ACP and conveys the pertinent training and information to HSX Staff at large.
3. Fire suppression and detection systems are supported by an independent back-up generator maintained by ACP.

E. Physical Access Control Procedures

1. Doors to the HSX Suite are electronically locked automatically.
2. Combinations and keys for organization-defined high-risk entry/exit points are changed when lost or stolen or combinations are compromised.
   - The loss is reported to the immediate HSX supervisor or the Chief Information Security Officer who will then follow the Vulnerability Management Plan protocols.
3. Intrusion detection systems (e.g., alarms and surveillance equipment) are installed on all external doors and accessible windows, the systems are monitored, and incidents/alarms are investigated by ACP Security Staff.
4. ACP Building Staff regularly tests alarms to ensure proper operation. The Operations Manager notifies HSX Staff concerning the dates of testing.

F. Additional Monitoring and Review Procedures

1. HSX actively monitors unoccupied areas within the HSX Suite at all times and sensitive and restricted areas in real time as appropriate for the area.
2. Any security threats presented by neighboring premises are identified by ACP, relayed to the Operations Manager who notifies HSX Staff at large.
3. HSX maintains an electronic log of alarm system events and reviews the logs monthly.

4. Definitions

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

5. References

Responsible Owner:	Chief Information Security Officer	**Contact: email**	Brian.Wells@healthshareexchange.org
Approved By:	Brian Wells	**Version #**	1.2

Current Approval Date:	September 26, 2022	**Review Dates:**	October 28, 2023 December 20, 201 October 9, 2021 October 20, 2020 March 19, 2019 April 1, 2017
Date Procedure to go into Effect:	September 26, 2022		
Related Documents:	American College of Physicians Tenant Manual Data and Media Sanitization Policy Document Retention and Destruction Policy Physical Security and Access Policies Vulnerability Management Policy		