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

Business Continuity Management Policy

Version	Approval Date	Owner
1.1	September 28, 2017	Technical Operations

1. Purpose

To provide management direction and a foundational framework for developing plans to ensure the safety of HealthShare Exchange (HSX) employees and the resumption of time-sensitive operations and services in the event of an emergency or disaster (e.g., fire, power or communications blackout, tornado, hurricane, flood, earthquake, civil disturbance, hacking or other security attacks etc.).

Business continuity planning relates to the establishment, maintenance, and effective implementation of plans for emergency response and post-disaster recovery. Business continuity planning ensures the availability of critical information resources and continuity of operations in emergency situations.

2. Scope

This policy applies to all employees, interns, contractors, members, participants, users, vendors and third parties who access or use HSX information assets, regardless of physical location.

IT resources include all HSX owned, licensed, leased, or managed hardware and software, and use of the HSX network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

This policy applies to information technology administered centrally, personally-owned computing devices connected by wire or wireless to the HSX network, hosted platforms and infrastructure and to off-site computing devices that connect remotely to HSX's network.

3. Policy

Business Continuity Management Policy:

- HSX shall develop, implement, test, and maintain a Business Continuity Plan (BCP) that covers all information assets that deliver or support core critical business functions.
- HSX shall require all contractors and third parties supporting HSX systems to demonstrate that business continuity and contingency plans along with disaster recovery plans are in place and are tested. HSX shall further require copies of these plans to be provided to HSX for storage and review in concert with HSX plans.
- For purposes of this policy, the BCP shall be the overall plan that facilitates sustaining critical operations during and after a business disruption. The BCP shall include, at a minimum, plans for the recovery of critical business operations in the event of a disruption due to technology failure, natural disaster, human error, terrorism or pandemic which will include the following plans specifically:
    - Continuity of Operations Plan
    - Crisis Communications Plan
    - Critical Infrastructure Protection Plan (CIP)
    - Cyber Incident Response Plan
    - Disaster Recovery Plan (DRP)
    - Information System Contingency Plans (ISCP)
    - Emergency Plan
- The BCP shall ensure that HSX maintains compliance with statutory requirements (e.g., HIPAA, HITRUST, applicable state regulations, etc.) during and after a business disruption.

Business Impact Analysis:

- HSX shall conduct a risk assessment of events that can cause interruptions to its operational processes and identify, estimate, and prioritize risks to these processes.
- HSX shall conduct a business impact analysis to identify critical operational processes and to determine recovery criticality.
    - HSX shall identify outage impacts and estimated down time.
    - HSX shall identify resource requirements.
    - HSX shall identify recovery priorities for critical systems along with recover time objectives.
- HSX shall identify mitigation options, steps, and costs.

Design and Develop the Business Continuity Plan:

- HSX shall develop and implement Information System Contingency Plans (ISCP) to ensure HSX can restore operations and establish availability of information in the required time frame following interruption to, or failure of, critical operational business processes.
- HSX shall identify roles and responsibilities and designate the BCP owner.

- HSX shall develop backup and recovery strategies for information assets according to the *Backup Policy*.
- HSX shall ensure the secure protection of confidential data, and ensure that confidentiality, accessibility and integrity are preserved.
- HSX shall identify and implement an alternate, geographically-separated site for back-up and recovery continuity support, including equipment and budget for the site.
- HSX shall develop BCP activation criteria including notification and escalation plans.
- HSX shall develop BCP deactivation criteria including notification of the return to normal operations and clean up procedures.
- HSX shall develop a communications plan at a level necessary to reasonably cover most likely scenarios including but not limited to, communications with employees, interns, contractors, members, participants, users, and third parties who access or use HSX information assets, as well as the press and public. The alternate telecommunications services shall be sufficiently separated from the primary service provider and shall be established with priority-of-service provisions.

Implement the Business Continuity Plan:

- HSX shall prepare emergency response procedures and checklists.
- HSX shall prepared detailed recovery procedures and checklists.
- HSX shall provide business continuity training and awareness to all personnel.
- HSX shall store the BCP in a geographically separated remote location.
- HSX shall develop a BCP distribution list and distribute copies of the BCP to key contingency personnel.
- HSX employees shall receive business continuity and crisis management awareness training on an annual basis.

Test the Business Continuity Plan:

- HSX shall test the BCP annually at a minimum, to ensure that it is up-to-date and effective.
- HSX shall define the type of testing exercises and testing scenarios.
- HSX shall ensure that all relevant staff members can perform their roles and carry out their responsibilities when the BCP is activated.
- HSX shall evaluate the results of BCP tests where possible and provide a report to senior leadership, including improvement recommendations and resource requirements.

Maintain the Business Continuity Plan:

- HSX shall review and update the BCP at a minimum annually.

- HSX shall update the BCP with lessons learned during the testing exercises.
- HSX shall update the BCP upon acquisition of new equipment, upgrading of systems, or other business events including but not limited to the following:
    - Changes in personnel, location, facilities, or resources
    - Revisions in legislation
    - Updated processes and procedures
    - Changes to operational and financial risk
- HSX shall distribute the updated BCP to relevant staff members.

4. Procedure

The following procedures apply to HSX internal operations only:

- Business Continuity Plan
- Disaster Recovery Plan
- Member Technology Services (MTS) Disaster Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Incidence Response Plan

5. Enforcement

- The CISO and Privacy Officer 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(a)(1)(ii)(A), HIPAA § 164.308(a)(7)(i), HIPAA § 164.308(a)(7)(ii)(A), HIPAA § 164.308(a)(7)(ii)(B), HIPAA § 164.308(a)(7)(ii)(C), HIPAA § 164.308(a)(7)(ii)(D), HIPAA § 164.308(a)(7)(ii)(E), HIPAA § 164.310(a)(2)(i), HIPAA § 164.310(d)(2)(iv), HIPAA § 164.312(a)(2)(ii), HIPAA § 164.312(c)(1)
- HITRUST Reference: 12.a Including Information Security in the Business Continuity Management Process, 12.b Business Continuity and Risk Assessment, 12.c

Developing and Implementing Continuity Plans Including Information Security, 12.d Business Continuity Planning Framework, 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans

- PCI Reference: PCI DSS v3 12.10.1

Policy Owner	Technical Operations	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Leadership Team	**Approval Date**	September 28, 2017
Date Policy In Effect	May 25, 2017	**Version #**	1.1
Original Issue Date	May 25, 2017	**Last Review Date**	September 16, 2020 December 1, 2018
Related Documents	Backup Policy Glossary		