SECURE HIT SECURE HEALTH INFORMATION TECHNOLOGY		**BUSINESS CONTINUITY PLAN POLICY**
Category: Administrative Safeguard		P & P #: 2024
Prepared By: e-Signature on file Janet Rios CEO	**Revised By: e-Signature on file** José Miranda ISSO	**Approved By: e-Signature on file** Janet Rios, CEO
Effective Date: May 2018 Last revision: Jan 2024	Expiration Date: N/A	Page 1 of 3

1.0 PURPOSE

The purpose plan is to establish and implement, as necessary, procedures to facilitate the continuity of critical business processes, ensuring that SecureHIT operates in emergency mode.

This plan works together with the Disaster Recovery Plan and Emergency Operations Mode Procedure. An operation plan in emergency mode is part of the contingency plan that establishes the processes that SecureHIT must activate to continue operating in the event of:

1.1 Fires
1.2 Floods
1.3 Bomb threat or bomb explosion
1.4 Civil disobedience
1.5 Environmental conditions
1.6 Natural disasters that may affect employees when they arrive, stay or leave work
1.7 Human Error
1.8 Equipment failure
1.9 Thief
1.10 Act of terrorism
1.11 Security Incidents
1.12 Pandemic
1.13 Earthquake
1.14 National emergency

2.0 SCOPE

This BCP policy includes analyzing potential risks, developing strategies to reduce or mitigate risk, testing the plan regularly, having documented continuity processes in place, and training employees on the procedures outlined in the BCP.

3.0 POLICY

From an activation of the contingency plan or the declaration of emergency involving operations in emergency mode, the Customer Service Officer along with the Chief Executive Officer will respond according to the Disaster Recovery Plan and this policy.

The Customer Service Officer along with the Chief Executive Officer will ensure that all the following components of this operation plan in emergency mode are ready:

- Activate the essential personnel.
- Prepare the necessary computerized equipment in an alternate place (if necessary).
- Monitor the main business systems during the emergency.
- Execute, if necessary, the procedures of the Disaster Recovery Plan.
- Ensure that every administrative operation is in service.
  - Contact Vendor List; refer to the accounting system (Intuit: QuickBooks)
    - Vendor List, PDF Document 2020
- Maintain communication with the workforce, services and systems contractors regarding technical support, if necessary.
- Establish procedures that ensure the health and safety of employees during the emergency.

The approved BCP shall be revised on an annual basis.

4.0 DEFINITIONS

Electronic Health Information (EHI) - Electronic Protected Health Information, and any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in "electronic media," as defined at 45 CFR § 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Electronic Protected Health Information (ePHI): has the meaning assigned to such term at 45 CFR § 160.103.

ePHI - "*Electronic Protected Health Information*" – Health Information in electronic form, related

to an individual or patient, as defined in the Safety Rule of the federal HIPAA law.

P&P - Policy and Procedure

5.0 Refer to Business Continuity Plan

6.0 RESPONSIBILITIES

The Customer Service Officer, under the authority delegated by the Chief Executive Officer, will ensure the implementation of all elements of this policy and related procedures.

7.0 COMPLIANCE

Failure to comply with this or any other security policy may result in disciplinary action under the Sanction Policy. SecureHIT may make referrals to relevant state and federal agencies with jurisdiction over the laws and regulations associated with the violations.

The Business Continuity Policy Plan supports SecureHIT compliance with the corresponding required implementation specification in the Administrative Safeguards category of the HIPAA Security Rule.

8.0 REVISIONS

Contact:	Title:	Date:	Comments:
Janet Rios Colon	Chief Executive Officer	Nov 2018	
Janet Rios Colon	Chief Executive Officer	Sept 2020	
Jose A. Miranda	ISSO	June 2021	
Jose A. Miranda	ISSO	June 2022	
Jose A. Miranda	ISSO	Jan 2023	
Jose A. Miranda	ISSO	Jan 2024	

9.0 REGULATORY REFERENCES

HIPAA Final Security Rule, 45 CFR 164.308(a)(7), Department of Health and Human Services.

Janet Ríos Colón

Digitally signed by Janet Ríos Colón
Date: 2024.03.13 12:05:55 -04'00'