Cherokee Indian Hospital Authority

The Mission of the Cherokee Indian Hospital is to be the provider of choice for the community by providing accessible, patient and family centered quality healthcare with responsible management of the Tribes resources.

TITLE: CIHA Contingency Planning Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 2/15/2023

LAST REVIEWED: 2/15/2023

PURPOSE:
To provide a security framework that ensures the protection of the Cherokee Indian Hospital Authority (CIHA) information and data from unauthorized access, loss, or damage while supporting the organization's business-driven needs and meeting compliance with North Carolina State departments, including the North Carolina Department of Information Technology (NCDIT), the North Carolina Department of Health and Human Services (NCDHHS), and NC Medicaid.
The information may be:

- Verbal;
- Digital; and/or
- In hardcopy form.

The information may also be:

- Individually controlled or shared;
- Stand-alone or networked;
- Used for administration, research, marketing, or other purposes.

In support of the purpose, this *Contingency Planning Policy* has been developed to ensure the confidentiality, integrity, availability (CIA), privacy, and security of the information assets of CIHA through the establishment of safeguards to prevent theft, abuse, and misuse while exceeding State departments' compliance requirements.

Failure to comply with this Policy may subject the CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce) to potential penalties and disciplinary action that may include termination of employment or contract.

STAFF GOVERNED BY THIS POLICY:
This Policy applies to all:

- CIHA workforce;
- CIHA vendors and subcontractors, who process, store, transmit, and have connectivity to the Information Technology (IT) infrastructure.

POLICY:
[NIST CP-1]
Note CP = Acronym used by NIST for Contingency Planning
CIHA shall implement and maintain a Contingency Planning Policy in compliance with National Institute of Standards and Technology (NIST) and State departments. This Policy shall be reviewed annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary.

The *CIHA Contingency Planning Policy* shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a contingency planning policy and procedural guidelines;
- Coordination of contingency plan testing and exercises;
- Establishment of an alternate storage site for systems;
- Establishment of an alternate processing site;
- Establishment of alternate telecommunications services;
- Conduct secure backups of system-level information;
- Provide for the recovery and reconstitution of mission essential functions (MEFs) and critical business functions.

DEFINITIONS:
Chief Executive Officer (CEO)
The Chief Executive Officer (CEO) is the executive sponsor for CIHA who provides direction on major hospital policies, including, but not limited to, strategic, financial, risk management, infrastructure, regulatory, and governance issues. The CEO is responsible for delegation of tasks needed to ensure CIHA information security (IS) and cyber risks are managed through an appropriate governance committee. The CEO shall also ensure that both strategic and operational processes are empowered and supported. The CEO will monitor progress on all major initiatives.

Chief Information Officer (CIO)
The Chief Information Officer (CIO) is responsible for CIHA's overall information technology strategy and operations. The CIO delegates responsibility for information technology strategy and information technology operations activities, as appropriate. The CEO authorizes the CIO to

pursue appropriate activities and actions, which help achieve the strategy and operations objectives consistent with this Policy.

Chief Information Security Officer (CISO)
The Chief Information Security Officer (CISO) is responsible for ensuring that CIHA information is protected. The CISO will delegate responsibility to steadfast individuals for approving and reviewing access rights to information. The CISO is responsible for ensuring that CIHA's security objectives are achieved. The CEO authorizes the CISO to pursue appropriate activities and actions that are consistent with this Policy, which contribute to achieving CIHA's security objectives.

CIHA Workforce
CIHA workforce includes all full-time or part-time CIHA staff/personnel/agents/employees (i.e., contractors, volunteers, interns, trainees, students, contract employees/workers, other third parties, guests), non-employees, and other persons/individuals whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

National Institute of Standards and Technology (NIST)
NIST is one of the nation's oldest physical science laboratories. NIST provides technology, measurement, and standards for the smallest to the largest technologies. CIHA has adopted the Cyber Security Framework (CSF) provided by NIST, which provides guidance on how to prevent, detect, and respond to cyberattacks.

Procedural Guidelines
Guidelines for developing operational procedures.

PROCEDURAL GUIDELINES:
CIHA ensures that all applicable users follow the procedural guidelines for purposes of complying with CIHA policies.

Contingency Plan Policy and Procedural Guidelines
[NIST CP-1]
Internal Controls:
All CIHA information assets must meet the required security controls defined in this Policy that are based on NIST. This Policy addresses CIHA's requirements, which will be used to implement the contingency planning process and the family of contingency planning security controls. The contingency planning process is required to ensure that all information systems are designed and configured using controls sufficient to safeguard CIHA's information systems. CIHA has adopted the Contingency Planning principles established in NIST, "Contingency Planning" control guidelines, as the official standards for this security domain. The "CP" designator identified in each control represents the NIST-specified identifier for the Contingency Planning control family. NIST outlines the Contingency Planning requirements that CIHA must implement and maintain in order to be compliant with this Policy.

CIHA develops, documents, disseminates, implements, and maintains this Policy to all covered personnel involved in the acquisition, development, operation, and cybersecurity maintenance of information systems, technology devices, and supporting infrastructure:

i. This Policy to address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
ii. The Contingency Planning procedures must include the necessary controls to facilitate the implementation of this Policy.

Policies and procedures are a critical component of CIHA's system of internal controls, which helps to ensure that all personnel have a clear understanding of roles, responsibilities, acceptable uses, and other important information that relates to contingency planning in accordance with information security's best practices. As such, policies and procedures relating to the stated criteria herein are to be reviewed and updated on an annual basis to ensure that their overall adequacy and sufficiency meets CIHA's needs.

Contingency Plan
[NIST CP-2]

CIHA's information assets shall be available to authorized users when needed. CIHA is required to manage information technology risks appropriately as required in state and federal laws. CIHA shall develop a Contingency Plan/Disaster Recovery Plan for the recovery of information assets for which CIHA is named as owner for all known threats to information system availability, including natural disasters, accidents, malicious destruction, failures, and denial of services. Management shall coordinate Contingency Plan development with organizational elements responsible for formally documenting the Business Continuity (BC) and Disaster Recovery (DR) Plan that covers all of CIHA's critical applications and includes procedures or references to procedures to be used for the recovery of systems that perform CIHA's MEFs and critical business processes.

The four (4) categories of application criticality are as follows:

- Hospital-wide Critical;
- Department Critical;
- Program Critical;
- Non-Critical.

Any owner of CIHA Critical Systems shall provide disaster recovery capabilities to ensure timely recovery and restoration of service as part of their disaster recovery strategy. CIHA shall coordinate Contingency Plan development and execution with CIHA divisions and groups responsible for related plans. Plans related to Contingency Plans for CIHA information systems include, for example, BC Plans, DR Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans. CIHA Plans shall include the following:

a. Be developed prior to implementation as part of the development life cycle for technology development or deployment by CIHA to address all production processing environments and assets;
b. Identify MEFs and critical business functions and associated contingency requirements;
c. Provide recovery time and recovery point objectives, restoration priorities, and metrics and estimate the following three (3) downtime factors for consideration because of a disruptive event:
    i. Maximum Tolerable Downtime (MTD) - The amount of time MEFs/critical business functions can be disrupted without causing significant harm to CIHA's mission;
    ii. Recovery Time Objective (RTO) - The maximum amount of time that an information system resource can remain unavailable before there is an unacceptable impact on other system resources, supported MEFs/critical business functions, and the MTD;
    iii. Recovery Point Objective (RPO) - The point in time, prior to a disruption or system outage, to which MEFs/critical business functions data shall be recovered (given the most recent back-up copy of the data) after an outage;
d. Identify contingency roles, responsibilities, and assigned individuals with contact information;
e. Address eventual, full information asset restoration without deterioration of the security measures originally planned and implemented;
f. Be reviewed and approved by designated officials within CIHA;
g. Be distributed to relevant system owners and stakeholders;
h. Coordinate Contingency Planning activities with incident handling activities;
i. Be revised to address changes to CIHA, information asset, or environment of operation and problems encountered during Contingency Plan implementation, execution, or testing;
j. Protect the Contingency Plan from unauthorized disclosure and modification;
k. Address the protection of the health and safety of CIHA personnel;
l. Address the protection of CIHA assets and minimize financial, reputational, legal and/or regulatory exposure;
m. Create crisis teams and response plans for threats and incidents;
n. Require that the CIHA workforce are to be made aware of their roles and responsibilities in the BC/DR Plan and in Plan execution through training and awareness programs;
o. Coordinate with Contingency Plan Administrators and the Operations Team shall occur for all potential outages that may result in a failover or recovery situation;
p. Be reviewed and submitted to the CIHA CISO on an annual basis and as otherwise requested by the CIHA CISO;
q. Support the resumption of MEFs and critical business functions within CIHA-defined time of Contingency Plan activation;
r. Define the time for resumption of MEFs/critical business functions dependent on the severity/extent of disruptions to an information system and its supporting infrastructure;

s. Define within the Contingency Plan and the Business Impact Analysis (BIA) the time in which an information system needs to be operational to support MEFs and critical business functions.

Contingency Training
[NIST CP-3]
CIHA shall train personnel in their contingency roles and responsibilities with respect to the information assets. Training and awareness programs shall ensure that CIHA personnel understand the roles of each individual within CIHA during a disaster/or adverse situation. CIHA shall provide contingency training to information system users for the following conditions:

a. Prior to assuming a contingency role or responsibility;
b. When required by information system changes;
c. Annually, thereafter.

Contingency Plan Testing
[NIST CP-4]
CIHA shall coordinate Contingency Plan testing with CIHA departments responsible for related plans, by executing the following:

a. Developing test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration procedures;
b. Testing and/or exercising the Contingency Plan for the critical information assets annually, at a minimum, to determine the Plan's effectiveness and CIHA's readiness to execute the Plan;
c. Developing a Contingency Plan exercise based on the action report that was generated after the contingency testing and exercises;
d. Initiating corrective actions to ensure the procedures are adequate to restore/recover critical application processes.

Table 1 – Test Types:

Test Type	Description
Walk-Through	A participatory session featuring an oral walk-through of the Technology Recovery Plan and of the specific tasks documented within the Plan. This exercise should confirm the Plan's design and identify role and responsibility gaps or other weaknesses in the Plan. This type of exercise can be used on alternating years, between more complete testing for lower criticality systems.

Test Type	Description
Table-Top	A participatory session using example interruptions led by a facilitator, who presents scenarios to personnel about their roles and responsibilities in an emergency and poses questions based on the scenarios that test the integrity of the Disaster Recovery Plan, as well as the readiness of the participating personnel to respond to an adverse event.
Stand-Alone	Tests one or more specific components of a Technology Recovery Plan in isolation from other components. Focuses on data restoration with network connectivity and is usually limited to a single platform or system. It may or may not include testing application interdependencies.
Partial Integration	Tests one or more specific components of a Technology Recovery Plan. Includes testing data restoration with network connectivity and testing some interdependencies with applications and/or platforms.
Full End-to-End	Tests the Technology Recovery Plan in a technology recovery testing environment without risk to the production environment tests all components of the Technology Recovery Plan and all functionality of an application. Includes testing transactions and testing all interdependencies with other applications and/or platforms. Tests shall be conducted at alternate sites or other recovery arrangements of the testing department, personnel equipment, facilities and processes.

Alternate Storage Site

[NIST CP-6]

CIHA shall establish an alternate storage site for systems that are defined as critical, including necessary agreements to permit the storage and recovery of information asset back-up information. CIHA shall implement the following:

a. Ensure that the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site;
b. Establish a site in a location that is separate from the primary facility to ensure that the risk of a disruption (e.g., natural disasters, structural failures, hostile cyberattacks) affecting both the primary and alternate site is low or otherwise is at an acceptable level, based on an assessment of risk;
c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane,

regional power outage) with such determinations made by CIHA based on assessments of risk. Explicit mitigation actions include, for example:

i. Duplicating back-up information at other alternate storage sites if access problems occur at originally designated alternate sites;
ii. Planning for physical access to retrieve back-up information if electronic accessibility to the alternate site is disrupted.

Alternate Processing Site

[NIST CP-7]

CIHA shall do the following:

a. Establish an alternate processing site including necessary agreements to permit the resumption of information asset operations for MEFs and critical business functions within defined recovery times and recovery points when the primary processing capabilities are unavailable. Alternate processing sites shall provide a Service Level Agreement (SLA) that contains priority-of-service provisions in accordance with the information system's requirements in the event of a disruption or disaster. This may be in the form of a priority-of-service provision or through a provider with a sufficient network of facilities to ensure available capacity;
b. Ensure that equipment and supplies required to resume operations are available at the alternate site or that contracts are in place to support delivery to the site in time to support the CIHA-defined time for transfer/resumption;
c. Ensure that the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site;
d. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats;
e. Determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern;
f. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster;
g. Outline and document explicit mitigation actions within the Contingency Plan;
h. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with CIHA availability requirements (including RTOs). Priority-of-service agreements refer to negotiated agreements with service providers that ensure that CIHA receives priority treatment consistent with their availability requirements, including defined RTOs and RPOs as defined in the BIA and Contingency Plan.

Telecommunications Services

[NIST CP-8]

CIHA shall do the following:

a. Establish alternate telecommunications services with telecommunication service providers that provide communications transmission services to maintain a state of readiness or to respond to and manage any event or crisis;

b. Ensure that communications transmission services include necessary agreements to permit the resumption of information asset operations for MEFs and critical business functions within defined recovery time and recovery points when the primary telecommunications capabilities are unavailable;
c. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with CIHA availability requirements (including RTOs);
d. Request Telecommunications Service Priority [(TSP) a program that authorizes national security and emergency preparedness organizations to receive priority treatment for vital voice and data circuits] for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier;
e. Consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions;
f. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

System Backup
[NIST CP-9]
CIHA shall conduct backups of system-level information (e.g., operating system files and application software from CIHA managed laptops, workstations, servers, and user level information, such as user level files stored on a shared network drive) at a frequency that is consistent with CIHA-defined RTOs and RPOs. In addition, CIHA shall protect the confidentiality and integrity of back-up information at storage location(s).

System Backup – Testing for Reliability and Integrity
[NIST CP-9(1)]
CIHA shall test back-up information quarterly to verify media reliability and information integrity.

System Recovery and Reconstitution
[NIST CP-10]
CIHA shall do the following:
a. Provide for the recovery and reconstitution of CIHA's MEFs/processes and/or critical business services, including transaction-based information systems, to a known state after a disruption, compromise, or failure within defined RTOs and RPOs;
b. Ensure that applications categorized as CIHA Critical Systems are recommended to have viable disaster recovery support, approval, and budget in place and be exercised according to policy;
c. Ensure that plan activations are documented and recorded and that post-activation reviews are conducted to evaluate the effectiveness of the plan(s);

d. Update the plan(s) where necessary and provide a formal report to the CIHA CISO within thirty (30) days of post-activation review.