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 Cybersecurity Planning Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 7/20/2023

LAST REVIEWED: 7/20/2023

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

The purpose of the Cherokee Indian Hospital (CIHA) Cybersecurity Planning Policy is to provide a security framework that ensures the protection of the Cherokee Indian Hospital Authority (CIHA) information systems, technology devices, 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 *Cybersecurity 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/or subcontractors, who process, store, transmit, and have connectivity to the Information Technology (IT) infrastructure.

POLICY:

[NIST PL-1]

Note PL = Acronym Used by NIST for Planning

CIHA shall implement and maintain a Cybersecurity 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 Cybersecurity Planning Policy shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a planning policy and procedural guidelines;
- Development of a System Security and Privacy Plan (SSPP) that documents the structured process of planning adequate, cost-effective security protection for the CIHA information systems;
- Attestation that the CIHA security and privacy policies are available to individuals requiring access to information systems;
- Development of a Concept of Operations (CONOPS) for information systems, containing, at minimum, CIHA's intention to operate the system from an information security perspective;
- Development and maintenance of an information security architecture document.

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.

System Security and Privacy Plan (SSPP)
The SSPP provides an overview of the system's security and privacy requirements and describes the current or planned controls for meeting those requirements. The SSPP delineates responsibilities and expected behavior of all individuals who access the system.

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

Planning Policy and Procedural Guidelines
[NIST PL-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 planning process and the family of planning security controls. The 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 Planning principles established in NIST, "Planning" control guidelines, as the official standards for this security domain. The "PL" designator identified in each control represents the NIST-specified identifier for the Planning control family.

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

i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
ii. Requires that the Planning procedures 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 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.

System Security and Privacy Plans

[NIST PL-2]

An SSPP is a means to document security and privacy requirements and associated security and privacy controls that are implemented within a given system. An SSPP describes, at a high level, how the security and privacy controls and control enhancements meet those security and privacy requirements. However, detailed, technical descriptions of the specific design or implementation of the controls/enhancements are not provided. CIHA's SSPP must meet the following requirements which:

a. Include all critical information systems;
b. Are consistent with CIHA's enterprise architecture;
c. Explicitly define the authorization boundary for each system. An authorization boundary contains all components of each information system that have been authorized for operation by the CIHA CISO or delegate. However, separately authorized systems to which the information system is connected are excluded;
d. Describe the operational context of the information system in terms of mission essential functions (MEFs) and critical business functions;
e. Provide the security categorization of the information system, including supporting rationale;
f. Describe the operational environment for the information system;
g. Describe relationships with or connections to other information systems;
h. Provide an overview of the security and privacy requirements for the system;
i. Describe the security and privacy controls in place or planned for meeting those requirements, including the rationale for the decisions made during the tailoring and supplementation processes that resulted in the selected set of security and privacy controls for the information system;
j. Ensure that the plan is reviewed and approved by the CIHA CISO prior to its implementation;
k. Distribute copies of the SSPP to appropriate CIHA personnel, communicating any subsequent changes to the plan;
l. Review the SSPP for the information system semi-annually;
m. Update the SSPP to address any changes to the information system/environment of operation or any identified problems during plan implementation or security control risk assessments;
n. Explicitly define the information systems that receive, process, store, or transmit Restricted or Highly Restricted data.

CIHA shall plan and coordinate security and privacy-related activities affecting an information system with any other CIHA entity (departments, divisions, management, etc.) before conducting such activities in order to reduce the impact on other CIHA entities.

Security and privacy-related activities include, for example, security risk and vulnerability assessments, audits, hardware and software maintenance, patch management, continuous monitoring, and contingency plan testing. Advance planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process to plan and coordinate security and privacy-related activities as defined by CIHA can be incorporated, as appropriate, in the system security and privacy plans for information systems or other documents, which includes the following:

a. Security and privacy-related activities affecting the information system must be planned and coordinated before such activities are conducted in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals;
b. System owners shall identify the stakeholders and participants for each information system and security and privacy-related activity and coordinate with the following that include, but are not limited to:
    i. Business process owners;
    ii. Users;
    iii. Security personnel;
    iv. Operations support personnel;
    v. Appropriate personnel of connected systems;
c. Security and privacy-related activities that are either planned or out of cycle must take into consideration other known events or resource cycles. If necessary, alternative times must be identified and reflected in appropriate budget documents.

Rules of Behavior

[NIST PL-4]

CIHA shall make readily available to information system users the rules, which describe their responsibilities and expected behavior about information and information system usage. CIHA must receive a signed and/or acknowledged attestation from information system users, indicating that they read, understand, and agree to abide by the rules of behavior, before they are authorized access to information and the information system.

The rules of behavior are described in the *CIHA Internet and Electronic Mail Acceptable Use Policy* and Sec. 4.13. Use of phone, mail and office systems of the *CIHA Personnel Manual* and include the following:

a. The *CIHA Internet and Electronic Mail Acceptable Use Policy* must be distributed to and acknowledged in writing and/or acknowledged in an attestation by all information system users;
b. Signed acknowledgement and/or an acknowledged attestation from information system users, indicating that they read, understand, and agree to abide by the rules of behavior

in the *CIHA Internet and Electronic Mail Acceptable Use Policy*, must be received before they can gain access to information and information systems;

c. Information system users must receive training provided by the *CIHA Internet and Electronic Mail Acceptable Use Policy* before they can gain access to information and information systems;
d. Within the *CIHA Internet and Electronic Mail Acceptable Use Policy*, CIHA shall include explicit restrictions on the use of social media/networking sites and the posting of CIHA information on public websites. Sharing Restricted and Highly Restricted data on any social media/networking sites is prohibited;
e. The *CIHA Internet and Electronic Mail Acceptable Use Policy* shall be reviewed and updated annually, at minimum.

Concept of Operations

[NIST PL-7]

CIHA develops and maintains a CONOPS for each information system used by CIHA users. Each CONOPS contains, at minimum, how CIHA intends to operate that particular information system from an information security perspective and is included in the SSPP for that information system. Changes to the CONOPS will be reflected in the SSPP during ongoing updates, as well as in the information security architecture, and any other appropriate CIHA documents to be reviewed and updated semi-annually.

Security and Privacy Architectures

[NIST PL-8]

CIHA maintains and updates a security and privacy architecture document for each information system that consists of the following:

- Describing the overall philosophy, requirements, and approach to be taken to protect the CIA of organizational information;
- Describing how the security and privacy architecture integrates into and supports the enterprise architecture;
- Describing any security and privacy assumptions about and dependencies on external services.

CIHA shall review and update the security and privacy architecture annually. This allows for updates to be reflected in the enterprise architecture and ensures that these planned security and privacy architecture changes are reflected in the system security and privacy plan, the CONOPS, and organizational procurements/acquisitions.

CIHA CYBERSECURITY PLANNING POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 7/20/2023

Revision Information:

Date	Section Updated	Change
7/20/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
7/20/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA" and added "Cybersecurity" after "CIHA"
7/20/2023	Information Box	Added "Last Reviewed" date and added "Policy Owner" and identified the role
7/20/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
7/20/2023	Purpose	Added "North Carolina State departments, including NCDIT, NCDHHS, and NC Medicaid" as the entities that we must meet compliance requirements with and deleted "NCDHHS/EBCI Tribal Option Contract"
7/20/2023	Purpose	Changed "EBCI Tribal Option" to "State departments" in the following: In support of the purpose, this Policy has been developed to ensure CIA, privacy, and security of the information assets of CIHA, exceeding "State departments" compliance requirements

7/20/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"
7/20/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
7/20/2023	Policy	Added that a Planning Policy must be implemented and maintained in compliance with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"
7/20/2023	Policy	Amended the title of the "*EBCI Tribal Option Planning Policy*" by deleting "EBCI Tribal Option" and replacing it with "CIHA" and amended the Policy's title from "*Security Planning*" to "*Planning*" based on the *NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*
7/20/2023	Policy	Deleted "and procedures" as having to be reviewed annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary
7/20/2023	Policy	Deleted: "In addition, if modifications are required to meet a change in the DHHS Contract, a mutually agreed upon date shall be determined for a policy update" because this Policy now

		resides with CIHA, not EBCI Tribal Option
7/20/2023	Policy	Added "implementation and maintenance of a planning policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Planning Policy*
7/20/2023	Definitions	Amended definitions by supplementing additional language for "CEO," "CIO," "CISO," "NIST," and "SSPP" and deleted the definition for "EBCI" and "EBCI Tribal Option Contract" and added definitions for "CIHA Workforce" and "Procedural Guidelines"
7/20/2023	Procedural Guidelines	Changed the heading title from "PROCEDURES" to "PROCEDURAL GUIDELINES" and added "CIHA ensures that all applicable users follow the procedural guidelines for purposes of complying with CIHA policies"
7/20/2023	Procedural Guidelines	Updated NIST PL-1: Added the "Internal Controls" section on NIST PL-1 and included the information that CIHA develops, documents, disseminates, implements, and maintains this Policy to all covered personnel involved in the acquisition, development, operation, and maintenance of information systems and supporting infrastructure

7/20/2023	Procedural Guidelines	Added that "CIHA Planning procedures must include the necessary controls" to facilitate the implementation of this Policy
7/20/2023	Procedural Guidelines	Added "NC" to all instance of "DHHS" and deleted "EBCI Tribal Option" and added "CIHA" to all instances of "CISO"
7/20/2023	Procedural Guidelines	Added that policies and procedures are a critical component of CIHA's system of internal controls, which provides understanding to personnel about their roles, responsibilities, acceptable uses, and important information that relates to maintenance. Added that these policies and procedures are to be reviewed and updated annually
7/20/2023	Procedural Guidelines	Amended the following heading titles to reflect those in the *NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*: NIST PL-1, 2, 7, and 8 and deleted the heading title for NIST PL-2(3)(6)
7/20/2023	Procedural Guidelines	Added "and privacy" after the word "security" to all instances of "security requirements," "security controls," "security plans," and security-related activities" and changed the acronym SSP to SSPP to include "and privacy" as the first "P" to read as "System Security and Privacy Plan"

7/20/2023	Procedural Guidelines	Changed “mission and business processes” to “MEFs and critical business functions” when describing the operating context of the information system in these terms as a requirement CIHA’s SSPP must meet
7/20/2023	Procedural Guidelines	Changed “NCDHHS” to “CIHA CISO” as the responsible party who ensures that the SSPP is reviewed and approved prior to its implementation
7/20/2023	Procedural Guidelines	Changed the timeframe from “annually” to “semi-annually” as to when the SSP for the information system must be reviewed
7/20/2023	Procedural Guidelines	Added the word “risk” to “security control risk assessments” and amended “risk assessments” to “security risk assessments”
7/20/2023	Procedural Guidelines	When referring to a “signed acknowledgement,” the addition “or acknowledged attestation” was inserted
7/20/2023	Procedural Guidelines	Amended the title for the *CIHA Internet and Electronic Mail Acceptable Use Policy* and added Sec. 4.13. Use of phone, mail and office systems of the *CIHA Personnel Manual* as the rules of behavior to follow
7/20/2023	Procedural Guidelines	Deleted the word “security” before all instances of “CONOPS”

7/20/2023	Procedural Guidelines	Changed the timeframe from "annually" to "semi-annually" for any appropriate CIHA documents to be reviewed and updated that pertain to changes to the CONOPS
7/20/2023	Procedural Guidelines	Deleted "Meeting compliance with the DHHS/EBCI Tribal Option Contract" as an item for which CIHA maintains and updates a security and privacy architecture document for each information system
7/20/2023	Policy Implementation/ Revision Information	Added policy revision information table