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 Program Management 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 Authority (CIHA) Cybersecurity Program Management Policy is to provide a security framework that ensures the protection of the 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 Program Management 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 PM-1]
Note PM = Acronym used by NIST for Program Management
CIHA shall implement and maintain a Cybersecurity Program Management 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 Program Management Policy* shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a program management policy and procedural guidelines;
- Information Security Program Leadership Role: Chief Information Security Officer (CISO);
- Information Security and Privacy Resources;
- Plan of Action and Milestones (POA&M) Process;
- System Inventory;
- Measures of Performance;
- Enterprise Architecture;
- Critical Infrastructure Plan;
- Risk Management Strategy;
- Authorization Process;
- Mission and Business Process Definition;
- Insider Threat Program;
- Security and Privacy Workforce;
- Testing, Training, and Monitoring;
- Security and Privacy Groups and Associations;
- Threat Awareness Program.

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.

External (Third-Party) Service Providers

External (third-party) service providers, which include vendors, suppliers, service bureaus, contractors, interns, and other organizations, provide information system development, information technology services, outsourced applications, and network and security management.

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.

Program Management Policy and Procedural Guidelines

[NIST PM-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 program management process and the family of program management security controls. The program management 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 Program Management principles established in NIST, "Program Management" control guidelines, as the official standards for this security domain. The "PM" designator identified in each control represents the NIST-specified identifier for the Program Management 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 Program Management 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 program management 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.

Information Security Program Leadership Role

[NIST PM-2]

CIHA shall appoint a CISO with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Information Security and Privacy Resources

[NIST PM-3]

CIHA ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement. Additionally, CIHA shall employ a business case, a justification for the proposed undertaking, in order to record their sources required and to ensure information security resources are available for expenditure as planned.

Plan of Action and Milestones Process

[NIST PM-4]

CIHA implements a process for ensuring that Plan of Action and Milestones (POA&M) for the security program and associated organizational information systems are developed and maintained and that they document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations. Additionally, CIHA shall ensure that the POA&M initiatives are reported to the CIHA Security Steering Committee and that the POA&M is reviewed for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

System Inventory

[NIST PM-5]

CIHA shall develop and maintain an inventory of its information systems.

Measures of Performance

[NIST PM-6]

CIHA shall develop, monitor, and report on the results of information security measures of performance.

Enterprise Architecture

[NIST PM-7]

CIHA shall develop and maintain an enterprise architecture with consideration for information security and the resulting risk to organizational operations, assets, and other organizations.

Critical Infrastructure Plan

[NIST PM-8]

CIHA addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Risk Management Strategy

[NIST PM-9]

CIHA has a comprehensive strategy to manage risk to organizational operations, assets, and other organizations, associated with the operation and use of information systems. CIHA implements

the risk management strategy consistently across the organization and reviews and updates the risk management strategy annually or as required, to address organizational changes.

Authorization Process
[NIST PM-10]
CIHA manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and fully integrates the security authorization processes into an organization-wide risk management program.

Mission and Business Process Definition
[NIST PM-11]
CIHA defines mission and business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, and other organizations; and determines information protection needs arising from the defined mission and business processes and revises the processes as necessary, until achievable protection needs are obtained.

Insider Threat Program
[NIST PM-12]
CIHA shall implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Security and Privacy Workforce
[NIST PM-13]
CIHA has established an information security steering committee, which includes privacy workforce development and improvement program.

Testing, Training, and Monitoring
[NIST PM-14]
CIHA has implemented a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: are developed and maintained; continue to be executed in a timely manner; and will review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Security and Privacy Groups and Associations
[NIST PM-15]
CIHA has established and continues to institutionalize contact with selected groups and associations within the security community:

a. To facilitate ongoing security education and training for organizational personnel;
b. To maintain currency with recommended security practices, techniques, and technologies;

c. To share current security-related information including threats, vulnerabilities, and incidents.

Threat Awareness Program

[NIST PM-16]

CIHA shall implement a threat awareness program that includes cross-organization information-sharing capabilities.

CIHA CYBERSECURITY PROGRAM MANAGEMENT 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 Program Management Policy must be implemented and maintained in compliance with NIST and State departments and deleted “NCDHHS/EBCI Tribal Option Contract”
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 program management policy and procedural guidelines” as preventive and timely maintenance activities in the *CIHA Program Management Policy*
7/20/2023	Definitions	Amended definitions by supplementing additional language for “CEO,” “CIO,” “CISO,” and “NIST,” and deleted the definition for “EBCI” and “EBCI Tribal Option Contract” and added

		definitions for "CIHA Workforce," "External (Third-Party) Service Providers," 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 PM-1: Added the "Internal Controls" section on NIST PM-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 Program Management 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 PM-1, 2, 3, 4, 5, 6, 10, 11, 13, and 15
7/20/2023	Procedural Guidelines	Added "and privacy" after the word "security" to all instances of "Security Resources," "Security Workforce," and "Security Groups and Associations"
7/20/2023	Procedural Guidelines	Changed "senior information security officer" to "CISO" as to who CIHA appoints to coordinate, develop, implement, and maintain an organization-wide information security program
7/20/2023	Procedural Guidelines	NIST PM-3: Defined "business case" as being "a justification for the proposed undertaking"
7/20/2023	Procedural Guidelines	NIST PM-4: The party which CIHA ensures the POA&M initiatives are reported to was changed from "OMB FISMA reporting requirements" to the "CIHA Security Steering Committee"
7/20/2023	Procedural Guidelines	NIST PM-7: Deleted "organizational" as the adjective for "assets" and deleted "individuals" as entities who considerations are made for in regard to information security and the resulting risk when CIHA develops and maintains an enterprise architecture
7/20/2023	Procedural Guidelines	NIST PM-9: Deleted "individuals" as an entity who CIHA has a comprehensive strategy for to manage risk

7/20/2023	Procedural Guidelines	NIST PM-11: Changed all instances of "mission/business processes" to "mission and business processes"
7/20/2023	Procedural Guidelines	NIST PM-13: Added to the sentence that CIHA has established information security "steering committee, which includes privacy" workforce development and improvement program
7/20/2023	Procedural Guidelines	NIST PM-15: Added CIHA has established "and continues to" institutionalize contact with selected groups and associations within the security community
7/20/2023	Procedural Guidelines	NIST PM-16: changed singular "capability" to plural "capabilities" in regard to CIHA shall implement a threat awareness program that includes cross-organization information-sharing capabilities
7/20/2023	Policy Implementation/ Revision Information	Added policy revision information table