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 Personnel Security Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 5/25/2023

LAST REVIEWED: 5/25/2023

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Personnel Security 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 *Personnel Security 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 or subcontractors, who process, store, transmit, and have connectivity to the Information Technology (IT) infrastructure.

POLICY:
[NIST PS-1]
Note PS = Acronym used by NIST for Personnel Security
CIHA shall implement and maintain a Personnel Security 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 Personnel Security Policy* shall include preventive and timely cybersecurity maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a personnel security policy and procedural guidelines;
- Risk designation for positions;
- Personnel screening;
- Personnel termination;
- Personnel transfer;
- Access agreements;
- External personnel security;
- Personnel sanctions.

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.

Personnel Security Policy and Procedural Guidelines

[NIST PS-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 personnel security process and the family of personnel security controls. The personnel security 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 Personnel Security principles established in NIST, "Personnel Security" control guidelines, as the official standards for this security domain. The "PS" designator identified in each control represents the NIST-specified identifier for the Personnel Security 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 Personnel Security 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 personnel security 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.

Position Risk Designation

[NIST PS-2]

CIHA shall assign information security responsibilities as an integral part of each CIHA information security program. Information security policy and job descriptions should provide general guidance on the various security roles and responsibilities within CIHA, including the following:

a. Assign a risk designation to all system user positions and establish screening criteria for personnel filling those positions by:
    i. Considering the following areas when CIHA defines security job responsibilities for system custodians and other managers with focused security positions (e.g., security analysts and business continuity planners) by:

- Identifying and clearly defining the various assets and security processes associated with each individual system for which the position holder will be held responsible;
- Clearly defining and documenting the agreed-upon authorization levels in which the position holder will have to make enhancements, modify source code, and promote updated code;

ii. Documenting for each asset shall include the following:
- Management's assignment of system responsibility to a specific manager/custodian;
- Manager/custodian acceptance of responsibility for the system;
- Detailed description of manager/custodian responsibilities;

b. Review and revise position risk designations annually and upon position vacancy or change in position description;

c. Apply this control for positions requiring security clearances or the completion of special training, etc. that is required before access is granted to an individual;

d. Ensure that position risk designations are consistent with the requirements stated in CIHA job classification policies.

Personnel Screening

[NIST PS-3]

CIHA shall define personnel screening activities to reflect applicable federal or state laws, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions, including the following:

a. Conduct background investigations of personnel prior to authorizing access to CIHA information and information systems;

b. Rescreen personnel as needed and in compliance with CIHA's EBCI Tribal Option's personnel screening procedures;

c. Ensure that screening is consistent with the following:
   i. OSHR policy, regulations, and guidance;
   ii. Internal Revenue Service (IRS) 1075 guidance for systems containing federal tax information (FTI) for applicable State departments;
   iii. Criteria established for the risk designation of the assigned position.

Personnel Termination

[NIST PS-4]

CIHA shall do the following upon termination of the individual's employment:

a. Disable information system access immediately upon notification of termination;

b. Disable user credentials immediately upon the account owner's termination from employment for CIHA or when the account owner no longer needs access to the system or application due to a leave of absence or temporary reassignment;

c. Conduct exit interviews to ensure that terminated personnel understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Exit interviews shall include, at a minimum, a discussion of confidentiality responsibilities and potential limitations on future employment. Exit interviews may not be possible for some terminated personnel, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors;
d. Retrieve all CIHA information system-related property (e.g., keys, identification badges, CIHA-owned and -issued mobile devices, including laptops, tablets, cellular phones, and hardware authentication tokens);
e. Ensure that appropriate personnel retain access to data stored on a departing employee's information system;
f. Notify CIHA's IT service desk and the individual's manager immediately upon notification of the individual's termination or when there is the need to disable the information system accounts of an individual who is in the process of being terminated but has yet to receive such notification.

Personnel Transfer
[NIST PS-5]
CIHA shall review and confirm access authorizations to information systems facilities when personnel are reassigned or transferred to other positions within CIHA and include the following required actions:

a. Returning old keys and issuing new keys;
b. Issuing identification badges as required;
c. Closing old information system accounts and establishing new accounts;
d. Changing system access authorizations (i.e., privileges);
e. Providing access to data and accounts created or controlled by the employee in their previous job capacity;
f. Notifying appropriate personnel, as required, of this individual's change of position.

Access Agreements
[NIST PS-6]
CIHA shall complete appropriate signed access agreements for personnel requiring access to CIHA information and information systems before authorizing access. CIHA shall review and update these agreements minimally on an annual basis. Access agreements should adhere to the following:

a. Including, at a minimum:
    i. Confidentiality responsibilities;
    ii. Facility access agreements;
    iii. Acceptable use agreements;
    iv. Conflict-of-interest agreements;

b. Ensuring that personnel who require access to CIHA information and information systems:
    i. Sign appropriate access agreements prior to being granted access that include an acknowledgement that personnel have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized;
    ii. Re-sign access agreements to maintain access to CIHA information and information systems when access agreements are updated or updated annually at minimum;
c. Reviewing all employee badge authorizations quarterly to verify the correct level of facility access for each employee. This review shall be conducted by the employee's manager;
d. Acknowledging electronic signatures are acceptable for use in access agreements.

External Personnel Security

[NIST PS-7]

CIHA shall develop, document, and disseminate personnel security requirements, including security roles and responsibilities for external (third-party) service providers and monitor provider compliance. External (third-party) service provider security should adhere to the following:

a. External (third-party) service providers shall comply with CIHA personnel security policy and procedures. External (third party) service providers shall be fully accountable to CIHA for any actions taken while completing their CIHA assignments;
b. CIHA workforce overseeing the work of external (third party) service providers shall be responsible for communicating and enforcing applicable laws, as well as CIHA security policy and procedures;
c. Confidentiality responsibilities and/or a Business Associate Agreement (BAA) shall be signed by authorized representatives of the external (third party) service providers before any information technology services are delivered;
d. CIHA operational and/or restricted information must not be released to external (third party) service providers without properly executed contracts and confidentiality responsibilities. These contracts must specify conditions of use and security requirements and the access, roles, and responsibilities of external (third party) service providers before access is granted;
e. Access must be granted to external (third-party) service provider users only when required for performing work, along with the full knowledge and prior approval of the information asset owner;
f. All new connections between external (third party) service providers and CIHA shall be documented in an agreement that includes information technology security requirements for the connections. This agreement shall be signed by a CIHA employee who is legally authorized to sign on behalf of CIHA and by a representative from the external (third party) service provider who is legally authorized to sign on behalf of the external (third party) service provider. The signed document must be kept on file with the relevant groups;
g. External (third-party) service providers shall notify the CIHA CIO of any transfers or terminations of external (third-party) service providers who possess CIHA credentials or

badges or who have information system privileges as soon as transfers or terminations are known and a justification for the replacement request is submitted;

h. CIHA shall define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with personnel transferred;

i. Contracts with vendors providing offsite hosting or cloud services must require the vendor to provide CIHA with an annual independent International Organization for Standardization (ISO) 27001 (and subsequent revisions) security risk assessment report or Service Organization Controls (SOC) 2 Type II to establish compliance with North Carolina General Statutes (N.C.G.S.) 143B-1378;

j. CIHA shall monitor external (third-party) service provider compliance.

Personnel Sanctions

[NIST PS-8]

CIHA shall employ a formal sanctions process for personnel failing to comply with established information security policy and procedures. Personnel sanctions may include:

a. Notifying CIHA Human Resources immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction;

b. Ensuring that the sanctions process is consistent with CIHA employment policies.