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 Physical and Environmental Protection 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) Physical and Environmental Protection 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 *Physical and Environmental Protection 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 PE-1]

Note PE = Acronym Used by NIST for Physical and Environmental Protection

CIHA shall implement and maintain a Physical and Environmental Protection 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 Physical and Environmental Protection Policy* shall include preventive and timely cybersecurity maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a physical and environmental protection policy and procedural guidelines;
- Development of physical access controls;
- Development of physical access of authorizations.

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.

Physical and Environmental Protection Policy and Procedural Guidelines
[NIST PE-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 physical and environmental protection process and the family of physical and environmental protection security controls. The physical and environmental protection 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 Physical and Environmental Protection principles established in NIST, "Physical and Environmental Protection" control guidelines, as the official standards for this security domain. The "PE" designator identified in

each control represents the NIST-specified identifier for the Physical and Environmental Protection 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 Physical and Environmental Protection 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 physical and environmental protection 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.

Physical Access Authorizations
[NIST PE-2]

CIHA restricts user access to physical property and facilities is restricted to authorized individuals and visitors only, by using the following CIHA-defined security measures:

a. Development of access policies for authorized personnel as well as visitors to CIHA facilities;
b. Risk assessment aids in selecting the type of media and associated information within it that requires restricted access;
c. System owners must document policies and procedures about access to restricted media, personnel who are authorized to access this media, and the specific measures taken to restrict it;
d. Authorization credentials (e.g., keys, badges, identification cards, and smart cards, etc.) shall be issued to workforce who requires access to a restricted area:
    i. The level of access provided to each individual shall not exceed the level of access required to complete the individual's job responsibilities;
    ii. The level of access shall be reviewed and approved before access is granted;
    iii. Keys, badges, identification cards and smart cards, and combinations of these shall be issued to only those personnel who require access;
    iv. Any individual frequenting the CIHA facility must display either a CIHA identification (ID) badge or a current visitor badge that is numbered. These badges are the property of CIHA and are provided to employees, vendors, contractors and

visitors as a convenience. Badges must always be visible below the shoulders and above the waist;

v. Keys, other physical access devices, and combinations of these shall be secured at all times to prevent unauthorized access to CIHA facilities and assets. These shall be inventoried on a CIHA-defined frequency. The unauthorized duplication of keys is prohibited. All requests for duplicate keys shall be submitted to the CIHA Facilities Manager for review, approval, and fulfillment;

vi. Keys shall be retrieved from personnel when they retire, terminate employment, or transfer to another position;

vii. Electronic combinations for secure areas that house systems with CIHA data shall be changed at least semi-annually;

viii. Authorizations and requirements for access shall be coordinated with facility and personnel security managers, as required or needed;

e. Access lists and authorization credentials shall be reviewed and approved quarterly to ensure the following:
   i. Access shall be limited to authorized personnel only;
   ii. The level of access provided to each individual shall be consistent with the individual's job responsibilities;
   iii. Access rights shall be promptly removed for terminated and transferred personnel or for personnel no longer requiring access to the facility where the information system resides;

f. Physical access authorizations and physical access controls must be enforced to protect the CIHA information systems where Restricted or Highly Restricted data is received, processed, stored, or transmitted.

Physical Access Control

[NIST PE-3]

All sites and facilities that house CIHA information technology equipment shall be carefully evaluated and suitable controls are implemented to protect workforce and CIHA resources from environmental threats, physical intrusion, and other hazards and threats. To maintain physical access control, CIHA ensures:

a. Sites, buildings, and locations that house CIHA information technology assets to be safeguarded;

b. All locations that store restricted data shall be designed and secured in a manner that is commensurate with the information's classification status;

c. Physical access authorizations at entry/exit points to facilities where CIHA information systems that receive, process, store, or transmit restricted data reside shall be required to achieve the following:
   i. Verifying individual access authorizations before granting access to the facility;
   ii. Control ingress/egress to the facility through the use of physical access control systems/devices or guards;

d. Authorized personnel may include applicable CIHA workforce and vendors;
e. Physical access controls should include some form of visible identification such as a driver's license or some other picture identification (e.g., CIHA ID badge);
f. An audit trail of physical access for all personnel to data centers shall be maintained including entry and exit dates and times;
g. Control over the number of people who have physical access to areas housing computer equipment reduces the threats of theft, vandalism, and unauthorized system access. CIHA should consider the following measures to control and restrict access to facilities that house CIHA information systems:
    i. Access shall be restricted to personnel with authorized purposes for visiting the facility;
    ii. Instructions shall be issued to visitors explaining security requirements and emergency procedures;
    iii. Visitors shall be escorted and should wear visible identification that clearly indicates their restricted status;
    iv. Where appropriate, equipment shall be secured in lockable storage that provides physical security controls sufficient enough to protect the equipment from theft;
    v. Lockable file cabinets shall be used to store restricted data (e.g., paper documents and computer media) in a manner that is commensurate with the information's classification status;
h. Video cameras and/or access control mechanisms shall be used to monitor individual physical access to areas that house restricted data;
i. The use of personal cameras, video recorders and mobile computing devices shall be restricted from areas that house restricted data to protect the information being stored;
j. Duress alarms shall be used in areas where the safety of personnel is a concern. Alarms shall be provisioned to alert others such as staff, the police department, the fire department, etc.;
k. Videoconference calls where restricted information will be discussed shall be made in an area that is secured (i.e., offices or conference rooms where the door can be closed, and conversations cannot be overheard through thin walls);
l. Facilities that house restricted data for CIHA shall include, but are not limited to, the following security measures:
    i. Clearly defined, layered security perimeters to establish multiple barriers;
    ii. Walls (of solid construction and extending from real ceiling to real floor where necessary);
    iii. Card-controlled gates and doors;
    iv. Bars, alarms, locks, etc.;
    v. Bollards;
    vi. Video cameras and intrusion security system;
    vii. Staffed reception desk;

viii. Fire doors on a security perimeter shall be equipped with alarms, as well as devices that close the doors automatically.

Access Control for Transmission
[NIST PE-4]
CIHA shall control physical access to information system distribution and transmission lines within CIHA facilities:

a. Protective measures shall include the following:
   i. Locked wiring closets;
   ii. Disconnected or locked spare network jacks;
   iii. Protection of cabling by conduit or cable trays;
b. Publicly accessible network jacks in hospital facilities shall provide only access by default, unless additional functionality is explicitly authorized;
c. Physical access to networking equipment and cabling shall be restricted to authorized workforce.

Access Control for Output Devices
[NIST PE-5]
CIHA shall control physical access to information system output devices (e.g., computer monitors, facsimile machines, copiers, and printers) to prevent unauthorized personnel from obtaining the output by ensuring the following:

a. Where technically configurable, security functionality on printers, copiers and facsimile machines will be enabled, which will require users to authenticate with the device via a PIN or hardware token in order to access the device;
b. Physical access to output devices will be controlled by placing devices in controlled areas with keypad access controls or by limiting access to personnel with specifically authorized badges;
c. Physical access to monitors will be controlled through the use of privacy screens or by the re-positioning of monitors away from unauthorized users' view.

Monitoring Physical Access
[NIST PE-6]
CIHA shall ensure that physical access to information systems shall be monitored to detect and respond to physical security incidents by implementing the following measures:

a. Coordination with facility security management and personnel security management personnel shall occur when responsibilities are in different organizations;
b. Physical access logs shall be reviewed at least quarterly by the CIHA CISO or other designated CIHA official at management level;
c. Investigations of apparent security violations or suspicious physical access activities shall be conducted. Investigations and results of reviews shall be coordinated with CIHA's incident response protocol and shall include the following:

i. Remedial actions as identified through investigations to be developed and implemented;
ii. Incident investigations that adhere to the *CIHA Incident Response Policy* requirements on incident response;

d. Investigations of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, shall be part of CIHA's incident response procedures;

e. Operational procedures shall be developed to include how personnel respond to physical access incidents.

Monitoring Physical Access – Intrusion Alarms and Surveillance Equipment
[NIST PE-6(1)]
Physical intrusion alarms and surveillance equipment shall be installed and monitored for areas that house Highly Restricted data. Automated mechanisms to recognize potential intrusions and initiate designated response actions shall be employed.

Visitor Access Records
[NIST PE-8]
CIHA shall actively monitor the security access logs of areas housing information technology equipment by ensuring the following:

a. Visitor access records for computing facilities owned by CIHA address the following requirements:
i. Visitor's name and organization;
ii. Signature of the visitor;
iii. Verification of visitor's picture ID as well as the name or initials [e.g., initials of the guard, Human Resources (HR) staff member, or the Patient Access Registration desk staff member] of who verified the visitor's identification;
iv. Date of access;
v. Time of entry and departure;
vi. Purpose of visit;
vii. Name of CIHA personnel visited;
viii. Visitor access records shall be reviewed at least semi-annually;

b. Visitor access records for facilities housing highly restricted data shall be maintained for five (5) years. All other facilities access records shall comply with CIHA's records retention policies.

Power Equipment and Cabling
[NIST PE-9]
CIHA shall protect the power equipment and cabling for information systems from damage and destruction by:

a. Employing multiple electric feeds to avoid a single point of failure in the power supply that are physically separated to help ensure that power continues to flow in the event one (1) of the cables is cut or otherwise damaged;
b. Protecting both power and communication lines;
c. Employing automatic voltage controls for critical system components to help ensure that power continues to flow in the event voltage fluctuates to unacceptable levels and causes damage to the information system component.

Emergency Shutoff
[NIST PE-10]

CIHA shall provide the capability of shutting off power to the information system or individual system components in emergency situations by:

a. Positioning emergency power switches near emergency exits in equipment rooms to facilitate rapid power down;
b. Documenting the locations of emergency power shutoffs;
c. All necessary personnel must be informed of the emergency power shutoff locations and trained to operate the shutoffs safely;
d. Requiring emergency procedures for emergency power shutoffs to be readily available to key personnel;
e. Protecting the emergency power-off capability from accidental or unauthorized activation;
f. Positioning emergency shutoff switches in a visible location with clear labeling.

Emergency Power
[NIST PE-11]

CIHA shall protect critical information technology systems from damage and data loss by installing and routinely testing a source of continuous power that ensures that the systems continue to perform during power outages and electrical anomalies (e.g., brownouts and power spikes):

a. The three primary methods for providing continuous power are as follows:
    i. Multiple electric feeds to avoid a single point of failure in the power supply;
    ii. Uninterruptible power supply (UPS);
    iii. Backup generator(s);
b. CIHA shall examine the availability requirements (the agreed minimum up time and level of performance) for critical equipment and determine which combination of these three (3) methods best meets the needs of CIHA;
c. CIHA shall analyze the emergency power requirements for critical systems and implement solutions based on the following best practices:
    i. Use of a UPS is usually required to avoid abnormal shutdowns or to provide a clean power source during brownouts or surges. Note: Most UPS batteries do not last for more than four (4) hours after losing connection with a continuous supply of power;
    ii. In the event the UPS fails, contingency plans should include procedures to follow;

iii. UPS equipment must be periodically inspected to ensure its ability to sustain, for a predefined period, the power load of the systems and equipment it supports and that it is serviced according to the manufacturer's specifications;

d. In the event of a prolonged power failure, backup generators are usually combined with a UPS to protect critical IT systems that demand higher availability and continuous processing. Such combinations include both:
   i. Supporting an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss;
   ii. Providing continuous business operations if the cutover to the generator is too slow to provide power immediately with no interruption.

   CIHA assets and locations that require a backup generator should ensure the following:
   i. Follow contingency plan procedures in the event the backup generator fails;
   ii. Ensure the generator has the capacity to sustain the power load required by supported equipment for a prolonged period of time;
   iii. Ensure the generator is tested at least monthly according to the manufacturer's specifications;
   iv. Regularly inspect the generator to ensure it remains compliant with both safety and manufacturer requirements and has an adequate supply of fuel so that it can perform for a prolonged period of time.

Emergency Lighting
[NIST PE-12]

CIHA shall provide emergency lighting in case of a main power failure by:

a. Employing and maintaining automatic emergency lighting that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility;
b. Quarterly testing the automatic emergency lighting systems to ensure that they are fully operational;
c. Documenting the results of the test.

Fire Protection
[NIST PE-13]

CIHA shall employ security controls to assure continual service of critical production systems, including controls that alert, monitor, and log intrusions, fires, explosives, smoke, water, dust, vibrations, chemical and electrical effects, electrical supply interferences, and electromagnetic radiation. This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and network closets:

a. Where appropriate, CIHA shall provide fire-resistant storage for documents and media containing information critical to business function;

b. Most file cabinets or safes are not fire, smoke, or waterproof and a fireproof cabinet/safe may not be waterproof and may render any information that is stored in the cabinet/safe unusable; therefore, CIHA shall store information electronically;
c. Fire extinguishers must undergo an annual maintenance check, and the inspection date must be clearly labeled on each extinguisher;
d. All fire protection resources must be tested annually in accordance with local or CIHA fire regulations to ensure they can be successfully activated in the event of a fire.

Fire Protection – Suppression Systems – Automatic Activation and Notification
[NIST PE-13(2)]

a. CIHA shall install and maintain fire detection and suppression devices that are supported by an independent power source (e.g., a dry pipe sprinkler system);
b. Fire detection devices/systems should activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire for when the facility is not staffed on a continuous basis.

Environmental Controls
[NIST PE-14]

a. CIHA shall implement and maintain automatic temperature and humidity controls in the data center(s) to prevent fluctuations that could be potentially harmful to equipment;
b. CIHA shall employ temperature and humidity monitoring that provides an alarm or other notification for when temperature and humidity settings are exceeded due to heating, ventilation, and air conditioning (HVAC) failures, which may adversely impact information assets.

Water Damage Protection
[NIST PE-15]

a. CIHA shall include measures to prevent water damage in the design requirements for secure data storage;
b. The facility must have master shutoff valves that are accessible, working properly, and known to key personnel, in order to protect the information system from damage, as a result of water leakage.

Delivery and Removal
[NIST PE-16]

CIHA shall ensure that access to delivery areas (e.g. loading docks and warehouses) is restricted and possibly isolated from the information system and media libraries in order to effectively enforce authorizations for entry and exit of information system components by:

a. Authorizing, monitoring, and controlling any and all types of information system components and packages that are delivered to or removed from the facility;
b. Maintaining records of information system components and packages entering and exiting the facility.

Alternate Work Site

[NIST PE-17]

CIHA shall provide readily available alternate work sites (e.g., commercial locations, etc.) as part of contingency operations by:

a. Assessing the security controls at alternate work sites as feasible. Alternate work sites shall be equipped with any equipment needed to resume temporary operations such as telecommunications services (e.g., alternative telephone services, wireless communication services, satellite, and radio) that will allow employees to communicate with information security personnel in case of security incidents or problems;

b. Securing and protecting communications with CIHA information resources while personnel are working at alternate work sites. Remote access security requirements are defined in the Remote Access section of the *CIHA Access Control Policy*;

c. Ensuring alternate work sites meet CIHA security control requirements. If CIHA does not have direct control over the alternate work site, CIHA shall enter into a contract with the owner of the alternate work site that stipulates the access controls and protection the owner shall implement. The following shall be implemented for alternate work sites:

   i. The perimeter security and physical access controls to the site and to CIHA's data store;
   ii. Design requirements for secure data storage (i.e., fire detection and suppression equipment, HVAC, measures to prevent water damage, etc.);
   iii. Equipment being used or stored at an alternate work site must be secured when not in use;
   iv. Equipment transported in vehicles must be hidden from casual view;
   v. Equipment is prohibited from being stored in vehicles overnight;
   vi. NIST SP 800-46, Revision 1 (and all subsequent revisions) must be used as guidance for security in telework and remote access.

Location of System Components

[NIST PE-18]

CIHA must position information system components within the facility to minimize potential damage from physical and environmental hazards as well as the opportunity for unauthorized access.