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 Audit and Accountability Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 2/15/2023

LAST REVIEWED: 9/21/2023

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Cybersecurity Audit and Accountability 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 Audit and Accountability 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 AU-1]

Note AU = Acronym used by NIST for Audit and Accountability

CIHA shall implement and maintain a Cybersecurity Audit and Accountability 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 Audit and Accountability Policy* shall include preventive and timely maintenance activities that consist of: Development, documentation, dissemination, implementation, and maintenance of an audit and accountability policy and procedural guidelines;
- Comprehensive auditing and monitoring that effectively identifies necessary events to be captured by information systems;
- Reviews and updates of audited events;
- Content of audited records;
- Centralized management and configuration of the content to be captured in audit records;
- Assessment of storage capacity for audit records;
- Response to audit processing failures;
- Integration of audit review, analysis, and reporting;
- Correlation of audit review, analysis, and reporting across repositories;
- Integration of audit records with vulnerability scanning information, performance data, and information system monitoring;
- Correlation of information from audit records with information obtained by monitoring physical access;
- Automatic processing of audit records for all events of interest;

- Use internal system clocks to generate time stamps for audit records;
- Protection of audit information;
- Audit backup of separate physical systems/components with cryptographic protection and authorization for access of privileged users;
- Using auditing and capturing tools to maintain an effective chain of custody;
- Maintenance of effective protocols and support measures for ensuring audit events are logged, recorded, and reviewed;
- Review of audit records with time-correlation and standardized formats;
- Monitoring of information disclosures on any third-party sites;
- Use of session audit tools and methodologies to capture necessary information;
- Ensuring the identity of external organizations who access audit records.

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.

Native Logging
Activity logs which use a database server's built-in tools to record activity at the database, database object, and user level.

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.

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

Event Logging
[NIST AU-2]

An audit event is any observable occurrence in a CIHA information system that is significant and relevant to the security of information systems and the environments in which those systems operate. CIHA shall detect these events and protect the CIA of information systems by monitoring operational audit logs files:

a. A program for continuous monitoring and auditing of system use to detect unauthorized activity shall be implemented;
b. All network components and computer systems used for CIHA operations must have the audit mechanism enabled and include logs to record specified audit events;
c. Audit logs for information systems containing Restricted and Highly Restricted data must be audited at the operating system, software, and database levels;
d. A current, reliable baseline shall be established that can be compared to audit logs to determine whether any abnormalities are present;
e. Server and desktop and laptop computers shall be configured to audit for the following events, but not limited to:
    i. Server startup and shutdown;
    ii. Starting and stopping audit functions;
    iii. Loading and unloading services;
    iv. Installing and removing software;
    v. System alerts and error messages;
    vi. Application alerts and error messages;
    vii. Modifications to the application;
    viii. User logon and logoff;
    ix. System administration activities [e.g., use of the Windows run as or the Linux su (super user) command];
    x. Accesses to information, files, and systems;
    xi. Account creation, modification, or deletion;
    xii. Password changes;
    xiii. Modifications of access controls, such as change of file or user permissions or privileges (e.g., use of the Linux special file permissions called suid/guid and the Linux chown and su command);
    xiv. Additional security-related events, as required by the system owner or to support the nature of the supported business and applications;

xv. Clearing of the audit log file;
xvi. Remote access outside of the CIHA network communication channels [e.g., modems, dedicated virtual private network (VPN), and all dial-in access to the system];
xvii. Changes made to an application or database by a batch file;
xviii. Application-critical record changes;
xix. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);

f. Network devices (e.g., router, firewall, switch, wireless access point) shall be configured to audit for the following events:
   i. Device startup and shutdown;
   ii. Administrator logon and logoff;
   iii. Configuration changes;
   iv. Account creation, modification, or deletion;
   v. Modifications of privileges and access controls;
   vi. System alerts and error messages.

CIHA shall review and update the audited events quarterly or when a major change to a CIHA information system occurs. Over time, the events that CIHA believes should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

Content of Audit Records
[NIST AU-3]

Information systems shall be configured to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred in relation to the hardware/software components, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. CIHA information systems shall be configured to generate audit records containing sufficient information to identify, at a minimum, the following elements:

a. Date and time when the event occurred;
b. Software/hardware component of the information system where the event occurred;
c. Source and destination network addresses;
d. Source and destination port or protocol identifiers;
e. Type of event that occurred;
f. Subject identity (e.g., user, device, process context);
g. Outcome (i.e., success or failure) of the event;
h. Security-relevant actions associated with processing.

Content of Audit Records – Additional Audit Information
[NIST AU-3(1)]
System owners and business owners, in coordination with service providers for systems residing off CIHA infrastructure, shall ensure that service providers configure information systems to generate audit records, which contain the following additional elements:

a. Manufacturer-specific event name / type of event;
b. Full text recording of privileged commands;
c. Individual identities of group account users.

Central Management [NIST PL-9]
Each information system provides centralized management and configuration of the content to be captured in audit records generated by CIHA-defined information system components.

Each information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred in relation to the hardware/software components, the source of the event, the outcome of the event, the identity of any individuals or subjects associated with the event, and security-relevant actions associated with processing.

Each information system generates audit records containing the following additional elements:

a. Manufacturer-specific event name / type of event;
b. Full text recording of privileged commands;
c. Individual identities of group account users.

Audit Log Storage Capacity
[NIST AU-4]
CIHA must allocate audit record storage capacity to retain audit records for the required audit retention period of at least ten (10) years. This is to provide support for after-the-fact investigations of security incidents and to meet federal and/or state regulatory and CIHA information retention schedule requirements.

a. CIHA shall ensure that processing and storage capacity requirements are sufficient to capture and store the audit events without adversely impacting operations;
b. CIHA shall ensure that online audit logs are backed up to protected media well in advance before the online logs are filled to capacity so that no audit information is lost or overwritten.

Response to Audit Logging Process Failures
[NIST AU-5]
In the event of an audit processing failure (e.g., software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded), the following CIHA mechanisms shall be initiated:

a. Alerts must be sent to CIHA-defined personnel or roles;
b. Monitoring of system operational status using operating system or system audit logs and verification of functions and performance of the system. Logs shall identify where system process failures have taken place and provide information relative to the corrective actions that need to be taken by the system administrator;
c. A warning will be generated when allocated audit record storage volume reaches a maximum audit record storage capacity;
d. Each system should automatically alert designated personnel in the event of an audit failure or each time the audit record storage capacity for audit logs reaches seventy percent (70%), eighty percent (80%), and ninety percent (90%) respectively. This type of alert should be sent by a mechanism that allows system administrators to receive them after business hours and weekends (e.g., email or text message);
e. Once there is an audit failure or the maximum audit record storage capacity for audit logs is reached, the information system should overwrite the oldest audit records or automatically shut down to eliminate the chance of an incident, in the absence of auditing and accountability.

Response to Audit Logging Process Failures – Storage Capacity Warning
[NIST AU-5(1)]
Each CIHA information system provides a warning to the CIHA CIO within the CIHA-defined time period when allocated audit record storage volume reaches CIHA-defined percentage of repository maximum audit record storage capacity.

Response to Audit Logging Process Failures – Real-Time Alerts
[NIST AU-5(2)]
CIHA information systems provide an alert of audit processing failures within two (2) hours to CIHA CIO.

Audit Record Review, Analysis, and Reporting
[NIST AU-6]
CIHA shall detect unauthorized activity and protect the CIA of information systems by monitoring operational audit logs through the use of the following measures:

a. Designating defined personnel or roles to regularly review operational audit logs for abnormalities, including system, application, and user event logs;
b. Reporting any abnormalities and/or discrepancies discovered between the logs and the baseline to CIHA management;

c. Restricting access to audit log to only those authorized to view them, and the logs shall be protected from unauthorized modifications, if technically configurable, by use of file-integrity monitoring or change-detection software;
d. Reviewing and analyzing information system audit records at least weekly, or more frequently at the discretion of the information system owner, for indications of unusual activity related to potential unauthorized use.

Audit Record Review, Analysis, and Reporting – Automated Process Integration [NIST AU-6(1)]

CIHA shall employ automated mechanisms to integrate audit review, analysis, and reporting processes [e.g., security information and event management (SIEM) tool], which support CIHA processes for investigation and response to suspicious activities. CIHA processes that benefit from integrated audit review, analysis, and reporting includes, for example, incident response, continuous monitoring, contingency planning, and audits.

Audit Record Review, Analysis, and Reporting – Correlate Audit Record Repositories [NIST AU-6(3)]

CIHA shall analyze and correlate audit records across different repositories to gain CIHA-wide situational awareness across all three (3) tiers of risk management (i.e., organizational, mission/business process, and information system) while supporting cross-organizational awareness.

Audit Record Review, Analysis, and Reporting – Integrated Analysis of Audit Records [NIST AU-6(5)]

CIHA integrates analysis of audit records with analysis of information produced from the following areas to further enhance the ability to identify inappropriate or unusual activity:

a. Vulnerability scanning;
b. Performance data;
c. Information system monitoring.

Audit Record Review, Analysis, and Reporting – Correlation with Physical Monitoring [NIST AU-6(6)]

CIHA correlates information obtained from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. CIHA IT department reviews and analyzes information system audit records for abnormalities on a regular basis and reports findings to CIHA CISO.

Audit Record Reduction and Report Generation
[NIST AU-7]

a. CIHA shall implement audit reduction and report generation capability that does the following:
   i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents;
   ii. Does not alter the original content or time ordering of audit records;

b. Each CIHA information system shall provide the capability to process audit records for events of interest based on the standards and procedures of NIST AU-2 (Event Logging). Events of interest can be identified by the content of specific audit record fields, including, for example, identities of individuals or subjects associated with the event, event types, event locations, event times, event dates, system resources involved, internet protocol (IP) addresses involved, or information objects accessed;

c. CIHA may define audit event criteria to any degree of granularity required, including, for example, locations selectable by general networking location (e.g., by network or subnetwork) or by specific information system component.

Audit Record Reduction and Report Generation – Automatic Processing
[NIST AU-7(1)]

Each CIHA information system provides the capability to process audit records for events of interest:

a. Audit reduction and report generation capability shall be implemented that does the following:
   i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents;
   ii. Does not alter the original content or time ordering of audit records;

b. CIHA information system shall provide the capability to process audit records for events of interest based on AU-2. Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed;

c. Agencies may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.

Time Stamps
[NIST AU-8]

Internal system clocks shall be used to generate time stamps for audit records that are mapped to either Coordinated Universal Time [(UTC-the coordinated universal time scale maintained at NIST)] or Greenwich Mean Time (GMT) or local time with an offset from UTC that meets a CIHA-defined time synchronization and source.

System Time Synchronization– Synchronization with Authoritative Time Source [NIST AU-45(1)]

CIHA's information systems shall synchronize internal information system clocks at a CIHA-defined frequency to a CIHA-defined authoritative time source. This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Protection of Audit Information [NIST AU-9]

CIHA shall protect audit information and audit tools from unauthorized access, modification, and deletion. Information system protection controls include the following:

a. Writing audit trails to hardware-enforced, write-once media. Write-once, read-many (WORM) media includes, for example, Compact Disk Recordable (CD-R) and Digital Versatile Disk Recordable (DVD-R). **Protection of Audit Information – Hardware Write-Once Media [NIST AU-9(1)]**;
b. Backing up audit records onto a physically different system or system component than the system or component being audited. **Protection of Audit Information – Store on Separate Physical Systems or Components [NIST AU-9(2)]**;
c. Writing audit files to a log server on the internal network and subsequently backing them up to a secure location;
d. Using cryptographic mechanisms to protect the integrity of audit information and audit tools. Cryptographic mechanisms include, for example, signed hash functions that use asymmetric cryptography, which allows verification of the hash information. **Protection of Audit Information – Cryptographic Protection [NIST AU-9(3)]**;
e. Enforcing dual authorization for movement and/or deletion of audit information for information systems containing Restricted and Highly Restricted data.

Protection of Audit Information – Access by Subset of Privileged Users [NIST AU-9(4)]

CIHA shall authorize access to management of audit functionality to a CIHA-defined subset of privileged users. CIHA personnel with privileged access to an information system and who are also the subject of an audit by that system may affect the reliability of audit information by inhibiting audit activities or modifying audit records.

CIHA shall only authorize access to designated security administrator(s) or staff, other than the system and network administrator, to manage audit functionality. System and network administrators shall not be provided the capability to modify or delete audit log entries.

Non-Repudiation [NIST AU-10]

CIHA information systems protect against an individual (or process acting on behalf of an individual) falsely denying having performed an action. By utilizing various tools and

methodologies for auditing and capturing events on the CIHA information systems, an effective chain of custody is therefore established, creating unique identifiers that validate various information processing activities. This allows CIHA to utilize "non-repudiation services" through the use of these tools and methodologies, in order to determine if information was transmitted between parties or specific actions were taken.

To access the list of information systems deemed in scope for this Policy, refer to CIHA's A*sset Inventory List*, which provides necessary information, such as host name, description of the system, the purpose, logical/physical location and placement on the network, and other relevant information.

Audit Record Retention

[NIST AU-11]

CIHA will retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes by ensuring the following:

a. CIHA information systems shall retain audit records for at least ten (10) years per this Policy, which provides support for after-the-fact investigations of security incidents and to meet federal and state regulatory, CIHA, and state information retention schedule requirements;

b. Maintain audit records associated with known incidents, including those used for legal action, in accordance with CIHA's record retention schedule, which follows state and federal regulations, after the incident is closed;

c. Dispose of audit records when the retention time has expired, in accordance with CIHA's record retention schedule after the incident is closed.

Audit Record Generation

[NIST AU-12]

CIHA shall have the capability to generate audit records to monitor the use of information systems by employee and third-party contractor users. CIHA information systems shall do the following:

a. Provide audit record generation capability for the list of auditable events as defined in the standards and procedures of NIST AU-2. Designate CIHA personnel to select which auditable events are to be audited by specific components of the information system and generate audit records for the list of audited events defined in AU-2 with the content as defined in AU-3 (Content of Audit Records);

b. Be configured to provide audit record generation capability for the list of auditable events as defined in AU-2 with content prescribed in AU-3 on, at a minimum, the following information system components:
   i. Server, desktop and laptop computers (e.g., file and print, web, firewalls, end-user environment);
   ii. Network components (e.g., switches, wireless routers).

Audit Record Generation – System-Wide and Time-Correlated Audit Trail
[NIST AU-12(1)]
CIHA information systems compile audit records from CIHA-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within an organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.

Audit Record Generation – Standardized Formats
[NIST AU-12(2)]
CIHA information systems produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Monitoring for Information Disclosure
[NIST AU-13]
CIHA may, at any time, utilize various tools and methodologies that monitor for evidence of unauthorized information disclosure on any third-party sites, particularly when users access such third-party sites using CIHA information systems.

Tools used for monitoring include:

Internet and Electronic Mail Acceptable Use Policy:
The CIHA Internet and Electronic Mail Acceptable Use Policy provides users with explicit information and guidance pertaining to the use of Internet resources and ultimately defines what constitutes both acceptable and non-acceptable use of the Internet. The Internet is a critical resource provided by CIHA that must be adequately safeguarded at all times and with all reasonable and necessary means available. It is the responsibility of all users to read, understand, and acknowledge the contents of the *Internet and Electronic Mail Acceptable Use Policy*. Users must act responsibly when utilizing CIHA Internet resources and other additional supporting computer resources.

Social Media Policy:
The CIH Social Media Policy details the general guidelines, responsibilities, and acceptable use of social media forums. The use of these forums must be conducted with due care, using professional judgment at all times.

Monitoring tools and methodologies, the *Internet and Electronic Mail Acceptable Use Policy*, and the *Social Media Policy* are all resources used by CIHA to monitor for unauthorized information disclosure as required.

Session Audit
[NIST AU-14]
At any time, CIHA may utilize various session audit tools and methodologies that can capture necessary information for various purposes. Session audit techniques are those in which an information system provides the capability for authorized users to select a user session to capture/record or view/hear and can include monitoring keystrokes, tracking visited

websites, and recording information and/or file transfers. Session auditing activities shall be developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, state, tribal, executive orders, directives, policies, regulations, or standards.

Cross-Organizational Audit Logging

[NIST AU-16]

Cross-organizational auditing is a monitoring control that identifies external organizations and its specific users who access audit records, while ensuring the integrity of those records. CIHA will perform all necessary due-diligence and information system configuration procedures to ensure the safety and security of audit records for when an external organization and its users require and request access to those records.

Due-diligence measures are performed by the CIHA CIO and CISO in collaboration with legal and various IT personnel. System configuration procedures – those deemed necessary for allowing external organizations to access audit records – shall be administered by authorized IT personnel.

Configuration and Change Monitoring:

The implementation and use of specialized software, such as a Host Intrusion Detection System (HIDS), and/or change detection software programs to monitor servers provide the necessary capabilities to assist in capturing all of the required events previously stated in this Policy.

Configuration change monitoring tools detect any file changes made within a specified information system, which ranges from changes to commonly accessed files and folders to more granular based data, such as configuration files, executables, rules, and permissions. When a change is made, an alert is immediately generated, notifying the appropriate personnel. These tools effectively aid in capturing and forwarding all events in real-time, thus mitigating issues relating to native logging protocols, which can be accessed by users with elevated privileges on servers themselves, resulting in the disabling and modification of its services and the resulted output.

Performance and Utilization Monitoring / Microsoft Windows:

To ensure that Microsoft Windows servers are actively being monitored for all necessary performance and utilization measures, the following utilization measures are employed:

- **Central Processing Unit (CPU) Utilization**
  Identifies current, real-time capacity of the CPU and provides alerting and notification measures regarding capacity limits along with underutilization metrics.
- **Disk Utilization**
  Identifies current, real-time disk space and provides alerting and notification measures if disk space is low.
- **Memory Utilization**

Identifies current, real-time memory usage and provides alerting and notification measures if memory usage is high and/or if memory availability is low.

- **Microsoft Windows Service Monitoring**
  Monitors all critical Windows services and provides alerting and notification measures as needed.
- **Network Interface Monitoring**
  Monitors the overall health and status of the network interface.
- **Process Monitoring**
  Monitors all critical processes and provides alerting and notification measures when processes fail.

When appropriately configuring all Microsoft Windows servers, authorized personnel shall ensure that the aforementioned measures are in place via tools that provide agent-based monitoring, where a service is installed to run in the background on the system being monitored, the use of native agents on the specified information system itself, and agentless monitoring, where no service or process needs to run in the background on the system being monitored, if applicable. CIHA utilizes Microsoft's System Center Operations Manager (SCOM), an agent-based monitoring solution, as its performance and utilization monitoring tool.

CIHA CYBERSECURITY AUDIT AND ACCOUNTABILITY POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 2/15/2023

Revision Information:

Date	Section Updated	Change
2/15/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
2/15/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA"
2/15/2023	Information Box	Added "Last Reviewed" date and added that the Policy was reviewed and approved by "CIHA Executive Committee"
2/15/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
2/15/2023	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"
2/15/2023	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
2/15/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"

2/15/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
2/15/2023	Policy	Added that a Cybersecurity Audit and Accountability Policy must be implemented and maintained in compliance with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"
2/15/2023	Policy	Amended the title of the "*EBCI Tribal Option Cybersecurity Audit and Accountability Policy*" by deleting "EBCI Tribal Option" and replacing it with "CIHA"
2/15/2023	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
2/15/2023	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
2/15/2023	Policy	Added "implementation and maintenance" of an audit and accountability policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Cybersecurity Audit and Accountability Policy*
2/15/2023	Policy	Amended the bullet: "Using auditing and capturing tools to maintain an effective chain of "custody" (instead of "command")
2/15/2023	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" and "Procedural Guidelines"
2/15/2023	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"
2/15/2023	Procedural Guidelines	Updated NIST AU-1: Added the "Internal Controls" section on NIST AU-1 and included the information that 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"
2/15/2023	Procedural Guidelines	Added that "CIHA Cybersecurity Audit and Accountability procedures must include the necessary controls" to facilitate the implementation of this Policy
2/15/2023	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
2/15/2023	Procedural Guidelines	Added "NC" to all instance of "DHHS" and changed "State" to "NCDHHS"

2/15/2023	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 AU-2, 4, 5, 5(1), 5(2), 6, 6(1), 6(3), 6(5), 6(6), 7, 7(1), 12, 12(1), 12(2), 14, and 16; and deleted NIST AU-2(3) [and incorporated it into AU-2], AU-3(2) [and replaced it with PL-9], AU-8(1) [and replaced it with AU-45(1); and added the titles for AU-9(1), 9(2), and 9(3)
2/15/2023	Procedural Guidelines	Changed the timeframe from "annually" to "quarterly" for when CIHA reviews and updates the audited events or when a major change to a CIHA information system occurs
2/15/2023	Procedural Guidelines	Changed "CIHA CISO" to "CIHA CIO" as the individual who receives a warning from each information system when allocated audit record storage volume reaches a defined percentage of storage capacity; changed "CISO" to "CIO" as the individual who receives the alert of audit processing failures from CIHA information systems
2/15/2023	Procedural Guidelines	Changed "EBCI Tribal Option" to the "CIHA IT department" as the department who reviews and analyzes information system audit records for abnormalities on a regular basis and reports findings to the "CIHA CISO" [instead of the original wording of "EBCI Tribal Option management"]
2/15/2023	Procedural Guidelines	Amended the title of the *CIHA Internet and Electronic Mail Acceptable Use Policy*
2/15/2023	Policy Implementation/ Revision Information	Added policy revision information table
9/21/2023	Policy Title	Added "Cybersecurity" after "CIHA" in the title

9/21/2023	Information Box	Updated “Last Reviewed” date and added “Policy Owner” and identified the role
9/21/2023	Purpose	Added information “systems and technology devices” as items that must be protected from unauthorized access, loss, or damage
9/21/2023	Staff Governed By This Policy	Added “and/” to “CIHA vendors and/or subcontractors”
9/21/2023	Procedural Guidelines	Deleted “NIST outlines the Audit and Accountability requirements that CIHA must implement and maintain in order to be compliant with this Policy”