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 Assessment, Authorization, and Monitoring Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 1/5/2023

LAST REVIEWED: 12/16/2025

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

The purpose of this Policy is to provide a security framework that ensures the protection of the Cherokee Indian Hospital Authority (CIHA) information systems, technology devices, and data from unauthorized access, loss, or damage while supporting the organization's business-driven needs and meeting compliance with North Carolina State departments, including the North Carolina Department of Information Technology (NCDIT), the North Carolina Department of Health and Human Services (NCDHHS), and NC Medicaid. The information may be:

- Verbal;
- Digital; and/or
- In hardcopy form.

The information may also be:

- Individually controlled or shared;
- Stand-alone or networked;
- Used for administration, research, marketing, or other purposes.

In support of the purpose, this *Cybersecurity Assessment, Authorization, and Monitoring 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:

CIHA shall implement and maintain a Cybersecurity Assessment, Authorization, and Monitoring Policy in compliance with National Institute of Standards and Technology (NIST) and State departments.

Assessment, Authorization, and Monitoring Policy and Procedural Guidelines
[NIST CA-1]

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 assessment, authorization, and monitoring 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 annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary to ensure that their overall adequacy and sufficiency meets CIHA's needs.

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 assessment, authorization, and monitoring process and the family of assessment, authorization, and monitoring security controls. The assessment, authorization, and monitoring 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 Assessment, Authorization, and Monitoring principles established in NIST, "Assessment, Authorization, and Monitoring" control guidelines, as the official standards for this security domain. The "CA" designator identified in each control represents the NIST-specified identifier for the Assessment, Authorization, and Monitoring 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 Assessment, Authorization, and Monitoring procedures include the necessary controls to facilitate the implementation of this Policy.

The *CIHA Cybersecurity Assessment, Authorization, and Monitoring Policy* shall include preventive and timely cybersecurity maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of an assessment, authorization, and monitoring policy and procedural guidelines that include:
  - Security controls;
  - Control enhancements;
  - Assessment procedures to determine security control effectiveness;
- All System Interconnections are authorized using Interconnection Security Agreements (ISAs);
- A Plan of Action and Milestones (POA&M) is put in place to ensure that all control weaknesses requiring remediation are, in fact, being corrected;
- The CIHA Chief Information Officer (CIO) is the authorizing official for the information systems, and the CIHA Chief Information Security Officer (CISO) is responsible for Security Authorization;
- Continuous monitoring program ensures that an effective program is in place for monitoring all relevant policies, procedures, and practices for information systems;
- Internal System Connections are to be initially configured, provisioned, and approved by authorized personnel.

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 Governance, Risk, and Compliance (GRC) Tool
The GRC tool is used to ensure CIHA is operating within legal and ethical boundaries by managing potential risks and maintaining compliance with regulations on state and federal levels.

CIHA Workforce
The CIHA workforce, consistent with *Section 2.01 Applicability* of the CIHA Employee Handbook, includes all designated CIHA direct employees and contractors, volunteers, interns, trainees, students, third parties, non-employees, and others whose conduct, while performing work for CIHA or a business associate or covered entity, is under the direct control of CIHA and/or the business associate or covered entity, regardless of payment status.

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.

Security Information and Event Management (SIEM) Software
SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure from host systems and applications to network and security devices such as firewalls and endpoint protection filters.

The software then identifies, categorizes, and analyzes security-related incidents and events.

The software delivers on two (2) main objectives, which are to:

- Provide reports on security-related incidents and events, such as successful and failed logins, malware activity, and other possible malicious activities;
- Send alerts if analysis shows that an activity runs against predetermined rulesets, thus indicating a potential security issue.

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

Control Assessments
[NIST CA-2]

CIHA shall assess the risk associated with the CIHA organization and its information systems to determine what security requirements are applicable. The security assessments determine organizational deficiencies and the appropriate placement of each system and application within the security framework and evaluates the network resources, computing systems, data, and applications based upon their criticality. CIHA security assessments must observe the following requirements:

1. Security controls must be assessed under a Continuous Monitoring Plan, which supports a frequency as defined by the CIHA CISO at least once every three (3) years or when significant changes are made to the system or supported environment until the system is decommissioned;
2. Annual compliance and assessment reports must ensure that CIHA identifies their security deficiencies and estimated time and cost for remediation and records that information on a Corrective Action Plan (CAP). The reports may include the following:
    a. Security boundary devices [i.e., firewalls, Intrusion Detection and Prevention Systems (IDPSs)];
    b. Vulnerability management (i.e., network, application and systems scanning);
    c. Patch Management (i.e., operating systems, software, firmware updates, and bug fixes);
    d. Resource constraints identified on the CAP;
    e. Cybersecurity training/awareness deficiencies;
    f. System development life cycle (SDLC) deficiencies;
3. When changes are made to an information system, a Security Impact Analysis shall be conducted to determine the extent to which changes to the information system will affect CIHA operations. These analyses are conducted as part of the SDLC to ensure that security and privacy functional (and nonfunctional) requirements are identified and addressed during the development and testing of the system;
4. CIHA shall adhere to the following procedural guidelines when significant changes are made to the information system:
    a. Conduct a vulnerability assessment for the change;
    b. Conduct a risk assessment for the change;
    c. Document assessment results, including correction or mitigation recommendations to enable risk management and oversight activities;
    d. The security controls in the information system will be assessed on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
    e. Cloud vendors must provide a third-party independent security risk and vulnerability assessment report as an attestation of compliance.

Control Assessments-Independent Assessors:
[NIST CA-2(1)]

CIHA shall employ independent third-party assessors to conduct security controls risk assessments. Independent third-party assessors are individuals or groups who conduct impartial assessments of CIHA's information systems. To achieve impartiality, assessors should **not** do the following:

- Create a mutual or conflicting interest with the organizations where the assessments are being conducted;
- Assess their own work;
- Act as management or employees of the organizations in which they are serving;
- Place themselves in advocacy positions for the organizations acquiring their services.

CIHA CISO:

1. Develops a security assessment plan that describes the assessment's scope, including:
    a. The security controls and control enhancements, which are under assessment;
    b. Assessment procedures, which will be used to determine security control effectiveness;
    c. Assessment environment, independent third-party assessors and assessment roles and responsibilities;
2. Assesses the security controls in the information system as well as its environment of operation on an annual basis to determine the extent in which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security risk assessment report, which documents the assessment results;
4. Provides the results of the security controls risk assessment (performed by the independent third-party assessors) to the CIHA CIO and CEO.

Information Exchange
[NIST CA-3]

For dedicated connections between information systems (i.e., System Interconnections), CIHA shall carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, within the internal organization as well as the external organizations.

Authorized personnel at CIHA shall adequately determine the risks associated with information system connections and the appropriate controls employed.

- If interconnecting systems between CIHA and another third-party have the same authorizing official, a description of the interface characteristics between those interconnecting systems is to be documented in the respective security plans;
- If interconnecting systems have different authorizing officials within CIHA, that is, two different systems from CIHA are interconnecting with another third-party, then CIHA is to either develop an ISA or describe the interface characteristics between systems in the security plans for the respective systems.

Additionally, CIHA will also incorporate ISA information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations, except for those entities covered by the Business Associate Agreement (BAA).

All CIHA information systems must have authorized connections to other information systems that do the following:

1. Connect through the use of the ISAs, the BAA, service level agreement (SLA), etc.;
2. For each connection, document the interface characteristics, security requirements, incident handling procedures, roles and responsibilities, costs incurred under the agreement, and the nature of the information communicated;
3. Employ a deny-all, allow-by-exception policy for allowing systems that receive, process, store, or transmit data to connect to external information systems;
4. Monitor the information assets connections on an annual basis to verify enforcement of security requirements;
5. Adhere to the following procedures for connections to systems outside of the network:
    a. Connect through the use of an approved Memorandum of Agreement (MOA) or ISA signed by the CIHA CIO or CEO;
    b. Submit a connection request as well as a Privacy Threshold Analysis (PTA) document to the CIHA CIO and the CIHA Privacy Officer. The request shall include the following:
        i. Type of connection to be established;
        ii. Type of connection requirements;
        iii. Key personnel to help coordinate the planning efforts of the system interconnection;
        iv. Duration of the interconnection;
        v. Point of contact for the external organization requesting the interconnection of data and the level of sensitivity of the data being exchanged;
    c. Prior to system interconnection, system owners must complete a Security Impact Analysis. The results must be provided to CIHA CISO for risk determination and approval;
    d. Review and update ISAs annually at minimum or whenever there is a significant change to any of the interconnected systems;
    e. Terminate all interconnections when any of the following conditions are met:
        i. The ISA, Memorandum of Understanding (MOU)/MOA, or SLA has expired or is withdrawn;

ii. The business requirement for the interconnection no longer exists;
iii. A significant change in the environment increases the risk to an unacceptable level of operations.

Note: The controls of the permanent dedicated connections between information systems do not apply to transitory, user-controlled connections, such as website browsing.

Plan of Action and Milestones
[NIST CA-5]

As part of the security assessment that is undertaken annually, CIHA shall put in place a working and documented POA&M for ensuring that all control weaknesses requiring remediation are, in fact, being corrected. The safety and security of CIHA's information systems are highly dependent upon assessing, correcting, – and ultimately confirming – all relevant gaps and weaknesses identified during the annual security assessment. The associated POA&M for any deficiencies found is to be encompassed into CIHA's overall Risk Management program. Changes, modifications, and enhancements to controls ultimately require authorized personnel to submit change requests as needed, which is to follow a documented and formalized change control process.

1. Document the planned remedial actions to correct weaknesses or deficiencies noted during the security controls risk assessment and to reduce or eliminate known vulnerabilities in the system;
2. Update existing action plans and milestones based on the findings from security controls risk assessment, Security Impact Analysis, and continuous monitoring activities;
3. All discovered weaknesses, recommendations, and their sources of discovery shall be traceable to the related CAP. CIHA CISO shall review and validate completed CAPs to ensure that artifacts (i.e., screenshots, scan results, attestations, etc.) are in place supporting the closure of the identified weakness or deficiency. Those CAPs not meeting criteria to close shall be returned to the CIHA CISO for remediation and resubmission for closure;
4. The following information shall be included in each CAP:
    a. Type of weakness;
    b. Identity of the Agency, Division, Office responsible for resolving the weakness;
    c. Estimated funding required for resolving the weakness;
    d. Scheduled completion date for weakness remediation or mitigation;
    e. Key milestones with completion dates;
    f. Source of weakness discovery;
    g. Status of the corrective action, (i.e., Ongoing or Completed);
    h. Security Incidents;
5. Identify and document any CIHA CISO or delegate's decision to accept a weakness in a CAP;
6. CAPs must be reviewed and updated quarterly at minimum;

7. Identified weaknesses must be analyzed to determine level of risk, (i.e., Critical, High, Medium, Low);
8. Document weaknesses using the CIHA GRC tool on the following timelines:
    a. Weaknesses identified as Critical level of risk must be entered if they cannot be remediated or mitigated within seven (7) days of discovery;
    b. Weaknesses identified as High level of risk must be entered if they cannot be remediated or mitigated within thirty (30) days of discovery;
    c. Weaknesses identified as Medium level of risk must be entered if they cannot be remediated or mitigated within sixty (60) days of discovery;
    d. Weaknesses identified as Low level of risk must be entered if they cannot be remediated or mitigated within ninety (90) days of discovery;
    e. All remediated or mitigated weaknesses must have supported artifacts (i.e., screenshots, scan results, etc.).

Authorization
[NIST CA-6]

The CIHA CIO is the authorizing official for the information systems. This individual is therefore responsible for a wide range of activities relating to the information systems, such as the following:

- Ensure that the responsible individual authorizes the information asset for processing before commencing operations;
- Ensure the information system meets state, federal, and other mandates for compliance on an annual basis;
- Authorization levels shall be reviewed regularly to prevent disclosure of information through unauthorized access;
- The CIHA CIO shall consider whether granting an individual the authorization to use a system utility (i.e., disk cleanup, disk defragmenter, system restore, disk compression, and archival) may violate segregation of duties if the utility allows bypassing or overriding of segregation controls. If granting authorization to use a system utility could potentially violate segregation controls, CIHA shall enact precautions to ensure that this violation does not occur. Detailed auditing or two-person control could provide assurance that segregation of duties is maintained. System utility misuse can cause the deletion or movement of files, the deletion of system restore points, or errors to occur in registry files;
- System documentation and user procedures shall be updated to reflect changes based on the modification of applications, data structures, and/or authorization processes;
- Access shall require authentication and authorization to access needed resources, and access rights shall be regularly reviewed;
- Authorization for the operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of agreed-upon security controls;
- Provide budgetary oversight for organizational information systems and/or assume responsibility for the mission/business operations supported by those systems;
- Responsible and accountable for security risks associated with the operation and use of organizational information systems;

- Responsible for implementing continuous monitoring programs, for which critical information contained in authorization packages (i.e., security plans, security assessment reports, and POA&M) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation;
- Utilizing the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions;
- Updates the security authorization annually.

Continuous Monitoring
[NIST CA-7]

CIHA shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. This includes systems that are organically managed or cloud hosted by contracted vendors. All hardware that is either connected to the CIHA network or cloud hosted shall be configured to support CIHA management and monitoring standards.

CIHA must complete an annual security risk and vulnerability assessment of their critical systems and infrastructure to ensure that there are ongoing processes in place to assess the current posture of the environment. The Continuous Monitoring Program ensures that the CIHA environment is assessed annually at minimum. The Continuous Monitoring Program includes the following:

1. Establishment of performance metrics to be monitored;
2. Ongoing security controls risk assessments in accordance with CIHA's Continuous Monitoring Program;
3. Ongoing security status monitoring of organization-defined metrics in accordance with CIHA's Continuous Monitoring Program;
4. Correlation and analysis of security-related information generated by assessments and monitoring;
5. Response actions to address analysis results of security-related information;
6. Reporting the security status of organization and the information system to the CIHA CISO and the CIHA CIO within thirty (30) days of completion of an assessment;
7. The systems are monitored on a daily basis;
8. Monitoring assessments are performed on an annual basis;
9. Security controls risk assessments are performed on an annual basis.

The CIHA CISO and CIO, in coordination with the state's Security Liaison(s) for state data residing in non-state locations, (i.e., cloud or off-site hosted systems), shall ensure service providers do the following:

1. CIHA must ensure vendor compliance with statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval;
2. Implement the Continuous Monitoring Plan;

3. Obtain and maintain one of the following independent third-party certifications:
    a. Federal Risk and Authorization Management Program (FedRAMP);
    b. Service Organization Controls (SOC) 2 Type II;
    c. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 (and subsequent revisions) Information Security Management Standard;
    d. Health Information Trust (HITRUST);
4. Correlate and analyze system level security-related information generated by assessments and monitoring to identify weaknesses and develop corrective actions;
5. Report system-level security status to the state Security Liaison;
6. Demonstrate to State departments that ongoing continuous monitoring activities are in place and compliance is being met for the following requirements:
    a. Security;
    b. Privacy and Confidentiality;
    c. Availability (Business Continuity Management);
    d. Processing Integrity.

Continuous Monitoring Plan

CIHA has developed a Continuous Monitoring Plan, which requires that CIHA complete an annual security risk and vulnerability self-assessment of their critical systems and infrastructure and that there are ongoing processes in place to assess the current posture of the environment. The Continuous Monitoring Plan is designed as a three (3)-year plan to ensure that CIHA is assessed using the following identified assessment method:

- Independent third-party assessor.

It is CIHA's responsibility to ensure that an appropriate budget amount is requested to meet this mandate.

Within thirty (30) days of completion of an assessment, CIHA is required to provide the CIHA Security Steering Committee with the results and submit a plan to remediate the findings.

CIHA has adopted the Risk Assessment security principles established in NIST SP 800-53, using these "Risk Assessment" control guidelines as the official policy for this security domain.

Risk Management Program Activities:

The Risk Management Program at a minimum shall focus on the following five (5) types of activities:

- **Identification of Risks**
  A continuous effort to identify which risks are likely to affect business continuity and security functions and document their characteristics.

- **Analysis of Risks**
  An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.

- **Mitigation Planning**
  Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For moderate- or high-rated risks, mitigation plans should be developed, documented, and assigned to managers. Plans should include assigned manager's signatures.

- **Reporting**
  Creation of reports and results from the assessment and review with the CIHA Security Steering Committee for the remediation timeline and initiatives.

- **Tracking and Controlling Risks**
  Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

Business Continuity Risk Management Processes:

For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt CIHA operations. CIHA should identify the potential impacts to develop the strategies and justify the resources required to provide appropriate level of continuity initiatives and programs. CIHA should conduct business impact analysis activities that include the following:

a. Define CIHA's critical business functions and services;
b. Define the resources (technology, staff, and facilities) that support each critical function or service;
c. Identify key relationships and interdependencies among CIHA's critical resources, functions, and services;
d. Estimate the decline in effectiveness over time of each critical function or service;
e. Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact;
f. Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service;
g. Estimate financial losses over time of each critical function or service;
h. Estimate tangible (non-financial) impacts over time of each critical function or service;
i. Estimate intangible impacts over time of each critical function or service;
j. Document any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority (e.g., tax filing dates, reporting deadlines, etc.);
k. Identify any critical non-electronic media required to support CIHA's critical business functions and/or services;

l. Identify any interim or workaround procedures that exist for CIHA's critical business functions and/or services;
m. Assess the professional capability of third parties and ensure that they provide adequate contact with CIHA and meet CIHA's requirements. Review dependence on third parties and take actions to mitigate risk;
n. Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.

Security Risk Process:
The focus of security risk management is an assessment of those security risk outcomes that may jeopardize CIHA assets and critical business functions and/or services. CIHA shall identify those impacts to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical CIHA business functions and/or services in the event of a security incident. The lack of appropriate security measures would jeopardize CIHA critical business functions and/or services. Security Impact Analysis activities include identification of the following:

a. Federal, state, and local regulatory or legal requirements that address the security, CIA, and privacy requirements for CIHA critical business functions and/or services;
b. Restricted or highly restricted information stored in CIHA's files, as well as the potential for fraud, abuse/misuse, and/or other illegal activity;
c. Essential access control mechanisms used for requests, authorization, and access approval in support of critical CIHA critical business functions and/or services;
d. Processes used to continuously monitor and report to management on the applications, tools, and technologies CIHA has implemented to adequately manage the risk as defined by CIHA (i.e., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.);
e. CIHA's IT Change Management and Vulnerability Assessment processes;
f. Security mechanisms that are in place to protect CIHA data (e.g., the use of encryption, data masking, etc.).

Continuous Monitoring – Independent Assessment:
[NIST CA-7(1)]
CIHA shall employ independent third-party assessors to monitor the security controls in the information system on an ongoing basis. CIHA can maximize the value of security controls risk assessments during the continuous monitoring process by requiring that such assessments be conducted by independent third-party assessors with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should **not** do the following:

- Create a mutual or conflicting interest with the organizations where the assessments are being conducted;
- Assess their own work;

- Act as management or employees of the organizations they are serving;
- Place themselves in advocacy positions for the organizations acquiring their services.

Internal System Connections

[NIST CA-9]

Security compliance checks must be performed between the CIHA information systems and (separate) system components (i.e., intra-system connections), including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, internal connections for a class of components with common characteristics and/or configurations may be authorized (e.g., all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration).

CIHA CISO:

a. Authorizes internal connections for CIHA defined classes and subclasses of components to the information system;
b. Documents for each internal connection the interface characteristics, security requirements, and the nature of the data that will be included in the connection.

CIHA CYBERSECURITY ASSESSMENT, AUTHORIZATION, AND MONITORING POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 1/5/2023

Revision Information:

Date	Section Updated	Change
1/5/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
1/5/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA
1/5/2023	Information Box	Added "Last Reviewed" date and added that the Policy was reviewed and approved by "CIHA Executive Committee"
1/5/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA" and changed all instances of "organization" and "company" to "CIHA" where applicable to add specificity
1/5/2023	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"
1/5/2023	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
1/5/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"
1/5/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
1/5/2023	Policy	Added that a Cybersecurity Assessment, Authorization, and Monitoring Policy must be implemented and maintained in compliance with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"
1/5/2023	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
1/5/2023	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
1/5/2023	Policy	Added "documentation, dissemination, and implementation of an assessment, authorization, and monitoring policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Cybersecurity Assessment, Authorization, and Monitoring Policy* and added all of the bullets except for the first three
1/5/2023	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"
1/5/2023	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"
1/5/2023	Procedural Guidelines	Updated NIST CA-1: Added the "Internal Controls" section on NIST CA-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
1/5/2023	Procedural Guidelines	Added that "CIHA Cybersecurity Assessment, Authorization, and Monitoring procedures must include the necessary controls" to facilitate the implementation of this Policy
1/5/2023	Procedural Guidelines	Added "NC" to all instance of "DHHS" and deleted "EBCI Tribal Option" and added "CIHA" to all instances of "CISO"
1/5/2023	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
1/5/2023	Procedural Guidelines	Deleted information in NIST CA-2 on maintaining, documenting, and disseminating this Policy through an electronic repository to all workforce that utilize IT resources because it was redundant to information in NIST CA-1
1/5/2023	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 CA-1, 2, 2(1), 3, 5, 6
1/5/2023	Procedural Guidelines	Added "organizational deficiencies" as an item that security assessments determine
1/5/2023	Procedural Guidelines	Deleted the EBCI Tribal Option's state requirement: "As the critical nature of the data and applications increases, the security measures required to protect the data and applications also increase" and deleted the information about the "annual compliance and assessment reports [being sent] to the NCDHHS Security Representative" and any deficiencies [must be] addressed in a CAP" because this Policy now resides with CIHA, not EBCI Tribal Option
1/5/2023	Procedural Guidelines	Added "Conduct a vulnerability assessment for the change" as a procedural guideline that CIHA must adhere to when significant changes are made to the information system

1/5/2023	Procedural Guidelines	Deleted the procedural guidelines that EBCI Tribal Option must "provide the assessment results to the NCDHHS Security Representative within thirty (30) days from the completion of the assessment"
1/5/2023	Procedural Guidelines	Deleted the "i.e.," (id est): Service Organization Controls (SOC) 2 Type II]" for a "third-party independent security risk and vulnerability assessment" report that cloud vendors must provide as an attestation of compliance
1/5/2023	Procedural Guidelines	Added the word "risk" to "security controls risk assessments"
1/5/2023	Procedural Guidelines	Changed "critical functions and services" and "critical functions or services" to "critical business functions and/or services"
1/5/2023	Procedural Guidelines	Deleted "NCDHHS/EBCI Tribal Option Contract [i.e., Prepaid Health Plans (PHPs)]" when referencing the exclusion of entities covered by the Contract when incorporating ISA information into formal contracts, especially for interconnections established between federal agencies and nonfederal organizations
1/5/2023	Procedural Guidelines	Deleted "PCCM" Contract" as an authorized connection when connecting to other information systems
1/5/2023	Procedural Guidelines	Added "CIHA Privacy Officer" as someone who a connection request as well as a PTA document must be submitted to when connecting to systems outside of the network
1/5/2023	Procedural Guidelines	Deleted all of the NCDHHS/EBCI Tribal Option requirements that had to be met regarding failures in data exchanges and interfaces that are not resolved immediately through normal operations
1/5/2023	Procedural Guidelines	Changed "State Security Liaisons" with "CIHA CISO" as the person responsible for reviewing and validating completed CAPs to ensure that artifacts are in place supporting the closure of the identified weakness or deficiency and for remediation and resubmission for closure
1/5/2023	Procedural Guidelines	Deleted "EBCI Tribal Option GRC tool" and replaced it with "the risk assessment form" as what to use when documenting weaknesses
1/5/2023	Procedural Guidelines	Added "(and subsequent revisions)" to include future publications of ISO/IEC 27001
1/5/2023	Procedural Guidelines	Changed "NCDHHS" to "State departments" as the entities that service providers must demonstrate to that continuous monitoring activities are in place and compliance is being met for specific requirements
1/5/2023	Procedural Guidelines	Changed "EBCI Tribal Option" to "CIHA" when referencing the "Continuous Monitoring Program"
1/5/2023	Policy Implementation/ Revision Information	Added policy revision information table
9/7/2023	Policy Title	Added "Cybersecurity" after "CIHA" in title
9/7/2023	Information Box	Added "Last Reviewed" date and added "Policy Owner" and identified the role
9/7/2023	Purpose	Added information "systems and technology devices" as items that must be protected from unauthorized access, loss, or damage
9/7/2023	Staff Governed By This Policy	Added "and/" to "CIHA vendors and/or subcontractors"
9/7/2023	Procedural Guidelines	Added "as it applies" and "technology devices" to "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"
9/7/2023	Procedural Guidelines	Deleted "NIST outlines the Assessment, Authorization, and Monitoring requirements that CIHA must implement and maintain in order to be compliant with this Policy"
9/20/2024	Policy	Added "cybersecurity" before "maintenance" to provide further clarification for readers
9/20/2024	Policy and Procedural Guidelines	Moved NIST CA-1 language from the Procedural Guidelines section and combined it with the NIST CA-1 language in the Policy section
12/16/2025	Policy Header	Updated the CIHA seal
12/16/2025	Definitions	Added "CIHA GRC tool" and amended "CIHA Workforce" definition
12/16/2025	Procedural Guidelines	Deleted "risk assessment form" and replaced it with "CIHA GRC tool" as what to use when documenting weaknesses
12/16/2025	Procedural Guidelines	NIST CA-5 – added "Critical level" as a weakness that must be documented on the following timeline: must be entered if they cannot be remediated or mitigated within 7 days of discovery
12/16/2025	Procedural Guidelines	NIST CA-7 – Changed "quarterly" to "annual" basis for when security controls risk assessments are performed
12/16/2025	Procedural Guidelines	NIST CA-7 – Added "HITRUST" as an independent third-party certification