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 Risk Assessment Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 7/20/2023

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 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 Risk Assessment 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 Risk Assessment Policy in compliance with National Institute of Standards and Technology (NIST) and State departments.

Risk Assessment Policy and Procedural Guidelines
[NIST RA-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 risk assessment 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 risk assessment process and the family of risk assessment security controls. The risk assessment 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 Risk Assessment principles established in NIST, "Risk Assessment" control guidelines, as the official standards for this security domain. The "RA" designator identified in each control represents the NIST-specified identifier for the Risk Assessment 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 Risk Assessment procedures include the necessary controls to

facilitate the implementation of this Policy.

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

- Development, documentation, dissemination, implementation, and maintenance of a risk assessment policy and procedural guidelines;
- Categorization of security requirements for information technology vendor partners;
- Development of a risk assessment, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- Requirement of vulnerability scanning;
- Ability to readily update vulnerability scanning tools;
- Ability to readily update information system vulnerabilities when they are identified and reported;
- Ensure privileged access authorization for vulnerability scanning activities.

DEFINITIONS:

Access to Organizational Information Systems

Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., non-local access).

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
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.

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.

Security Categorization
[NIST RA-2]
CIHA must address the following requirements:

a. Categorization of information and the information systems in accordance with applicable state and federal laws, policies, regulations, standards, and guidance. NIST SP 800-60 (and subsequent revisions) serve as a guidance for the categorization process. The security categories are based on the potential impact on CIHA should certain events occur that jeopardize the CIA of the information and information systems needed by CIHA to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The impact to CIHA, workforce and other external entities must be considered during the security categorization process;
b. System owners need to be involved with the security categorization of an information system if they are responsible for:
    i. Any interconnected system dependencies (i.e., systems that share information);
    ii. A system that may inherit a security control from their respective system;
c. Inclusion of the security categorization process as a part of the system development life cycle (SDLC). The security categorizations shall be developed early in the initiation stage

ensuring the planning and implementation of the appropriate security controls throughout the SDLC;

d. Assurance that the security categorization decision is reviewed and approved by the authorized or designated representative;
e. Documents shall be updated to address changes to an information system/environment of operation or problems identified during plan implementation or security controls risk assessments;
f. The business owner, system owner, and CIHA IT staff must assist with the development of the security categorization.

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by CIHA. CIHA's information shall be classified and handled in a manner that protects the information from unauthorized or accidental disclosure, modification, or loss. CIHA must use the North Carolina Department of Information Technology's Data Classification and Handling Policy for detailed requirements for the storage, labeling, classification, and destruction of CIHA data.

Risk Assessment

[NIST RA-3]

Risk assessments consider risks posed to CIHA operations and assets or individuals from external parties, including, but not limited to, entities such as:

- Service providers;
- Contractors operating information systems on behalf of CIHA;
- Individuals accessing CIHA data and information systems;
- Outsourcing organizations.

CIHA conducts security risk and vulnerability assessments to evaluate the level of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

CIHA conducts security risk and vulnerability assessments at minimum annually, or whenever there are significant changes to the critical information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

A CIHA-wide third-party independent security risk and vulnerability assessments (Restricted or Highly Restricted) and associated security controls is conducted at a minimum every three (3) years:

a. All assessment results will be provided to the CIHA Security Steering Committee within thirty (30) days of completion;
b. The security risk and vulnerability assessments must consider risks posed to CIHA's operations, assets, or individuals from external parties, including, but not limited to, the following:
    i. Organizations, such as foreign nations and business competitors, that may have an interest in information supplied to CIHA;

ii. Service Providers:
    - Contractors operating information systems on behalf of CIHA;
    - Individuals accessing CIHA's information systems;
    - Outsourcing entities [e.g., cloud service providers (CSPs)]:
        - CIHA needs to obtain prior approval from the CIHA CIO before contracting with cloud-hosted solutions or off-site hosting;
        - CIHA must ensure vendor compliance with CIHA security policies and State departments;
        - CIHA shall ensure that contract language requires vendors to provide, an attestation to their compliance, an industry recognized third-party independent security risk and vulnerability assessments report. Examples of acceptable attestation reports include SOC 2 Type II and ISO 27001 (and subsequent revisions);
        - Procurement language must also require, in addition to initial validation, that cloud/vendor must annually provide CIHA validation of their continued compliance to CIHA policies and procedures. This requirement includes all vendors supporting Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS). Examples of acceptable assessment reports include SOC 2 Type II and ISO 27001 (and subsequent revisions). CSPs must demonstrate to CIHA that continuous monitoring activities are in place and that compliance is being met;

c. When planning and budgeting for security risk and vulnerability assessments, CIHA must follow these requirements:
    i. Multi-year planning and budgeting techniques must be used;
    ii. Annual assessments must be included in information system budgets and planning;
    iii. Other significant, planned activities must be considered in budgets and planning (e.g., life cycle activities, enhancements, audits) to ensure cost effective use of resources;
    iv. All information systems in CIHA must be considered to ensure resource efficiencies;
    v. Assessments must be coordinated between information systems with security control inheritance and other relational dependencies;
    vi. CIHA shall conduct security risk and vulnerability assessments using NIST SP 800-53 controls that includes at a minimum their critical systems;
    vii. CIHA may perform an annual self-assessment of their organization or system if they are storing, processing, or transmitting data that is classified as Low or Medium. Independent third-party security risk and vulnerability assessments shall be completed every three (3) years for systems storing, processing, or transmitting data classified as Medium;
    viii. If CIHA or a system stores, processes, or transmits data classified as Highly Restricted, CIHA shall use an independent third-party assessor to conduct the annual assessment;

ix. An independent third-party assessor shall assess the security controls in the information system using NCDIT's security risk assessment template, which can be accessed at https://it.nc.gov. (Using the Search box, type "ESRMO-SAR Template." Once this template is open, click on the embedded link to "Table 4-1 – Risk Exposure" to access the security risk assessment template.);

d. A Plan of Action and Milestones (POA&M) or Corrective Action Plan (CAP) for the system documenting the planned, remedial actions to correct weaknesses or deficiencies in security controls and to reduce or eliminate known vulnerabilities must be developed;
e. The existing POA&M or CAP must be updated weekly based on findings of weaknesses, including, but not limited to, the following:
    i. Reviews, tests, audits, or assessments;
    ii. Security impact analyses;
    iii. Independent verification and validation findings;
    iv. Continuous monitoring activities;
    v. Incidents;
f. All findings, recommendations, and their source must be tracked to the related item in the POA&M or CAP;
g. Findings must be analyzed as to their level of risk (i.e., Critical, High, Medium, Low) and a determination must be made for appropriate action(s) to be taken to correct or mitigate, as appropriate, the identified weaknesses to an acceptable level of risk;
h. One (1) or more tasks to remediate a finding must be documented in the POA&M or CAP for any of the following:
    i. Critical-level risks that are not remediated within seven (7) days;
    ii. High-level risks that are not corrected within twenty-one (30) days;
    iii. Medium-level risks that are not corrected within thirty (60) days;
    iv. Low-level risks, as required by the EBCI Tribal Option CIO/CISO, that are not corrected within ninety (90) days;
i. All findings must be entered into a CAP.

Risk Assessment/Analysis:

Risk assessment or analysis is the act of determining the probability that a risk will occur and the impact that an event would have if it does occur. This analyzes the cause and effect of each possible event. Once risks have been identified and documented, risk analysis must be performed. During the risk analysis process, each potential risk event will be evaluated for the following:

a. The probability that the risk will occur;
b. The impact of the risk if it occurs.

These two (2) factors of assessing the risk involving probability and impact shall be measured for probability using a scale of Low, Medium, and High and giving each an associated number.

For impact, CIHA shall use a qualitative method for analysis, as it is typically a quicker and usually more cost-effective way to analyze risks. Analysis will be performed with the goal of gathering data on the following:

a. The likelihood of the risk occurring;
b. The qualitative impact on CIHA, system, or data;
c. The quality of the risk data being utilized.

Business Risk Analysis of each business system shall be utilized to assist in impact determination.

Impact Definitions:

Magnitude of Impact	Impact Definition
High	If an event could be expected to have a severe or catastrophic adverse effect on CIHA operations, CIHA assets, or individuals and cause a loss of mission capability for a period that poses a threat to human life or results in a loss of major assets.
Moderate	If an event could be expected to have a serious adverse effect on CIHA operations, CIHA assets, or individuals and cause significant degradation in mission capability, place CIHA at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.
Low	If an event could be expected to have a limited adverse effect on CIHA operations [including mission essential functions (MEFs), functions, image, or reputation], CIHA assets, or individuals and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.

As risks are identified and quantified, they are stored in a security folder in CIHA's Microsoft Teams repository. All risks are reported based on type of risk, probability, impact, and overall risk. To determine and quantify the overall risk, the following table (based on NIST SP 800-30) is used:

Threat Likelihood	Low (10)	Medium (50)	High (100)
High (1.0)	**Low** 10 x 1.0 = 10	**Medium** 50 x 1.0 = 50	**High** 100 x 1.0 = 100
Medium (0.5)	**Low** 10 x 0.5 = 5	**Medium** 50 x 0.5 = 25	**High** 100 x 0.5 = 50
Low (0.1)	**Low** 10 x 0.1 = 1	**Medium** 50 x 0.1 = 5	**High** 100 x 0.1 = 10

Risk Response:

For each identified risk, a response must be identified. The CIHA CISO will select a risk response for each risk. The probability and impact of the risk will be the basis of recommending which actions should be taken to mitigate the risk. During response planning, strategies and plans are developed to minimize the effects of the risk to a point where the risk can be controlled and managed.

Avoid
Risk avoidance involves changing aspects of the overall business process or system architecture to eliminate the threat.

Transfer
Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat; it simply makes another party responsible for managing it. This would include identifying avenues of insurance, etc.

Mitigate
Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.

Accept
Risk acceptance should normally only be taken for Low-priority risks. All risks should have a recommendation of control(s) and/or alternative solutions to mitigate risk.

Use of Independent Third-Party Assessors:
When assessments must be conducted by an entity with an explicitly determined degree of independence to CIHA, independence must be determined by the CIHA CISO based on the security categorization of an information system and/or the risk to CIHA operations and assets and to individuals.

To make an informed, risk-based decision, the selection of independent third-party assessors must consider the following criteria to ensure credibility of the security risk and vulnerability assessment results and to receive the most objective information possible. Preserving the impartial and unbiased nature of the assessment process includes, but is not limited to, freedom from any perceived or actual conflicts of interest with respect to the following:

a. The development, operation, and/or management of an information system;
b. The chain of custody associated with an information system;
c. The determination of security control effectiveness;
d. A competitive relationship with any organization associated with an information system that is being assessed or that impacts on their reputations;
e. Undue influence because of a contractual or other related relationship;
f. The assessor's technical expertise and knowledge of state and federal requirements.

Vulnerability Monitoring and Scanning

[NIST RA-5]

CIHA Risk Management programs must include the following requirements:

a. All malware scanning software shall be current, actively running on deployed workstations and servers, and capable of generating audit logs of virus events;
b. Vulnerability scans in information systems and hosted applications must be performed at least every seven (7) days and when new vulnerabilities potentially affecting the system/applications are identified and reported;
c. Vulnerability scanning shall include scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms;
d. Real-time scanning for spyware, adware, and bots (software robots) with one (1) or more anti-spyware programs that detect these malicious programs and help inoculate the system against infection;
e. Scan for malware on files that are downloaded from the Internet or any other outside source, including all external media [e.g., flash drives, compact disks (CDs), etc.] shall be conducted;
f. Viruses, worms, spyware, Trojan horse applications, and other malicious code may cause damage to CIHA's infrastructure via web browsers, and therefore, all Internet traffic shall be scanned to prevent malicious code from infecting CIHA infrastructure;
g. External computers or networks making remote connection to internal CIHA computers or networks shall utilize a CIHA-approved active virus scanning and repair program and a CIHA-approved personal firewall system (hardware or software). CIHA shall ensure that updates to virus scanning software and firewall systems are available to users. Non-CIHA computers or networks making a remote connection to a public web server are exempted;
h. CIHA shall scan their networks to identify any multifunctional devices (MFDs) on the network that are vulnerable and/or configured insecurely and shall take remediation actions;
i. Prior to commencing vulnerability scanning efforts, the following should be addressed:
    i. Scanner selection – evaluate the mandated tools for use within the respective environments;
    ii. The network and host-based vulnerability scanner shall provide the following capabilities:
        - Identify active hosts on networks;
        - Identify active and vulnerable services (ports) on hosts;
        - Identify vulnerabilities associated with discovered operating systems and applications.

The CIHA CIO shall implement a suite of automated monitoring tools to effectively monitor and identify vulnerabilities on networked computer servers and workstations. Vulnerability scanning tools and techniques are employed to promote interoperability among tools and automate parts of the vulnerability management process by using standards for the following:

a. Enumerating platforms, software flaws, and improper configurations;
b. Formatting and making transparent, checklists and test procedures;

c. Measuring vulnerability impact;
d. Analyzing vulnerability scan reports and results from security risk assessments;
e. Remediating legitimate vulnerabilities within CIHA-defined response times, in accordance with a CIHA security risk and vulnerability assessments.

Sharing information obtained from the vulnerability scanning process and security risk assessments with designated personnel throughout CIHA helps eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Vulnerability Management:
System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application services and ports are enabled and opened in the system's firewall, as applicable. Vulnerabilities that threaten the security of CIHA's network or IT assets shall be addressed through updates and patches based upon assigned vulnerability ratings:

a. Personnel shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches and updates, and eliminating or disabling unnecessary services;
b. CIHA shall use, where possible, tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities;
c. Perform scans, typically, on systems and networks known to be stable and preferably during times of least impact to the critical functionality of the system. Expect vulnerability scanning to occur during various phases of the system's life cycle.

Vulnerability Risk Rating:
Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure using a scale of 0 to 10.0 as per the CVSS v3 "Qualitative Severity Rating Scale" for proper prioritization. If the additional combined information previously stated is not available, then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected, may be used. For general vulnerabilities that do not easily relate back to a CVE, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above "info," or a score of 0, may be used after appropriate review.

The risk ratings are assigned to a vulnerability. They are as follows:

a. **Critical-level Risk**
(Priority/CVSS 9.0-10.0)**:** A vulnerability that could cause grave consequences and potentially lead to leakage of sensitive data, if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, as identified by the data owner and could cause

functionality to cease, exfiltration of data, or an intruder to gain access to the network or IT asset;

b. **High-level Risk**
(Priority/CVSS 7.0-8.9)**:** A vulnerability that could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe. This vulnerability could cause functionality to cease or control of the network or IT asset to be gained by an intruder;

c. **Medium-level Risk**
(Priority/CVSS 4.0-6.9)**:** A vulnerability that should be addressed within the established timeframe. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner;

d. **Low-level Risk**
(Priority/CVSS 0.1-3.9)**:** A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited, and/or it is of little consequence to the data owner. Vulnerabilities of this nature are common among most networks and IT assets and usually involve a simple patch to remedy the problem. These patches can also be defined as enhancements to the network or IT asset.

Vulnerability Mitigation and Remediation:

a. Mitigation and remediation timeframes for identified or assessed vulnerabilities shall be based on the assigned Vulnerability Risk Rating:
   i. **Critical-level risk** vulnerabilities must be mitigated as soon as possible. "Critical-level risk" vulnerabilities must be, at a minimum, mitigated and remediated within seven (7) days;
   ii. **High-level risk** vulnerabilities must be mitigated or remediated within thirty (30) days;
   iii. **Medium-level risk** vulnerabilities must be mitigated or remediated within sixty (60) days;
   iv. **Low-level risk** vulnerabilities must be mitigated or remediated within ninety (90) days;

b. CIHA vulnerability mitigation and remediation procedures must specify, at a minimum, the proposed resolution to address identified vulnerabilities, required tasks necessary to affect changes, and the assignment of the required tasks to appropriate workforce;

c. Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified, but a patch is not currently available (zero-day vulnerability, which is a situation where an exploit is used before the developer of the software knows about the vulnerability). When a vulnerability risk is "critical" or "high-level" and no patch is available, steps must be taken to mitigate the risk through other compensating control methods (e.g., group policy objects, firewalls, router access control lists). A patch needs to be applied when it becomes available.

d. When a “critical” or “high-level” risk vulnerability cannot be totally mitigated within the requisite time frame, the CIHA CISO needs to be notified of the condition;
e. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed;
f. Appropriate notification shall be provided after vulnerability mitigation and remediation plans have been executed;
g. In the event of a zero-day vulnerability, CIHA shall mitigate the vulnerability immediately, if possible, and apply patches as soon as possible after the vendor provides them.

Vulnerability Information Review and Analysis:

a. Relevant vulnerability information from appropriate vendors, third-party research, and public domain resources shall be reviewed on a regular basis, per CIHA’s policies and procedures;
b. Relevant vulnerability information, as discovered, shall be distributed to the appropriate CIHA workforce;
c. Appropriate CIHA workforce shall be alerted or notified in near real-time about warnings or announcements involving "High-risk" vulnerabilities.

Requirements for Compliance:

a. CIHA must develop procedures to ensure the timely and consistent use of security patches and use a consistent vulnerability naming scheme to mitigate the impact of vulnerabilities in systems;
b. CIHA shall have an explicit and documented patch management and vulnerability management policy, as well as a systematic, accountable, and documented set of processes and procedures for handling patches and system vulnerabilities;
c. The patching and vulnerability management policy shall specify techniques CIHA will use to monitor for new patches and vulnerabilities and workforce who will be responsible for such monitoring;
d. CIHA’s patching process shall define a method for deciding which systems are patched and which patches are installed first, as well as the method for testing and safely installing patches;
e. A CIHA process for handling patches shall include the following:
    i. Using organizational inventories;
    ii. Using the Common Vulnerabilities and Exposures vulnerability naming scheme for vulnerability and patch monitoring (Refer to the CVE website at https://www.cve.org/ProgramOrganization/CNAs);
    iii. Patch prioritization techniques;
    iv. Organizational patch databases;
    v. Patch testing, patch distribution, patch application verification, patch training, automated patch deployment, and automatic updating of applications;

f. CIHA shall develop and maintain a list of sources of information about security problems and software updates for the system and application software and monitor these sources regularly;
g. CIHA shall establish a procedure for monitoring those information sources;
h. CIHA shall evaluate updates for applicability to the systems;
i. CIHA shall plan the installation of applicable updates;
j. CIHA shall install updates using a documented plan;
k. CIHA shall deploy new computers with up-to-date software;
l. After making any changes in a system's configuration or its information content, CIHA shall create new cryptographic checksums (a hash function used to test data to verify that the data has not been maliciously changed) or other integrity-checking baseline information for the system.

CIHA shall employ vulnerability monitoring and scanning tools that include the capability to update the information system vulnerabilities to be scanned. The vulnerabilities to be scanned need to be updated as new vulnerabilities are discovered and announced and scanning methods are developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

Vulnerability Monitoring and Scanning – Update Vulnerabilities To Be Scanned
[NIST RA-5(2)]
CIHA updates the information system vulnerabilities scanned prior to a new scan or when new vulnerabilities are identified and reported.

Vulnerability Monitoring and Scanning – Privileged Access
[NIST RA-5(5)]
CIHA shall implement privileged access authorization to an information system for vulnerability scanning activities. In certain situations, the nature of the vulnerability scanning may be more intrusive, or the information system component that is the subject of the scanning may contain Highly Restricted information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

CIHA CYBERSECURITY RISK ASSESSMENT POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 7/20/2023

Revision Information:

Date	Section Updated	Change
7/20/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
7/20/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA" and added "Cybersecurity" after "CIHA"
7/20/2023	Information Box	Added "Last Reviewed" date and added "Policy Owner" and identified the role
7/20/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
7/20/2023	Purpose	Added "North Carolina State departments, including NCDIT, NCDHHS, and NC Medicaid" as the entities that we must meet compliance requirements with and deleted "NCDHHS/EBCI Tribal Option Contract"
7/20/2023	Purpose	Changed "EBCI Tribal Option" to "State departments" in the following: In support of the purpose, this Policy has been developed to ensure CIA, privacy, and security of the information assets of CIHA, exceeding "State departments'" compliance requirements
7/20/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"
7/20/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
7/20/2023	Policy	Added that a Risk Assessment Policy must be implemented and maintained in compliance with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"
7/20/2023	Policy	Deleted "and procedures" as having to be reviewed annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary
7/20/2023	Policy	Deleted: "In addition, if modifications are required to meet a change in the DHHS Contract, a mutually agreed upon date shall be determined for a policy update" because this Policy now resides with CIHA, not EBCI Tribal Option
7/20/2023	Policy	Added "implementation and maintenance" of a risk assessment policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Risk Assessment Policy*
7/20/2023	Definitions	Amended definitions by supplementing additional language for "CEO," "CIO," "CISO," and "NIST" and deleted the definition for "EBCI" and "EBCI Tribal Option Contract" and added definitions for "CIHA Workforce" and "Procedural Guidelines"
7/20/2023	Procedural Guidelines	Changed the heading title from "PROCEDURES" to "PROCEDURAL GUIDELINES"
7/20/2023	Procedural Guidelines	Updated NIST RA-1: Added the "Internal Controls" section on NIST RA-1 and included the information that CIHA develops, documents, disseminates, implements, and maintains this Policy to all covered personnel involved in the acquisition, development, operation, and maintenance of information systems and supporting infrastructure
7/20/2023	Procedural Guidelines	Added that "CIHA Risk Assessment procedures must include the necessary controls" to facilitate the implementation of this Policy
7/20/2023	Procedural Guidelines	Added that policies and procedures are a critical component of CIHA's system of internal controls, which provides understanding to personnel about their roles, responsibilities, acceptable uses, and important information that relates to maintenance. Added that these policies and procedures are to be reviewed and updated annually
7/20/2023	Procedural Guidelines	Deleted the "Continuous Monitoring Plan NIST RA-1" and moved it to the *CIHA Cybersecurity Assessment, Authorization, and Monitoring Policy*
7/20/2023	Procedural Guidelines	Added "NC" to all instance of "DHHS" and changed "State" to "NCDHHS"
7/20/2023	Procedural Guidelines	Amended the following heading titles to reflect those in the *NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*: NIST RA-5, 5(2), and 5(5); and deleted NIST RA-5(1) [and incorporated it into RA-5]
7/20/2023	Procedural Guidelines	Added "(and subsequent revisions)" so as to include future revisions of NIST SP 800-60 and to "ISO 27001"
7/20/2023	Procedural Guidelines	Deleted "DHHS" as an external entity that must be considered during the security categorization process when considering the impact of events that could jeopardize the CIA of CIHA's information and information systems
7/20/2023	Procedural Guidelines	Changed all instances of "security/risk assessment" to "security risk and vulnerability assessments" and all instances of "third-party assessment of all critical systems" to "third-party independent security risk and vulnerability assessments" and changed "independent assessor" to "independent third-party assessor"
7/20/2023	Procedural Guidelines	Changed "supporting security liaison" to "CIHA IT staff"

7/20/2023	Procedural Guidelines	Deleted "DHHS" data as data that must be stored, labeled, classified, and destroyed when CIHA uses the NCDIT's Data Classification and Handling Policy for detailed requirements
7/20/2023	Procedural Guidelines	Changed "NC State Security Liaison" to "CIHA Security Steering Committee" as the party who receives all assessment results within 30 days of completion
7/20/2023	Procedural Guidelines	Changed that CIHA must ensure vendor compliance with "CIHA" (instead of "statewide") security policies and the "NCDIT" and deleted that CIHA must obtain a VRAR from the vendor prior to contract approval
7/20/2023	Procedural Guidelines	Changed "DHHS" assessment template to "NCDIT's security risk assessment template" and added instructions on how to access the template
7/20/2023	Procedural Guidelines	Included "mission essential functions (MEFs)" as an operation that is considered to have a low magnitude of impact if it were to be adversely affected
7/20/2023	Procedural Guidelines	Changed the "EBCI Tribal Option's GRC reporting and tracking tool" to "a security folder in CIHA's Microsoft Teams repository" as a place where risks that have been identified and quantified are stored
7/20/2023	Procedural Guidelines	Changed the "chain of command" to the "chain of custody" that is associated with an information system
7/20/2023	Procedural Guidelines	Changed CIHA "Risk Assessment" programs to "Risk Management" programs when referring to vulnerability monitoring and scanning
7/20/2023	Procedural Guidelines	Added "worms" as an application that may cause damage to CIHA's infrastructure via web browsers
7/20/2023	Procedural Guidelines	Deleted "Conduct scanning independently or as a coordinated effort with the NC State Security Liaison" as a required item from CIHA's Risk Management programs
7/20/2023	Procedural Guidelines	Changed CIHA "CISO" to "CIO" as the role who is responsible for implementing a suite of automated monitoring tools to effectively monitor and identify vulnerabilities on networked computer servers and workstations
7/20/2023	Procedural Guidelines	Changed "security control assessments" to "security risk assessments" when referring to these types of reports and results
7/20/2023	Procedural Guidelines	Changed "Restricted or Highly Restricted data" to "sensitive data" in the "Critical-level" vulnerability risk rating section; and added "as identified by the data owner" who identifies the type of vulnerability that is present within the most sensitive portions of the network or IT asset
7/20/2023	Procedural Guidelines	Added "and Remediation" to the "Vulnerability Mitigation" title heading of this section and to all instances of vulnerability mitigation within the section; deleted remediation "(if possible) within 21 days," changing it instead to 7 days
7/20/2023	Procedural Guidelines	Added "or critical" when identifying a vulnerability risk as "high-level"
7/20/2023	Procedural Guidelines	Amended the role of the "NC State Security Liaison to the "CIHA CISO" as the role who needs to be notified of the condition when a "critical" or "high-level" risk vulnerability cannot be totally mitigated within the requisite time frame
7/20/2023	Procedural Guidelines	Added "and monitor these sources regularly" as a requirement for compliance when CIHA shall develop and maintain a list of sources of information about security problems and software updates for the system and application software
7/20/2023	Procedural Guidelines	Added "vulnerability monitoring tools" as a tool that CIHA must employ, which has the capability to update the information system vulnerabilities to be scanned
7/20/2023	Policy Implementation/ Revision Information	Added policy revision information table
9/20/2024	Policy	Added "cybersecurity" before "maintenance" to provide further clarification for readers
9/20/2024	Policy and Procedural Guidelines	Moved NIST RA-1 language from the Procedural Guidelines section and combined it with the NIST RA-1 language in the Policy section
12/16/2025	Policy Header	Updated the CIHA seal
12/16/2025	Definitions	Amended "CIHA Workforce" definition
12/16/2025	Procedural Guidelines	NIST RA-3: Added "Critical" as a level of risk
12/16/2025	Procedural Guidelines	NIST RA-3: Changed the number of days from 21 to 30 in the following: One or more tasks to remediate a finding must be documented in the POA&M or CAP for high-level risks that are not covered within 30 days
12/16/2025	Procedural Guidelines	NIST RA-3: Changed the number of days from 30 to 60 in the following: One or more tasks to remediate a finding must be documented in the POA&M or CAP for medium-level risks that are not corrected within 60 days