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 Incident Response Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 4/18/2023

LAST REVIEWED: 2/20/2025

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Cybersecurity Incident Response 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 Incident Response 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 Incident Response Policy in compliance with National Institute of Standards and Technology (NIST) and State departments.

Incident Response Policy and Procedural Guidelines

[NIST IR-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 incident response 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 incident response process and the family of incident response security controls. The incident response 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 Incident Response principles established in NIST, "Incident Response" control guidelines, as the official standards for this security domain. The "IR" designator identified in each control represents the NIST-specified identifier for the Incident Response 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 Incident Response procedures include the necessary controls to facilitate the implementation of this Policy.

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

- Development, documentation, dissemination, implementation, and maintenance of an incident response policy and procedural guidelines;
- Incident Response Plan Training;
- Incident Response Plan Testing;
- Incident Handling;
- Incident Monitoring;
- Incident Reporting;
- Incident Response Assistance;
- Incident Response Plan.

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 Compliance Officer
The Cherokee Indian Hospital Authority Compliance Officer is charged with the overall responsibility of overseeing compliance with the *CIHA Compliance Plan* and other applicable standards.

CIHA Workforce
CIHA workforce includes all full-time or part-time CIHA staff/personnel/agents/employees (i.e., contractors, volunteers, interns, trainees, students, contract employees/workers, other third parties, guests), non-employees, and other persons/individuals whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

External (Third-Party) Service Providers
External (third-party) service providers, which include vendors, suppliers, service bureaus, contractors, interns, and other organizations, provide information system development, information technology services, outsourced applications, and network and security management.

National Institute of Standards and Technology (NIST)
NIST is one of the nation's oldest physical science laboratories. NIST provides technology, measurement, and standards for the smallest to the largest technologies. CIHA has adopted the Cyber Security Framework (CSF) provided by NIST, which provides guidance on how to prevent, detect, and respond to cyberattacks.

Procedural Guidelines
Guidelines for developing operational procedures.

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

Incident Response Training
[NIST IR-2]
All CIHA workforce and service providers with access to the CIHA network must be trained in their incident response roles. Incident response training must be provided to information system users that is consistent with assigned roles and responsibilities.

CIHA will:

a. Provide incident response training prior to:
   - Assuming an incident response role or responsibility; or
   - Acquiring access;
b. Provide incident response training and any additional or supplemental training when required by information system changes and annually thereafter;

c. Include user incident response training, regarding the identification and reporting of suspicious activities, both from external and internal sources;
d. Review and update incident response content on a regular basis and/or following CIHA-defined events, including, but not limited to, assessment or audit findings or changes to guidelines;
e. Maintain a comprehensive record of all incident response-related training. The electronic log shall include names of participants, information system name(s), type of training, and date of completion. Log entries shall be maintained by the CIHA CISO or his/her designee.

Incident Response Testing
[NIST IR-3]
All CIHA incident response personnel and service providers must perform the following testing:
a. Identify mission essential functions (MEFs) and critical business functions and associated incident response requirements;
b. Perform tabletop exercises using scenarios that include a breach of Restricted or Highly Restricted data and test CIHA's *Cybersecurity Incident Response Policy* and procedures;
c. A subset of all employees and contractors with access to Restricted or Highly Restricted data must be included in tabletop exercises;
d. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies;
e. The incident response capability will be tested at least annually.

Incident Handling
[NIST IR-4]
CIHA shall protect technology resources by conducting proper investigations:
a. The CIHA CISO shall evaluate the proper response to all information technology security incidents reported;
b. The CIHA CISO shall work with other CIHA leadership to decide what resources, including law enforcement, are required to best respond to and mitigate the incident;
c. After the initial reporting and/or notification, CIHA management shall review and reassess the level of impact that the incident created;
d. CIHA shall coordinate incident handling activities with contingency planning activities;
e. CIHA shall ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization. This will help ensure consistency in the incident handling procedure put in place in terms of steps/logistics, communications, coordination, and planning functions needed to resolve an incident in a structured and efficient manner. This is best achieved by following NIST guidelines and all subsequent revisions, such as the following:
    i. NIST SP 800-61 Computer Security Incident Handling Guide, Revision 2 (Section 3, Handling an Incident);
    ii. NIST SP 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, Revision 1;
    iii. NIST SP 800-92 Guide to Information Security Log Management;

f. An investigation into an information technology security incident must identify its cause, if possible, and appraise its impact on systems and data. The extent of damage must be determined and course of action planned and communicated to the appropriate parties;
g. CIHA shall investigate information system failures to determine whether the failure was caused by malicious activity or by some other means (i.e., hardware or software failure);
h. If any suspicious activities are detected, the CIHA CIO shall be notified immediately to ensure that proper action is taken;
i. CIHA shall establish controls to protect data CIA during investigations of information technology security incidents. Controls shall either include dual-control procedures or segregation of duties to ensure fraudulent activities requiring collusion do not occur;
j. Evidence of or relating to an information technology security breach shall be collected and preserved in a manner that is in accordance with state and federal requirements;
k. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions that may ensue as a result of the incident;
l. Any system, network, technical, or security administrator who observes an intruder on the CIHA network or system shall take appropriate action to terminate the intruder's access. (Intruder can mean a hacker, botnet, malware, etc.);
m. In the event of an active incident, CIHA management has the authority to decide whether to continue collecting evidence or to restrict physical and logical access to the system involved in the incident. **Note:** It may be necessary to isolate from the network until the extent of the damage can be assessed;
n. When dealing with a suspected incident, the following shall be done:
    i. Make an image of the system (including volatile memory, if possible) so that original evidence may be preserved;
    ii. Make copies of all audit trail information, such as system logs, network connections [including Internet Protocol (IP) addresses, Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports, length, and number], super user history files, etc.;
    iii. Take steps to preserve and secure the trail of evidence;
o. CIHA's CIO or his/her designee will determine if other agencies, departments, or workforce need to become involved in resolution of the incident;
p. All workforce directly involved with incident handling shall have signed a confidentiality agreement;
q. Incident details shall be discussed only on a need-to-know basis with authorized workforce;
r. When responding to a malware threat, the following tasks shall be performed:
    i. Verify threats to rule out the possibility of a hoax before notifying others;
    ii. Identify workforce responsible for mitigation of malware threats;
    iii. Have internal escalation procedures and severity levels;
    iv. Have processes to identify, contain, eradicate, and recover from malware events;
    v. Have a contact list of endpoint protection vendors;

s. The following and all subsequent revisions may be utilized for guidance regarding incident handling:
   i. NIST SP 800-61, Computer Security Incident Handling Guide, Revision 2;
   ii. NIST SP 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, Revision 1;
   iii. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response;
   iv. NIST SP 800-92, Guide to Computer Security Log Management;
   v. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS);
   vi. NIST SP 800-101, Guidelines on Mobile Device Forensics, Revision 1; and
   vii. Other appropriate guidance, as necessary;

t. CIHA shall activate and implement a security incident handling capability that is consistent with the Incident Response Plan during all stages of the NIST incident response life cycle (See Figure 1: NIST IR-4), including the following:
   i. Preparation;
   ii. Detection and Analysis;
   iii. Containment, Eradication, and Recovery;
   iv. Post-Incident Activities;

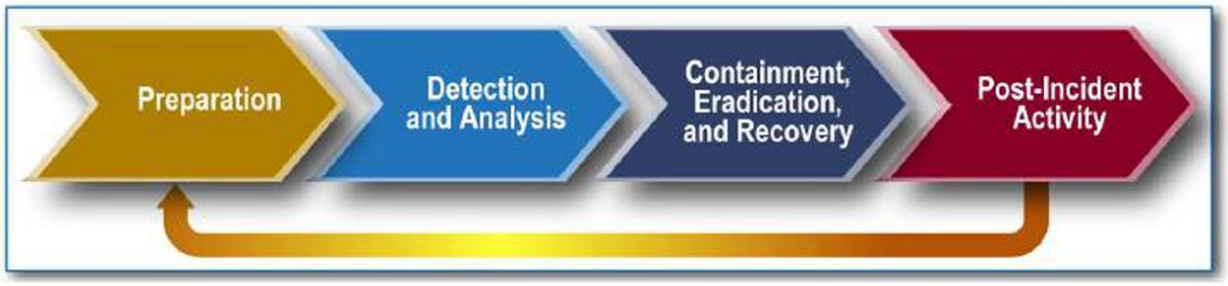

Figure 1

u. The integrity of information systems incident investigations shall be ensured by having the records of such investigations audited by qualified members of the workforce as determined by the CIHA CIO;

v. Records of information security breaches and the remedies used for resolution shall be maintained as references for evaluating any future security breaches. The information shall be logged and maintained in such a location that it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned;

w. The CIHA CISO and/or incident response coordinator shall determine the criticality of an incident (refer to NIST IR-6 for incident severity levels);

x. Lessons learned from incident handling activities shall be incorporated into incident response procedures, training, and testing/exercises; resulting changes shall be implemented within thirty (30) days;

y. CIHA shall create processes to provide information for the enhancement of information security awareness programs and incident response programs.

Incident Monitoring

[NIST IR-5]

Maintaining records about each information system incident, the status of the incident, and other pertinent information is necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including, for example, incident reports, incident response team (IRT), audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

a. Information system security incidents that potentially affect the confidentiality of all other Restricted and Highly Restricted data shall be tracked and documented;
b. If the incident is rated a severity 3 or higher (refer to NIST IR-6 for incident severity levels), subsequent reports to the CIHA CEO shall be provided;
c. The release of confidential security information during a security incident or investigation shall be monitored and controlled to ensure that only appropriate individuals have access to the information, such as law enforcement officials, legal counsel, or human resources;
d. A follow-up report shall be submitted to the CIHA CISO upon resolution by those directly involved within one (1) business day in addressing the incident and contain the following:
    i. Point of contact (PoC);
    ii. Affected systems and locations;
    iii. System description, including hardware, operating system, and application software;
    iv. Type of information processed;
    v. Incident description;
    vi. Incident resolution status;
    vii. Damage assessment, including any data loss or corruption;
    viii. Organizations contacted;
    ix. Corrective actions taken;
    x. Lessons learned.

Incident Reporting

[NIST IR-6]

Security incidents, for example, suspicious events (e.g., insider threat), software errors or weaknesses, system vulnerabilities associated with security incidents (e.g., ransomware), and lost or stolen CIHA computer equipment, shall be reported immediately to the CIHA Compliance Officer, CIO, and CISO:

a. CIHA and its IT vendors shall ensure all suspected security incidents or security breaches are reported to the CIHA CISO and CIO within twenty-four (24) hours of incident confirmation;
b. Contracts involving the storage and/or processing of CIHA data shall identify the vendor's security PoC;
c. For reporting security incidents to outside authorities, CIHA shall do the following:
    i. CIHA shall coordinate with the CIHA CISO and Compliance Officer in accordance with CIHA's Incident Response Plan. All security incidents shall be reported to the CIHA CISO when reported to an outside entity;

ii. The CIHA Compliance Officer shall notify external entities, such as the Social Security Administration (SSA) Regional Office and their SSA Systems Security Contact, and applicable State departments, etc. within one (1) hour of suspecting loss if a privacy or security incident involves the unauthorized disclosure of data;
iii. The CIHA Compliance Officer shall notify consumers in the event of a security breach resulting in the unauthorized release of unencrypted or unredacted records or data containing personal information with corresponding names. **Note:** The acquisition of encrypted data is only a breach if a confidential process or the key needed to unlock the data is breached or if the data is encrypted by an unauthorized or malicious process, such as ransomware;
iv. The CIHA CIO and/or his/her designee shall manage the dissemination of incident information to other participants, for example law enforcement or the press. Public release of information concerning a security incident shall be coordinated through the CIHA CIO, the IRT, and the CIHA Public Relations Director;

d. Information recorded about information technology security breaches shall cover the following at a minimum:
i. Identify the current level of impact on CIHA MEFs and critical business functions;
ii. Identify the type of information lost, compromised, or corrupted;
iii. Estimate the scope of time and resources needed to recover from the incident;
iv. Identify when the activity was first detected and when corrective actions were implemented;
v. Identify the number of systems, records, and users impacted;
vi. Identify the network location of the observed activity;
vii. Identify PoC information for additional follow-up;
viii. Identify the attack vector(s) that led to the incident;
ix. The method of breach detection and incident response actions;
x. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident;
xi. Provide any mitigation activities undertaken in response to the incident.

Incident Severity Levels:

The CIHA CISO is responsible for initially assessing an incident's impact and assigning a severity to the incident. This initial severity assignment dictates the level of response to the incident. As response to the incident progresses, it may be determined that the incident is more (or less) severe than originally realized, and a new severity level assigned. Security incidents are divided into five (5) levels of severity based on their potential to negatively impact CIHA operations, finances, and/or reputation. The characteristics in the following table should be used as baseline severity levels and may include additional threats categories.

Incident Severity	Incident Characteristics

5
General Attack(s)
SEVERE
	• Potential for or actual loss of lives or significant impact on the health or economic security of CIHA;
	• Significant risk of negative financial or public relations impact;
	• Loss of critical supervisory control and data acquisition (SCADA) systems;
	• Successful penetration or denial-of-service attack(s) detected with significant impact on CIHA network operations:
	  ○ Very successful, difficult to control or counteract;
	  ○ Large number of systems compromised;
	  ○ Significant loss of confidential data;
	  ○ Complete network failures;
	  ○ Mission-critical system or application failures;
	  ○ Compromise or loss of administrative controls of critical system.

4
Limited Attack(s)
HIGH
	• Low risk of negative financial or public relations impact;
	• Widespread instances of a computer virus or worm that cannot be handled by deployed endpoint protection (i.e., antivirus software);
	• A critical vulnerability is discovered, but no exploits are reported;
	• A critical vulnerability is being exploited, but there has been no significant impact;
	• Penetration or denial-of-service attack(s) detected with limited impact on CIHA network operations:
	  ○ There are credible warnings of increased probes or scans;
	  ○ Minimally successful, easy to control, or counteract;
	  ○ Small number of systems compromised;
	  ○ Little or no loss of confidential data;
	  ○ No loss of mission-critical systems or applications;
	  ○ A compromise of non-critical system(s) did not result in loss of data.

Incident Severity	Incident Characteristics
3 **Specific Risk of Attack** **ELEVATED**	• An exploit for a critical vulnerability exists that has the potential for significant damage; • A critical vulnerability is being exploited, and there has been a moderate impact; • There is a compromise of a secure or critical system(s) containing sensitive information; • There is a compromise of a critical system(s) containing non-sensitive information, if appropriate; • Widespread instances of a known computer virus or worm, easily handled by deployed endpoint protection (i.e., antivirus software); • Isolated instances of a new computer virus or worm that cannot be handled by deployed endpoint protection (i.e., antivirus software); • There is a distributed denial-of-service attack; • Significant level of network probes, scans, and similar activities detected, indicating a pattern of concentrated reconnaissance.
2 **Increased Risk of Attack** **GUARDED**	• A critical vulnerability is discovered, but no exploits are reported; • A critical vulnerability is being exploited, but there has been no significant impact; • A new virus is discovered with the potential to spread quickly; • There are credible warnings of increased probes or scans; • A compromise of non-critical system(s) did not result in loss of data; • Small numbers of system probes, scans, and similar activities detected on internal systems; • External penetration or denial-of-service attack(s) attempted with no impact to CIHA network operations; • Intelligence received concerning threats to which CIHA systems may be vulnerable.
1 **LOW**	• Small numbers of system probes, scans, and similar activities detected on internal and external systems; • Isolated instances of known computer viruses or worms, easily handled by deployed endpoint protection (i.e., antivirus software); • Unsubstantiated or inconsequential event.

Incident Reporting - Automated Reporting:
[NIST IR-6 (1)]
Automated processes shall be enacted for the purpose of reporting incidents [e.g., Security Information and Event Management (SIEM) technology].

Incident Reporting - Supply Chain Coordination:
[NIST IR-6 (3)]
A process shall be ensured to provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident. Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes, or personnel.

Incident Response Assistance
[NIST IR-7]
The CIHA CIO shall provide incident response support that offers advice and assistance to users of CIHA information systems for the handling and reporting of security incidents. These resources may include digital forensic services, vulnerability assessments, and incident response capability.

Incident Response - Automation Support for Availability of Information and Support:
[NIST IR-7 (1)]
The availability of incident response information and support shall be increased with the use of automated mechanisms. Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. Examples of automated mechanisms to provide incident response information and support include the following:

- Ticketing system for IT service desk;
- Distribution lists;
- Automated answering.

Incident Response Plan
[NIST IR-8]
CIHA's MEFs and critical business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. The Incident Response Plan must include the following requirements:

a. Provides CIHA with a roadmap for implementing its incident response capability;
b. Describes the structure and organization of the incident response capability;
c. Provides a high-level approach for how the incident response capability fits into CIHA;
d. Meets the unique requirements of CIHA, which relate to mission, size, structure, and functions;
e. Defines reportable incidents;
f. Provides steps to be taken within the security Incident Response Plan during and after cyberattacks;

g. Provides metrics for measuring the incident response capability within CIHA by incident response management function:
    i. Common organizational interfaces (e.g., communications, work coordination);
    ii. Protect (e.g., risk assessment, malware protection, vulnerability management);
    iii. Detect (e.g., continuous network security monitoring and alerting);
    iv. Respond (e.g., incident reporting, incident response, incident analysis);
    v. Sustain [e.g., Memorandums of Understanding (MOUs) and contracts, program management, security administration];
h. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
i. Addresses the sharing of incident information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving Restricted or Highly Restricted data (i.e., breaches), include a process to determine whether notice to oversight organizations or affected personnel is appropriate and provide that notice accordingly;
j. Be reviewed and approved by the CIHA CISO and CIO annually, at a minimum;
k. Explicitly designate the responsibility for incident response to a CIHA-defined role/personnel;
l. Be revised as needed to address system/agency changes or problems encountered during plan implementation, execution, or testing;
m. Communicate Incident Response Plan changes to the CIHA Security Steering Committee;
n. Distribute the Incident Response Plan to CIHA-identified incident response workforce;
o. Protect the Incident Response Plan from unauthorized disclosure and modification.

CIHA CYBERSECURITY INCIDENT RESPONSE POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 4/18/2023

Revision Information:

Date	Section Updated	Change
4/18/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
4/18/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA"
4/18/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
4/18/2023	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"
4/18/2023	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
4/18/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"
4/18/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
4/18/2023	Policy	Added that an Incident Response Policy must be implemented and maintained in compliance with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"

4/18/2023	Policy	Amended the title of the "*EBCI Tribal Option Incident Response Policy*" by deleting "EBCI Tribal Option" and replacing it with "CIHA"
4/18/2023	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
4/18/2023	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
4/18/2023	Policy	Added "implementation and maintenance" of an incident response policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Incident Response Policy*
4/18/2023	Definitions	Amended definitions by supplementing additional language for "CEO," "CIO," "CISO," "CIHA Compliance Officer," and "External (Third-Party) Service Providers," and "NIST" and deleted the definition for "EBCI" and "EBCI Tribal Option Contract" and added definitions for "CIHA Workforce" and "Procedural Guidelines"
4/18/2023	Procedural Guidelines	Changed the heading title from "PROCEDURES" to "PROCEDURAL GUIDELINES"
4/18/2023	Procedural Guidelines	Updated NIST IR-1: Added the "Internal Controls" section on NIST IR-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
4/18/2023	Procedural Guidelines	Added that "CIHA Incident Response procedures must include the necessary controls" to facilitate the implementation of this Policy
4/18/2023	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
4/18/2023	Procedural Guidelines	Added "NC" to all instance of "DHHS" and changed "State" to "NCDHHS"
4/18/2023	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 IR-2, 3, 6(1), 6(3), and 7(1)
4/18/2023	Procedural Guidelines	Added the timeframe of "annually thereafter" as when to provide incident response training and any additional or supplemental training when required by information system changes
4/18/2023	Procedural Guidelines	Identified essential missions and business functions as "MEFs" and "critical business functions"
4/18/2023	Procedural Guidelines	Added "and all subsequent revisions" to the NIST guidelines that were listed in item e. and s. of NIST IR-4 Incident Handling
4/18/2023	Procedural Guidelines	Replaced "NCDHHS" with "state" when referring to the "state and federal requirements" for evidence of or relating to an

		information technology security breach that is collected and preserved in the manner of
4/18/2023	Procedural Guidelines	Added the timeframe of "30 days" for when resulting changes are implemented for when lessons learned from incident handling activities are incorporated into incident response procedures, training, and testing/exercises
4/18/2023	Procedural Guidelines	Changed "CIHA CIO" to "CIHA CISO" as the role that a follow-up report must be submitted to upon resolution by those directly involved within one business day in addressing the incident
4/18/2023	Procedural Guidelines	Added "CIHA CIO" as one of the roles that "CIHA and its IT vendors must report to about all suspected security incidents or security breaches" within 24 hours of incident confirmation and deleted "NCDHHS" and "as required by NC general statute"
4/18/2023	Procedural Guidelines	Added "CIHA Compliance Officer" as one of the roles that "CIHA shall coordinate with in accordance with CIHA's Incident Response Plan" for reporting security incidents to outside authorities
4/18/2023	Procedural Guidelines	Replaced "NC Medicaid" and NCDHHS" with "applicable State departments" as an external entity that the CIHA Compliance Officer must notify for reporting security incidents to outside authorities
4/18/2023	Procedural Guidelines	Changed "EBCI Tribal Option functions or services (Functional Impact)" to "CIHA MEFs and critical business functions" when identifying the current level of impact IT security breaches has on them

4/18/2023	Procedural Guidelines	Replaced “IT help desk” with “IT service desk”
4/18/2023	Procedural Guidelines	Added “continuous” as the cadence in the example for network security monitoring and alerting
4/18/2023	Procedural Guidelines	Replaced “CIHA CIO, CEO, and NCDHHS” with the “CIHA Security Steering Committee” as the group that changes in the Incident Response Plan must be communicated to
4/18/2023	Policy Implementation/ Revision Information	Added policy revision information table
10/5/2023	Policy Title	Added “Cybersecurity” after “CIHA” in the title
10/5/2023	Information Box	Updated “Effective Date” and “Last Reviewed” date and added “Policy Owner” and identified the role
10/5/2023	Staff Governed By This Policy	Added “and/” to “CIHA vendors and/or subcontractors”
10/5/2023	Procedural Guidelines	Identified Figure 1: as “NIST IR-4”
2/20/2025	Policy	Added “cybersecurity” before “maintenance” to provide further clarification for readers
2/20/2025	Policy and Procedural Guidelines	Moved NIST IR-1 language from the Procedural Guidelines section and combined it with the NIST IR-1 language in the Policy section