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 System and Information Integrity Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 8/17/2023

LAST REVIEWED: 8/17/2023

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Cybersecurity System and Information Integrity 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 System and Information Integrity Policy* has been developed to ensure the confidentiality, integrity, availability (CIA), privacy, and security of the information assets of CIHA through the establishment of safeguards to prevent theft, abuse, and misuse while exceeding State departments' compliance requirements.

Failure to comply with this Policy may subject the CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce) to potential penalties and disciplinary action that may include termination of employment or contract.

STAFF GOVERNED BY THIS POLICY:

This Policy applies to all:

- CIHA workforce;
- CIHA vendors and/or subcontractors, who process, store, transmit, and have connectivity to the Information Technology (IT) infrastructure.

POLICY:

[NIST SI-1]

Note SI = Acronym used by NIST for System and Information Integrity

CIHA shall implement and maintain a Cybersecurity System and Information Integrity Policy in compliance with National Institute of Standards and Technology (NIST) and State departments. This Policy shall be reviewed annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary.

The *CIHA Cybersecurity System and Information Integrity Policy* shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a system and information integrity policy and procedural guidelines;
- Identification of information system flaws and remediation;
- Automated mechanisms to determine the state of information system components with regard to flaw remediation;
- Protections against malicious code at information system entry and exit points;
- Central management of protections against malicious code;
- Automatic updates to malicious code protection mechanisms;
- Monitoring of information systems;
- Automated tools for monitoring information systems inbound and outbound communications with system generated alerts;
- Security alerts, advisories, and directives from trusted sources on an ongoing basis;
- Verification of the correct operation of the system itself, the verification activities, and the notifications of failed security verification tests;

- Use of information integrity verification tools that perform integrity checks and automatically provides notification of integrity violations;
- Protection of CIHA resources from electronic mail (email) threats and updates for spam protection mechanisms;
- Checking validity of information inputs;
- Handling and generation of error messages;
- Management and handling of information within an information system and information output from the system;
- Implementation of security safeguards for memory protection.

DEFINITIONS:

Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) is the executive sponsor for CIHA who provides direction on major hospital policies, including, but not limited to, strategic, financial, risk management, infrastructure, regulatory, and governance issues. The CEO is responsible for delegation of tasks needed to ensure CIHA information security (IS) and cyber risks are managed through an appropriate governance committee. The CEO shall also ensure that both strategic and operational processes are empowered and supported. The CEO will monitor progress on all major initiatives.

Chief Information Officer (CIO)

The Chief Information Officer (CIO) is responsible for CIHA's overall information technology strategy and operations. The CIO delegates responsibility for information technology strategy and information technology operations activities, as appropriate. The CEO authorizes the CIO to pursue appropriate activities and actions, which help achieve the strategy and operations objectives consistent with this Policy.

Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is responsible for ensuring that CIHA information is protected. The CISO will delegate responsibility to steadfast individuals for approving and reviewing access rights to information. The CISO is responsible for ensuring that CIHA's security objectives are achieved. The CEO authorizes the CISO to pursue appropriate activities and actions that are consistent with this Policy, which contribute to achieving CIHA's security objectives.

CIHA Workforce

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

National Institute of Standards and Technology (NIST)
NIST is one of the nation's oldest physical science laboratories. NIST provides technology, measurement, and standards for the smallest to the largest technologies. CIHA have 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.

System and Information Integrity Policy and Procedural Guidelines
[NIST SI-1]

Internal Controls:
All CIHA information assets must meet the required security controls defined in this Policy that are based on NIST. This Policy addresses CIHA's requirements, which will be used to implement the system and information integrity process and the family of system and information integrity security controls. The system and information integrity 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 System and Information Integrity principles established in NIST, "System and Information Integrity" control guidelines, as the official standards for this security domain. The "SI" designator identified in each control represents the NIST-specified identifier for the System and Information Integrity 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 System and Information Integrity procedures include the necessary controls to facilitate the implementation of this Policy.

Policies and procedures are a critical component of CIHA's system of internal controls, which helps to ensure that all personnel have a clear understanding of roles, responsibilities, acceptable uses, and other important information that relates to the integrity of information systems in accordance with information security's best practices. As such, policies and procedures relating to the stated criteria herein are to be reviewed and updated on an annual basis to ensure that their overall adequacy and sufficiency meets CIHA's needs.

Flaw Remediation

[NIST SI-2]

CIHA shall have an explicit and documented patching and vulnerability policy, (refer to the *CIHA Cybersecurity Risk Assessment Policy*), as well as a systematic, accountable, and documented set of processes and procedures for flaw remediation. CIHA must do the following:

a. The patching and vulnerability policy shall specify techniques CIHA will use to identify, report, and correct information system flaws and personnel who will be responsible for the process:
    i. 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;
    ii. 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 those sources regularly;
    iii. Where technically configurable, CIHA shall use tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention (Refer to http://cve.mitre.org) that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities;
    iv. CIHA shall update and review vulnerability definitions and signatures prior to each scan or when new vulnerabilities are identified or reported;
    v. 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;
    vi. Relevant vulnerability information, as discovered, shall be distributed to the appropriate CIHA personnel;
    vii. System and application bug fixes or patches shall be accepted only from reliable sources, such as the software vendor;
    viii. Software patches addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources;
    ix. 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;
    x. 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 and remediation plan and execution of a plan;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates based on severity and associated risk. Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures;
d. Incorporate flaw remediation into CIHA's configuration management process:
    i. CIHA shall employ a centrally managed (per **Central Management [NIST PL-9]**) and automated mechanisms (per **Flaw Remediation – Automated Flaw Remediation Status [NIST SI-2(2)]**) to determine the state of information system components about flaw remediation.

Vulnerability Risk Ratings and Remediation:
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 and remediation timelines are assigned to a vulnerability. They are as follows:

- **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. Critical-level risk vulnerabilities must be, at a minimum, remediated within seven (7) days.

- **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.

- **Medium-level Risk**
  (Priority/CVSS 4.0-6.9)**:** A vulnerability that should be addressed within the established timelines. 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. 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.

- **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 information technology (IT) asset to be exploited, and/or it is of little consequence to the data owner.

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;

Malicious Code Protection

[NIST SI-3]

CIHA shall implement layers of information security (defense in depth) to defend against attacks on CIHA's information systems, including malicious code protection, such as endpoint protection (antivirus software) and anti-malware and Intrusion Detection Systems (IDSs). As applicable, malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles. CIHA shall do the following:

a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Update malicious code protection mechanisms whenever new releases are available in accordance with CIHA configuration management policy and procedures;
c. Configure malicious code protection mechanisms to do the following:
   i. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with this *CIHA Cybersecurity System and Information Integrity Policy*;

ii. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection;

iii. Allow users to manually perform scans on their workstation and removable media;

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system;
e. Centrally manage malicious code protection mechanisms (per **Central Management [NIST PL-9])** with automatic updates (per **Malicious Code Protection [NIST SI-3]**). Malicious code protection mechanisms include, for example, signature definitions. Updates shall be tested and approved according to the *CIHA Cybersecurity Configuration Management Policy*;
f. Ensure currently supported and patched software is installed to mitigate vulnerabilities and to reduce the risk of malicious activity;
g. Implement measures to filter unwanted traffic (spam, bots, etc.) attempting to enter the internal network;
h. CIHA shall ensure that updates to virus scanning software and firewall systems are available to users;
i. All files downloaded from a source external to the CIHA network, including all data received on a diskette, compact disc (CD), USB flash drive, email attachments, or any other electronic medium, shall come from a known, trusted source and shall be scanned for malicious software such as viruses, spyware, Trojan horses, worms, or other destructive code. This includes files obtained through any other file transfer mechanism;
j. CIHA shall ensure that web browser software is properly configured to protect CIHA's information technology systems. Configuration procedural guidelines for web browser software may be found in the *CIHA Cybersecurity Configuration Management Policy*.

System Monitoring
[NIST SI-4]

CIHA shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. This includes systems that are cloud hosted by contracted vendors or CIHA managed.

a. CIHA shall monitor information systems to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections;
b. CIHA shall identify unauthorized use of the information system:
    i. All hardware connected to the CIHA network or is cloud hosted shall be configured to support state and federal management and monitoring standards;
    ii. Monitoring for attempts to deny service or degrade the performance of information systems;
    iii. Conducting periodic reviews of system logs for signs of misuse, abuse, or attack;
c. CIHA shall deploy monitoring devices and controls to help secure CIHA's resources. These controls shall include the following:
    i. Securing interfaces between CIHA-controlled and non-CIHA-controlled or public networks;

ii. Standardizing authentication mechanisms in place for both users and equipment;

iii. Appropriate user access controls and separation of duties shall be employed to provide review and monitoring of system usage of personnel normally assigned to this task;

iv. Monitoring for anomalies or known signatures via IDSs and/or intrusion prevention system (IPSs). Intrusion Detection and Prevention Systems (IDPSs) signatures shall be up to date;

d. CIHA shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to CIHA operations and assets, individuals, or other organizations based on law enforcement information, intelligence information, or other credible sources of information;
e. Provide information system monitoring information to the designated CIHA officials as needed;
f. CIHA shall obtain legal opinion about information system monitoring activities in accordance with applicable federal laws, directives, policies, or regulations.

Control Enhancements

System Monitoring – Automated Tools and Mechanisms for Real-Time Analysis [NIST SI-4(2)]

CIHA shall employ automated tools to support near real-time analysis of events. Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by CIHA information systems.

a. **System Monitoring – Inbound and Outbound Communications Traffic [NIST SI-4(4)]:**
   i. CIHA shall monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within CIHA information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components;
   ii. CIHA shall enable logging features on firewalls, [network and web application firewalls (WAF)], to capture all packets dropped or denied by the firewall. CIHA shall review those logs at least monthly;
   iii. CIHA shall review and verify their firewall policies at least quarterly. If an outside entity manages the firewall, then that entity shall be responsible for

providing CIHA's firewall policy to the CIHA IT personnel for review and corrective actions, at minimum quarterly;

b. **System Monitoring – System-Generated Alerts [NIST SI-4(5)]:**
   i. CIHA information systems shall alert authorized personnel, such as system administrators, mission/business owners, system owners, or information system security analysts, when indications of compromise, potential compromise, or detected suspicious events occur. CIHA shall take necessary actions to address suspicious events once detected;
   ii. Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, WAF, or boundary protection devices, such as proxies, gateways, wireless access points, routers, firewalls, encrypted tunnels, and web content filters. Alerts can be transmitted, for example, by telephone, electronic mail messages, or text messages.

Security Alerts, Advisories, and Directives
[NIST SI-5]

CIHA shall do the following:

a. Receive information system security alerts, advisories, and directives from external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as considered necessary;
c. Disseminate security alerts, advisories, and directives to the designated CIHA management and technical personnel as appropriate;
d. Implement security directives in accordance with established timeframes of the degree of noncompliance;
e. Take appropriate actions in response to security alerts/advisories:
   i. Any updates or notices from State departments must be implemented per CIHA change control and/or incident response procedures;
   ii. State departments must be contacted with any security alert/advisory concerns or must be notified when the actions are completed.

CIHA employs automated mechanisms to make security alert and advisory information available throughout its organization (per **Security Alerts, Advisories, and Directives – Automated Alerts and Advisories [NIST SI-5(1)]**).

The CIHA CISO shall maintain contact with special interest groups (e.g., information security forums) that do the following:

i. Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies);
ii. Provide access to advice from security professionals;
iii. Improve knowledge of security best practices.

Security and Privacy Function Verification

[NIST SI-6]

CIHA ensures that the information systems verify the correct operation of the system itself, perform this verification as necessary, notify the CIHA CISO of failed security verification tests, and if necessary, shuts the information system down and restarts the information system when anomalies are discovered.

CIHA's information systems:

a. Verify the correct operation of the following security functions:
   i. User log-in activity, both failed and successful, including user IDs, log-in date/time, log-out date/time;
   ii. Unauthorized access attempts to network or system resources, including audit files;
   iii. Changes to critical application system files;
   iv. Changes to system security parameters;
   v. System start-ups and shutdowns;
   vi. Application start-ups, restart and/or shutdown;
   vii. Attempts to initialize, remove, enable, or disable accounts or services;
   viii. Changes to the auditing function, including enabling or disabling auditing and changing events to be audited;
   ix. User credential creation and deletion;
   x. Attempts to create, remove, or set passwords or change system privileges;
   xi. All uses of special system privileges;
   xii. System errors and corrective action(s) taken;
   xiii. Failed read-and-write operations on the system directory;
   xiv. All actions taken with administrative privileges;
b. Verifies Information systems operation on a regular basis.

Software, Firmware, and Information Integrity

[NIST SI-7]

CIHA shall employ integrity verification tools to detect unauthorized changes to CIHA software, firmware, and information.

a. Error logs generated by information technology systems shall be regularly monitored and reviewed for abnormalities and shall be:
   i. Cross-checked for known security events based on network, size, system type, and logical and physical location;
   ii. Enabled on each device or system on the network, such as servers, firewalls, routers, switches, cache engines, IDSs and applications, if performance requirements are not affected;

iii. Monitored on a weekly basis at a minimum;

iv. Checked against baselines to effectively verify variations from normal work-related activities.

Software, Firmware, and Information Integrity – Integrity Checks [NIST SI-7(1)]

a. CIHA information systems shall perform an integrity check of CIHA-defined software, firmware, and information at transitional states, such as, system start-ups, restart, shutdown, and abort, as well as when any security-relevant events occur. Security-relevant events include, for example, the identification of a new threat to which CIHA information systems are susceptible and the installation of new hardware, software, or firmware;
b. The integrity of backup or image files shall be validated using file hashes for backups, restores, and virtual machine migrations;
c. 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.

Software, Firmware, and Information Integrity – Automated Notifications of Integrity Violations [NIST SI-7(2)]

CIHA employs automated tools that provide notification upon discovering discrepancies during integrity verification.

Software, Firmware, and Information Integrity – Automated Response to Integrity Violations [NIST SI-7(5)]

The information system automatically implements security safeguards when integrity violations are discovered.

Software, Firmware, and Information Integrity – Integration of Detection and Response [NIST SI-7(7)]

CIHA incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.

Least Functionality – Binary or Machine Executable Code [NIST CM-7(8)]

CIHA:

a. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the CIHA CIO.

Spam Protection

[NIST SI-8]

CIHA shall do the following to protect CIHA resources from electronic mail (email) threats:

a. Employ spam protection mechanisms at information system entry and exit points to detect and act on unsolicited email messages (spam);
b. Update spam protection mechanisms when new releases are available in accordance with CIHA configuration management policy and procedures;
c. Protect CIHA resources by not acting on unsolicited commercial electronic mail. Recipients shall not open or respond to unsolicited email;
d. Educate users on the potential security risks involved in responding to spam, including responding to an invitation contained in such email to have one's email address removed from a sender's list;
e. Establish procedures that address the following issues:
    i. Attacks on email (e.g., viruses, interception, user identification, defensive systems);
    ii. Activating or clicking on hyperlinks in documents or email messages that are from unknown sources or part of unsolicited messages;
    iii. Responding to or following hyperlinks asking for user names and passwords when asked to do so by unsolicited phishing emails;
    iv. Protection of electronic mail attachments using such techniques as filtering, stripping, and store and forward;
    v. Use of cryptography to protect the confidentiality and integrity of electronic messages.

CIHA information systems shall automatically update spam protection mechanisms (per **Spam Protection – Automatic Updates [NIST SI-8(2)]**).

Information Input Validation

[NIST SI-10]

CIHA information systems shall check the validity of information inputs by doing the following:

a. Rule check the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) required to execute job functions;
b. Prescreen and validate inputs prior to passing to interpreters to prevent the content from being unintentionally interpreted as commands.

Error Handling

[NIST SI-11]

CIHA information systems shall do the following:

a. Generate error messages that provide information necessary for corrective actions without revealing information, including, for example, erroneous log-on attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account

numbers, social security numbers, and credit card numbers that could be exploited by adversaries;
b. Reveal error messages only to designated CIHA personnel.

Information Management and Retention
[NIST SI-12]
CIHA shall handle and retain information within an information system and information output from the system in accordance with applicable federal laws, directives, policies, regulations, State standards, and operational requirements.

Forwarding and auto-forwarding of CIHA data must follow the *CIHA Internet and Electronic Mail Acceptable Use Policy*. CIHA shall also develop procedures to encourage due care by users when forwarding electronic messages so that users do not do the following:

a. Knowingly send out an email message that contains viruses, Trojan horses, or other malware;
b. Use the electronic-mail system or network resources to propagate chain letters, misinformation, or hoax information;
c. Forward any Restricted or Highly Restricted information to any unauthorized party without prior management approval, and without appropriate protections, such as encryption;
d. Forward the wrong attachment;
e. Send information or files that can cause damage to the individuals served or having interaction with CIHA;
f. Send unsolicited messages to large groups of people except as required to conduct CIHA business.

Communications sent or received by CIHA email systems and/or email communications on CIHA business in personal email accounts may be public records as defined by the North Carolina Public Records Law, N.C.G.S. §132.1, *et seq.*.

Memory Protection
[NIST SI-16]
CIHA shall implement security safeguards to protect the volatile memory of its information systems from unauthorized code execution.

a. CIHA shall implement data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism;
b. CIHA shall protect the integrity and ensure the stability of the CIHA network from fraudulent use and/or abuse resulting from access and use of the network and to define the security attributes delivered with network services.

CIHA CYBERSECURITY SYSTEM AND INFORMATION INTEGRITY POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 8/17/2023

Revision Information:

Date	Section Updated	Change
8/17/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
8/17/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA" and added "Cybersecurity" after "CIHA"
8/17/2023	Information Box	Added "Last Reviewed" date and added "Policy Owner" and identified the role
8/17/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
8/17/2023	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"
8/17/2023	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
8/17/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"

8/17/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
8/17/2023	Policy	Added that a Cybersecurity System and Information Integrity Policy must be implemented and maintained in compliance with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"
8/17/2023	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
8/17/2023	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
8/17/2023	Policy	Added "documentation, dissemination, implementation, and maintenance of a system and information integrity policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Cybersecurity System and Information Integrity Policy*
8/17/2023	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"
8/17/2023	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
8/17/2023	Procedural Guidelines	Updated NIST SI-1: Added the "Internal Controls" section on NIST SI-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 cybersecurity maintenance of information systems, technology devices, and supporting infrastructure
8/17/2023	Procedural Guidelines	Added that "CIHA System and Information Integrity procedures must include the necessary controls" to facilitate the implementation of this Policy
8/17/2023	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
8/17/2023	Procedural Guidelines	Added "NC" to all instance of "DHHS" and changed "State" to "NCDHHS"
8/17/2023	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 SI-1, 4, 4(2), 4(4), 4(5), 6, and 12
8/17/2023	Procedural Guidelines	Changed "organization" to "CIHA"

8/17/2023	Procedural Guidelines	Amended NIST SI-2(1) to NIST PL-9, NIST SI-3(1) to NIST PL-9, NIST SI-3(2) to NIST SI-3, and Software, Firmware, and Information Integrity NIST SI-7(14) to Least Functionality NIST CM-7(8)SI-2;
8/17/2023	Procedural Guidelines	Added the reference to the *CIHA Cybersecurity Risk Assessment Policy* in regard to CIHA having an explicit and documented patching and vulnerability policy Item a(ix): Added the layman definition for "zero-day vulnerability" as follows, "which is a situation where an exploit is used before the developer of the software knows about the vulnerability" and Defined methods as being "other compensating control methods" in regard to when a vulnerability risk is "critical" or "high-level" and no patch is available, steps must be taken to mitigate the risk through these type of methods and deleted "workarounds" as being an example of this and added "group policy objects" in its place Item a(x): Deleted "EBCI Tribal Option management and the State's Security Liaison" and added in its place the "CIHA CISO" in regard to the person who needs to be notified of the condition and remediation plan and execution of a plan when a "critical" or "high-level" risk vulnerability cannot be totally mitigated within the requisite period
8/17/2023	Procedural Guidelines	SI-2: Vulnerability Risk Ratings and Remediation: Added "Where technically configurable" before "risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the CVSS, and system exposure using a scale of 0-10.0 Critical-level Risk:

		Added “and could cause functionality to cease, exfiltration of data, or an intruder to gain access to the network or IT asset,” regarding a critical-level risk present in most sensitive portions of the network or IT asset High-level Risk: Added “This vulnerability could cause functionality to cease or control of the network or IT asset to be gained by an intruder” Medium-level Risk: Added “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” Low-level Risk: Deleted “Low-level risk vulnerabilities must be mitigated or remediated within 90 days Vulnerability Mitigation and Remediation: Moved the low-, medium-, and high-level guidelines for how many days that mitigating or remediating these type of vulnerabilities needs to occur from the “Vulnerability Risk Ratings and Remediation” section to a new section titled, “Vulnerability Mitigation and Remediation”
8/17/2023	Procedural Guidelines	SI-3: Changed CIHA’s “information resources” to “information systems” as to what layers of information security to defend against attacks will be implemented on and Added “endpoint protection” as a layer of information security that defends against attacks on EBCI Tribal Option information systems Item c(i): Replaced “EBCI Tribal Option security policy” with “*CIHA Cybersecurity System and Information Integrity Policy*” to provide a more detailed description Item i: Added “spyware” as an example of malicious software

		Item j: Changed web browser software for configuration "requirements" to "procedural guidelines"
8/17/2023	Procedural Guidelines	SI-4: Item b(i): Changed the entity in the statement: all hardware connected to the CIHA network or is cloud hosted shall be configured to support "state and federal" instead of "State/EBCI Tribal Option" management and monitoring standards Item d: Deleted "the State" as being an entity that could be indicated as having an increased risk
8/17/2023	Procedural Guidelines	SI-4(4): Item a(3): Deleted the example of "DIT" as an outside entity that manages the firewall and added that "CIHA IT personnel" is who the outside entity who manages the firewall is responsible for providing CIHA's firewall policy to Item b(i): Changed "information system security officers" to "information system security analysts" as to those who will be alerted by CIHA information systems when indications of compromise, potential compromise, or detected suspicious events occur SI-4(5): Item b(ii): Added "wireless access points, encrypted tunnels, and web content filters" as examples of boundary protection devices
8/17/2023	Procedural Guidelines	SI-5: Item d: Deleted "notifies NCDHHS" as something CIHA does when implementing security directives in accordance with established timeframes of the degree of noncompliance Item e(i and ii): Changed "NCDHHS" to "State departments" as an entity from which any

		updates or notices from must be implemented per CIHA change control and/or incident response procedures, as well as the entity who must be contacted with any security alert/advisory concerns or must be notified when the actions are completed
8/17/2023	Procedural Guidelines	SI-7(1) Item c: Added non-technical language to identify "cryptographic checksums"
8/17/2023	Procedural Guidelines	SI-12: Amended the title of the EBCI Tribal Option policy from *Acceptable Use* to *CIHA Internet and Electronic Mail Acceptable Use Policy* and Changed that CIHA shall develop "procedures" instead of "policies" to encourage due care by users when forwarding electronic messages so that users do not do the things listed within this section In the information that communications sent or received by CIHA email systems and/or email communications on CIHA business in personal emails accounts may be public records, the following was deleted: These "shall be managed according to the requirements of EBCI Tribal Option's record retention policy"
8/17/2023	Policy Implementation/ Revision Information	Added policy revision information table