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 Configuration Management Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 1/5/2023

LAST REVIEWED: 9/28/2023

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Cybersecurity Configuration Management 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 Configuration Management 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 CM-1]

Note: CM = Acronym used by NIST for Configuration Management

CIHA shall implement and maintain a Cybersecurity Configuration Management 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 Configuration Management Policy* shall include preventive and timely maintenance activities that consist of:

- Developing, documenting, disseminating, implementing, and maintaining a configuration management policy and procedural guidelines;
- Establishing a minimum acceptable level of security;
- Training requirements for configuration management;
- Implementing automated tools and software for configuration management;
- Developing a Security Impact Analysis for configurations;
- Maintaining baseline configuration standards, automation, retention of previous configurations, and configurations for high-risk areas;
- Implementing the configuration of information systems that provide only essential capabilities in which systems can prevent the execution of non-essential programs, and a review of those functions performed periodically;
- Identifying all information system components through an asset inventory;
- Employing automated mechanisms to detect the presence of unauthorized hardware, software, and firmware;
- Ensuring only authorized individuals have appropriate access to configuring systems in which access is enforced through Role-Based Access Control;
- Implementing secure configurations that use automated mechanisms for central management, application, and verification of configuration settings, resulting in swift and immediate action when unauthorized changes are found;

- Documenting and formalizing practices that require all configuration changes to be requested, reviewed, evaluated, approved, and confirmed.

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.

Configuration Control Board

A Configuration Control Board (CCB)--also known as the Configuration Management Board--plays an essential role in an organization's overall information technology strategy. Typically chaired by the CIO, this Board includes voting representatives from every department in the entity for cross-functional input and analysis.

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.

System Hardening
A process intended to eliminate a means of attack by patching vulnerabilities and turning off non-essential services.

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

Configuration Management Policy and Procedural Guidelines
[NIST CM-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 configuration management process and the family of configuration management security controls. The configuration management 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 Configuration Management principles established in NIST, "Configuration Management" control guidelines, as the official standards for this security domain. The "CM" designator identified in each control represents the NIST-specified identifier for the Configuration Management 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 Configuration Management 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 configuration management 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.

Baseline Configuration

[NIST CM-2]

CIHA shall provide standard security configurations that provide a baseline level of security controls and reduce risk from security threats and vulnerabilities. The baseline incorporates industry standards and NIST requirements. These NIST requirements allow CIHA to improve information system performance, decrease operating costs, and ensure public confidence in the CIA of State departments and CIHA data. CIHA shall ensure the following is done:

1. For each information system, a current baseline configuration must be developed, reviewed, approved, documented, and maintained under configuration control. The CIHA IT Department shall be responsible for all baseline configurations;
2. A baseline configuration must document and provide information about the components of an information system, including the following:
    a. Standard operating system/installed applications with current version numbers;
    b. Standard software load for workstations, servers, network components, mobile devices, and laptops;
    c. Up-to-date patch level information;
    d. Network topology;
    e. Logical placement of the component within the system and enterprise architecture;
    f. Technology platform;
3. As the information system changes over time, new baselines must be created in order to maintain the baseline configuration;
4. An information system's baseline configuration is consistent with NIST. Product versions of security-related technologies must be either N or at N-1 and must be kept up to date by applying the latest security patches;
5. Using best practice system hardening baselines for the operating systems. Refer to **Configuration Settings** **[NIST CM-6]** for a list of approved baselines;
6. In cases where a baseline security configuration does not exist for an operating system, the CIHA CISO or designee shall ensure a baseline security configuration is developed, documented, disseminated, implemented, and approved;
7. Any exceptions to baseline security configurations are documented and approval is obtained by the CIHA CISO or designee;
8. Records are maintained to confirm the implementation of baseline security configurations for each IT system CIHA manages;
9. Previous versions of baseline configurations of the information system are retained to support rollback (i.e., hardware, software, firmware, configuration files, and configuration records);
10. The baseline configuration for information systems is reviewed and updated:

a. Annually, at a minimum;
b. When required, due to system upgrades, patches, or other significant changes which have occurred in the baseline configuration;
c. As an integral part of information system component installations and upgrades;
d. When there is an increase in interconnection with other systems outside the authorization boundary or when there are significant changes in the security requirements for the system.

Configuration Change Control

[NIST CM-3]

CIHA shall manage changes to systems and application programs to protect the systems and programs from failure as well as security breaches. Adequate management of system change control processes shall require the following:

1. Safeguard production systems during modification, including emergency changes;
2. Enforcement of formal change control procedures for documentation and authorizations;
3. Proper authorization and approvals at all levels;
4. Successful testing of updates and new programs, prior to being moved into a production environment;
5. Determining the types of changes to the information system that are configuration controlled;
6. Reviewing proposed configuration-controlled changes to the information system and approving or rejecting these changes with explicit consideration for Security Impact Analysis;
7. Documenting configuration change decisions associated with the information system;
8. Implementing approved configuration-controlled changes to the information system;
9. Retaining records of configuration-controlled changes to the information system for the life of the system;
10. Auditing and reviewing activities associated with configuration-controlled changes to the information system;
11. When configuration changes occur, a Configuration Control Board convenes to coordinate and provide oversight for configuration change control activities;
12. Testing, validating, and documenting changes to the information system before implementing the changes in the system;
13. Ensuring updates, which address significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources. Vulnerability Management requirements are addressed in the *CIHA Cybersecurity System and Information Integrity Policy*;
14. Integrating procedures for application change control and operational change control. This effort should include the following processes, controls, and best practices:

a. Controls and approval levels for updating libraries;
b. Requiring formal agreement and approval for any changes;
c. Restricting library content;
d. Restricting programmers' access to only those parts of the system necessary for their work;
e. Version control for each application;
f. Tying program documentation updates to source code updates;
g. Audit logs that track all accesses to libraries, copying and use of source code, and updates posted to libraries;

15. Defining job responsibilities/restrictions and establishing authority levels for the following:
    a. Program librarian(s);
    b. Developers (i.e., should neither test their own code nor promote it into production);
    c. Other IT personnel;
16. Identifying personnel who are authorized to make or submit changes to the source library (i.e., a program librarian) for each major application to control check-in/check-out;
17. Providing role-based training for business and technical users, covering new features and security controls introduced by the upgrade;
18. Providing role-based training for all security personnel;
19. Using rollback procedures that are designed to recover the previous stable version of programs.

Impact Analyses

[NIST CM-4]

When significant changes are planned for or made to a system, the system owners and the CIHA CISO shall conduct a Security Impact Analysis to determine which controls shall be assessed for proper implementation and operation. Security Impact Analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. The following Security Impact Analysis activities shall be incorporated into the documented configuration change control process by:

1. Identifying the federal, state, and local regulatory or legal requirements that address the security, CIA and privacy requirements for CIHA business functions and/or services;
2. Identifying restricted or highly restricted information stored in CIHA's files, as well as the potential for fraud, abuse/misuse, and/or other illegal activity. Data classifications are defined within the CIHA *Cybersecurity Media Protection Policy*;
3. Identifying essential access control mechanisms used for requests, authorization, and access approval in support of critical CIHA business functions and/or services;
4. Identifying the processes used to continuously monitor and report to management on the applications, tools, and technologies CIHA has implemented to adequately manage the risk as defined by CIHA (i.e., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.);

5. Identifying CIHA's IT Change Management and Vulnerability Assessment processes;
6. Identifying the security mechanisms that are in place to protect CIHA data (i.e., the use of encryption, data masking, etc.);
7. Analyzing and evaluating changes for their impact on security, prior to approval and implementation;
8. Referring to the CIHA *Cybersecurity Risk Assessment Policy* for the Security Impact Analysis requirements and definitions.

Configuration Settings

[NIST CM-6]

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Security-related configuration settings can include, for example:

- Cloud computing physical/virtual servers (i.e., database, electronic mail, authentication, web, proxy, file, domain name);
- Workstations, input/output devices (i.e., scanners, copiers, and printers);
- Network components [i.e., firewalls, routers, gateways, voice and data switches (telecommunication equipment), wireless access points, network appliances, sensors];
- Operating systems, middleware, and applications.

CIHA shall implement the following requirements:

1. A standard set of required configuration settings must be established and documented for information technology products. Standard Configuration Documents (SCDs) must detail the configuration settings;
2. The selected configuration settings are specifically designed for the information system, the settings must reflect the most restrictive mode consistent with operational requirements and must be derived from the following sources, listed in order of precedence:
    a. National Institute of Standards and Technology (NIST) Recommended Configurations and Checklists: http://checklists.nist.gov/; https://public.cyber.mil/stigs/https://benchmarks.cisecurity.org/downloads/benchmarks/
    b. IRS Safeguards Program, Resources Section: Safeguard Computer Security Evaluation Matrix (SCSEM): https://www.irs.gov/uac/safeguards-program, for systems that store, process, or transmit federal tax information (FTI);
3. To identify, document, and approve any deviations from established configuration settings for information systems;
4. To monitor and control changes to the configuration settings in accordance with CIHA policies and procedures.

Least Functionality

[NIST CM-7]

The principle of least functionality provides that information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports (serial, Ethernet, USB, etc.), protocols, and/or services that are not integral to the operation of that information system. This approach minimizes potential risks for the exploitation of the unnecessary ports and services.

CIHA shall implement the following requirements to provide least functionality:

1. Configure information systems to provide least functionality;
2. Where technically configurable, CIHA will limit component functionality to a single function per device (i.e., email server, web server, etc.);
3. Disable any functions, ports, protocols, and services within an information system that are deemed to be unnecessary and/or non-secure. CIHA can either make a determination of the relative security of a function, port, protocol, and/or service or base a security decision on the assessment of other entities.

The use of the following functions, ports, protocols, and/or services must be specifically prohibited or restricted, including, but not limited to:

a. ARINC-GATEWAY Port 55210 / Transmission Control Protocol (TCP)
b. Background File Transfer Protocol (BFTP) Port 152 / TCP
c. Border Gateway Protocol (BGP) Port 179 / (TCP)
d. Courier Port 530 / TCP, User Datagram Protocol (UDP)
e. File Transfer Protocol (FTP) Ports 20, 21 / TCP
f. Finger Port 79 / TCP
g. Hypertext Transfer Protocol (HTTP) Port 80 / TCP; 443 / TCP
h. HTTP-MGMT Port 280 / TCP
i. Identification Protocol (IDENT) Port 113 / TCP, UDP
j. Internet Control Messaging Protocol (ICMP) - block incoming echo request (ping and Windows traceroute) block outgoing echo replies, time exceeded, and destination unreachable messages except “packet too big” messages (type 3, code 4)
   Note: Blocking ICMP will restrict legitimate use of ping in an effort to restrict malicious activity.
k. Internet Message Access Protocol (IMAP) Port 143 / TCP, UDP
l. Internet Relay Chat (IRC) Port 194 / UDP
m. Lightweight Directory Access Protocol (LDAP) Port 389 / TCP, UDP
n. Line Printer Daemon (LPD) Port 515 / TCP
o. LOCKD Port 4045 / TCP, UDP
p. Network Basic Input Output System (NetBIOS) Ports 135, 445 / TCP, UDP; 137-138 / UDP; 139 / TCP
q. Network News Transfer Protocol (NNTP) Port 119 / TCP
r. Oracle Names (ORACLENAMES) Port 1575 / TCP, UDP

s. Port Mapper (PORTMAP/RPCBIND) Port 111 / TCP, UDP
t. Post Office Protocol 3 (POP3) Ports 109-110 / TCP
u. r Services Ports 512-514 / TCP
v. Session Initiation Protocol (SIP) Port 5060 / TCP, UDP
w. Shell Port 514 / TCP
x. SIDEWINDER-COBRA, (S) Port 2809 & 9002 / TCP
y. Simple Network Management Protocol (SNMP) Ports 161-162 / TCP, UDP
z. Snare Port 509 / TCP, UDP
aa. Socket Secure (SOCKS) Port 1080 / TCP
bb. SOFTWAREAGWEBMETHODS Port 6849 / TCP
cc. Structured Query Language (SQL) Port 118 / TCP, UDP; Port 156 / TCP, UDP
dd. Super Duper Telnet Port 95 / TCP
ee. SYMANTEC-ITA Port 3833-3836 / TCP
ff. Syslog Port514/UDP
gg. Telnet Port 23 / TCP
hh. TIMBUKTU Port 407 / TCP, UDP
ii. TIME Port 37 / TCP, UDP
jj. Trivial File Transfer Protocol (TFTP) Port 69 / UDP
kk. VNC-SERVER Port 5900 / TCP
ll. X Windows Ports 6000-6255 / TCP
mm. YAK-CHAT Port 258 / UDP

4. Identify and remove/disable unauthorized and/or non-secure functions, ports, protocols, services, and applications;
5. An information system shall prevent program execution in accordance with CIHA-defined policies regarding software program usage and restrictions and/or rules authorizing the terms and conditions of software program usage.

System Component Inventory

[NIST CM-8]

CIHA shall update the inventory of information system components as an integral part of component installations, removals, and information system updates. CIHA shall do the following:

1. Develop, document, and maintain an inventory of information system components that accurately reflects the current information system environment;
2. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories;
3. Inventory all components within the authorization boundary of the information system (this may include inter-connected systems). The inventory includes information deemed necessary to achieve effective property accountability and is at the level of granularity for tracking and reporting the following, for example:
   a. Hardware inventory specifications (manufacturer, type, model, serial number, physical location);
   b. Software license information;

c. Information system / component owner(s);
d. Associated component configuration standard;
e. Software/firmware version information;
f. Machine name and network address for a networked component/device;

4. Review and audit information system component inventory quarterly;
5. Include assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory;
6. Review and update the information system component inventory annually, at a minimum.

System Component Inventory-Automated Unauthorized Component Detection:
[NIST CM-8 (3)]
CIHA shall employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the CIHA IT network. CIHA may take one or more of the following actions when unauthorized components are detected:

a. Disable network access to such components;
b. Isolate the components;
c. Notify CIHA-defined personnel.

This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems. Automated mechanisms can be implemented within information systems or in other separate devices.

Configuration Management Plan

[NIST CM-9]
CIHA shall develop a Configuration Management Plan is developed in connection with the configuration baselines for the systems to support oversight of configuration changes to CIHA information technology systems and infrastructure. CIHA shall do the following:

1. Address roles, responsibilities, and configuration management processes and procedures;
2. Define the configuration items for the information system, and when in the system development life cycle (SDLC), the configuration items are placed under configuration management;
3. Establish the means for identifying configuration items throughout the SDLC and a process for managing the configuration of the configuration items;
4. Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development. In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process;
5. Define detailed processes and procedures for how configuration management is used to support SDLC activities at the information system level;

6. Describe how:
    a. To move a change through the Change Management process;
    b. Configuration settings and configuration baselines are updated;
    c. The information system component inventory is maintained;
    d. Development, test, and operational environments are controlled;
    e. Documents are developed, released, and updated;
7. Create a step-by-step implementation plan for every configuration change;
8. Require that software implementation plans follow change control procedures;
9. Protect the Configuration Management Plan from unauthorized disclosure and modification;
10. The configuration management approval process must include the following:
    a. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system;
    b. Designation of security personnel that would conduct an Impact Analysis prior to the implementation of any changes to the information system.

Software Usage Restrictions

[NIST CM-10]

CIHA shall ensure the following:

1. Providing CIHA employees, contractors, and other third parties with guidelines for obeying software licensing agreements to include open-source software and shall not permit the installation of unauthorized copies of software on technology devices that connect to the CIHA network:
    a. Employees, contractors, and other third parties involved in the illegal reproduction of software can be subject to civil damages and criminal penalties;
    b. Employees, contractors, and other third parties shall use software and associated documentation in accordance with contract agreements and copyright laws;
    c. Employees, contractors, and other third parties who make, acquire, or use unauthorized copies of software shall be disciplined as appropriate. Such discipline may include termination;
    d. Open-source software must adhere to a secure configuration baseline checklist from the U.S. Government or industry;
2. Informing their users about any proprietary rights in databases or similar compilations and the appropriate use of such data;
3. Controlling and documenting the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work;
4. Establishing procedures for using, distributing, and removing software within CIHA to ensure that their use of software meets all copyright and licensing requirements. Procedures shall include the development of internal controls to monitor the number of licenses available and the number of copies in use.

User-Installed Software

[NIST CM-11]

Only standard approved software shall be installed on CIHA-owned assets with any deviations being pre-approved by the CIHA CISO and reviewed by the CIHA CIO. For user-installed software, CIHA shall ensure the following:

1. Establishing policies that govern the installation of software by users;
2. Enforcing software installation policies through automated methods, if available and technically configurable;
3. Monitoring policy compliance quarterly, at a minimum;
4. Ensuring only software programs that are from validated media are installed and are free of harmful code or other destructive aspects.

Enforcement

Violations of this Policy or failure to implement provisions of this Policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

CIHA CYBERSECURITY CONFIGURATION MANAGEMENT POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 1/5/2023

Revision Information:

Date	Section Updated	Change
1/5/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
1/5/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA"
1/5/2023	Information Box	Added "Last Reviewed" date
1/5/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
1/5/2023	Purpose	Added "North Carolina State departments, including NCDIT, NCDHHS, and NC Medicaid" as the entities that we must meet compliance requirements with and deleted "NCDHHS/EBCI Tribal Option Contract"
1/5/2023	Purpose	Changed "EBCI Tribal Option" to "State departments" in the following: In support of the purpose, this Policy has been developed to ensure CIA, privacy, and security of the information assets of CIHA, exceeding "State departments'" compliance requirements
1/5/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"
1/5/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties

1/5/2023	Policy	Added that a Configuration Management Policy must be implemented and maintained in compliance with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"
1/5/2023	Policy	Amended the title of the "*EBCI Tribal Option Configuration Management Policy*" by deleting "EBCI Tribal Option" and replacing it with "CIHA"
1/5/2023	Policy	Deleted "and procedures" as having to be reviewed annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary
1/5/2023	Policy	Deleted: "In addition, if modifications are required to meet a change in the DHHS Contract, a mutually agreed upon date shall be determined for a policy update" because this Policy now resides with CIHA, not EBCI Tribal Option
1/5/2023	Policy	Added "dissemination" and "maintenance of a configuration management policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Configuration Management Policy*
1/5/2023	Policy	Added "for configurations" in the information bullet: Developing a Security Impact Analysis for configurations and added "components" in the information bullet: Identifying all information system components through an asset inventory
1/5/2023	Policy	Changed "Identifying" to "Maintaining" when referring to "baseline configuration standards, automation, retention of previous configurations, and configurations for high-risk areas

1/5/2023	Definitions	Amended definitions by supplementing additional language for "CEO," "CIO," "CISO," and "System Hardening" and deleted the definition for "EBCI" and "EBCI Tribal Option Contract" and added definitions for "CIHA Workforce," "NIST," and "Procedural Guidelines"
1/5/2023	Procedural Guidelines	Changed the heading title from "PROCEDURES" to "PROCEDURAL GUIDELINES" and added "CIHA ensures that all applicable users follow the procedural guidelines for purposes of complying with CIHA policies"
1/5/2023	Procedural Guidelines	Updated NIST CM-1: Added the "Internal Controls" section on NIST CM-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
1/5/2023	Procedural Guidelines	Added that "CIHA Configuration Management procedures must include the necessary controls" to facilitate the implementation of this Policy
1/5/2023	Procedural Guidelines	Added that policies and procedures are a critical component of CIHA's system of internal controls, which provides understanding to personnel about their roles, responsibilities, acceptable uses, and important information that relates to maintenance. Added that these policies and procedures are to be reviewed and updated annually
1/5/2023	Procedural Guidelines	Added "NC" to all instances of "DHHS"
1/5/2023	Procedural Guidelines	Added the sentence "The baseline incorporates industry standards and NIST requirements" in NIST CM-2

1/5/2023	Procedural Guidelines	Identified that the referenced NIST requirement allows CIHA to ensure public confidence in CIA of "State departments" and "CIHA" data (deleted "DHHS" data from the text)
1/5/2023	Procedural Guidelines	Amended that the "CIHA" IT Department be responsible for "all" baseline configurations and deleted that IT was responsible "for enterprise solutions"
1/5/2023	Procedural Guidelines	Amended the following heading titles to reflect those in the *NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*: NIST CM-4, 8, and 8(3)
1/5/2023	Procedural Guidelines	Deleted "EBCI Tribal Option" before all instances of "CISO" and added "CIHA" before all instances of "CISO" and "CIO"
1/5/2023	Procedural Guidelines	Replaced that an information system's baseline configuration is consistent with "NIST" instead of "statewide enterprise architecture"
1/5/2023	Procedural Guidelines	Added "disseminated" and "implemented" as actions that the CIHA CIOS or designee shall ensure be performed for baseline security configuration
1/5/2023	Procedural Guidelines	Replaced "NC State Liaison" with "CIHA CISO" as the individual whose approval must be obtained for any exceptions to baseline security configurations
1/5/2023	Procedural Guidelines	Added "documentation and authorizations" as to what "Enforcement of formal change control procedures" are for in the Configuration Change Control section
1/5/2023	Procedural Guidelines	Amended the title "*EBCI Tribal Option" System and Information Integrity Policy* to "*CIHA*"

1/5/2023	Procedural Guidelines	Added "Providing role-based training for all security personnel" as a requirement for adequate management of system change control processes
1/5/2023	Procedural Guidelines	Added "integrity and availability" to "confidentiality" when identifying the federal, state, and local regulatory or legal requirements that address it for CIHA business functions and/or services
1/5/2023	Procedural Guidelines	Amended the title of the "*EBCI Tribal Option Data Classification and Handling"* to *"CIHA Media Protection Policy"* where data classifications are defined from
1/5/2023	Procedural Guidelines	Added "continuously" to describe monitoring on the applications, tools, and technologies
1/5/2023	Procedural Guidelines	Amended the title "*EBCI Tribal Option" Risk Assessment Policy* to "*CIHA*"
1/5/2023	Procedural Guidelines	Changed "Mainframe computers" to "Cloud computing" and "servers" to "physical/virtual" servers and added "(telecommunication equipment)" as an example of "voice and data switches"
1/5/2023	Procedural Guidelines	Deleted "DHHS standards" as the selected configuration settings that are specifically designed for the information system
1/5/2023	Procedural Guidelines	Deleted "Defense Information Systems Agency-EBCI Tribal Option Security Checklists and Standard Technical Implementation Guides" and the web address; deleted "National Security Agency-EBCI Tribal Option Configuration Guidance" and the web address; deleted "the Centers for Internet Security Benchmarks" and the web address as required items

1/5/2023	Procedural Guidelines	Added "(serial, Ethernet, USB, etc.)" as examples of "ports" that are non-essential functions to the operation of that information system
1/5/2023	Procedural Guidelines	Deleted the following list items where use of them is strictly prohibited or restricted: • Domain Name System be (DNS) Port 53 / TCP, UDP • Network File System (NFS) Port 2049 / TCP, UDP • Network Time Protocol (NTP) Port 123 / TCP • Secure Shell (SSH) Port 22 / TCP • Secure File Transfer Protocol (SFTP) Port 115 TCP, UDP • Simple Mail Transfer Protocol (SMTP) Port 25 / TCP
1/5/2023	Procedural Guidelines	Added "quarterly" as the cadence to review and audit information system component inventory
1/5/2023	Procedural Guidelines	Changed the "information system" to the "CIHA IT network" as the place CIHA shall employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within
1/5/2023	Procedural Guidelines	Added the sentence "This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devise" before the sentence "Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems"
1/5/2023	Procedural Guidelines	Added "infrastructure" as another item of what CIHA shall develop a Configuration Management Plan to support oversight of configuration changes to

1/5/2023	Procedural Guidelines	Changed "DHHS network" to "CIHA network" as being unpermitted places where installation of unauthorized copies of software on technology devices connect to
1/5/2023	Procedural Guidelines	Changed "NC State security liaison" to "CIHA CIO" as the person who reviews standard approved software that is installed on CIHA owned assets and any deviations that have been pre-approved by the CIHA CISO
1/5/2023	Procedural Guidelines	Delete "Referring to the EBCI Tribal Option *Acceptable Use Policy* for additional requirements" as an item that CIHA ensures for user-installed software
1/5/2023	Procedural Guidelines	Deleted the reference to the *CIHA Internet and Electronic Mail Acceptable Use Policy*
1/5/2023	Policy Implementation/ Revision Information	Added policy revision information table
9/28/2023	Policy Title	Added "Cybersecurity" after "CIHA" in the title
9/28/2023	Information Box	Amended "Effective Date," updated "Last Reviewed" date, and added "Policy Owner" and identified the role
9/28/2023	Purpose	Added information "systems and technology devices" as items that must be protected from unauthorized access, loss, or damage
9/28/2023	Staff Governed By This Policy	Added "and/" to "CIHA vendors and/or subcontractors"
9/28/2023	Procedural Guidelines	Added "as it applies" and "technology devices" to "CIHA develops, documents, disseminates, implements, and maintains this Policy, as it applies, to all covered personnel involved in the acquisition, development, operation, and cybersecurity maintenance of information systems, "technology devices," and supporting infrastructure"

9/28/2023	Procedural Guidelines	Deleted “NIST outlines the Awareness and Training requirements that CIHA must implement and maintain in order to be compliant with this Policy”
9/28/2023	Procedural Guidelines	Added “Cybersecurity” after “CIHA” in the applicable cybersecurity policy titles listed within this document