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 Maintenance Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 3/15/2023

LAST REVIEWED: 10/19/2023

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Cybersecurity Maintenance 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 Maintenance 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 MA-1]

Note: MA = Acronym used by NIST for Cybersecurity Maintenance

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

- Developing, documenting, disseminating, implementing, and maintaining a cybersecurity maintenance policy and procedural guidelines;
- Using various best practice initiatives to ensure that all aspects of CIHA's cybersecurity maintenance activities are documented and performed as necessary to maintain the confidentiality, integrity, and availability (CIA) of information systems;
- Scheduling, performing, and documenting cybersecurity maintenance and repairs for all applicable information systems and reviewing those cybersecurity maintenance and repair records;
- Using initiatives for removing and sanitizing information systems for cybersecurity maintenance, along with ensuring information systems and related controls are functioning as designed;
- Assuring that only authorized personnel can perform cybersecurity maintenance activities, and that all necessary hardware and software tools will be available for performing all necessary cybersecurity maintenance activities.

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 has adopted the Cyber Security Framework (CSF) provided by NIST, which provides guidance on how to prevent, detect, and respond to cyberattacks.

Native Logging
Activity logs which use a database server's built-in tools to record activity at the database, database object, and user level.

Procedural Guidelines
Guidelines for developing operational procedures.

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

Cybersecurity Maintenance Policy and Procedural Guidelines
[NIST MA-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 cybersecurity maintenance process and the family of cybersecurity maintenance security controls. The cybersecurity maintenance 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 Cybersecurity Maintenance principles established in NIST, "Cybersecurity Maintenance" control guidelines, as the official standards for this security domain. The "MA" designator identified in each control represents the NIST-specified identifier for the Cybersecurity Maintenance 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 Cybersecurity Maintenance 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 cybersecurity maintenance 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.

Controlled Cybersecurity Maintenance

[NIST MA-2]

CIHA shall do the following:

1. Establish normal change controls and cybersecurity maintenance cycles for information technology resources (i.e. hardware, software, etc.);
2. Perform cybersecurity maintenance of operating systems in accordance with approved CIHA cybersecurity maintenance security procedures;
3. Consider the following issues when supporting operating systems:
    a. New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities;
    b. Periodic cybersecurity maintenance improves the performance of operating systems (i.e., hard drive defragmentation);
    c. The operating systems on servers, minicomputers, and mainframes usually require daily cybersecurity maintenance tasks and routines that may be initiated manually as a result of an alert or logged event or may be scripted to run automatically when a certain threshold or limit is exceeded;
4. Ensure that system administrators apply all current cybersecurity maintenance and security vulnerability patches and that only essential application services and ports are enabled and opened in the system's firewall;
5. Review and compare operating system cybersecurity maintenance logs to other system logs on a regular basis to ensure the following:
    a. Cybersecurity maintenance tasks continue to function as expected;
    b. Operating systems continue to operate within accepted thresholds;
    c. System security is not being compromised by cybersecurity maintenance tasks;
    d. Cybersecurity maintenance tasks do not adversely affect computer capacity or performance;
6. Ensure that software faults or bugs are formally recorded and will be reported to those responsible for software support and cybersecurity maintenance;
7. Restrict physical access to systems (i.e., locate the systems in a protected data center or dedicated, locked storage rooms);
8. Apply a comprehensive set of management tools (i.e., cybersecurity maintenance utilities, remote support, enterprise management tools, and backup software) in order to keep information technology systems up-to-date (i.e., by applying approved change management and patch management processes);
9. Monitor information systems [i.e., using Simple Network Management Protocol (SNMP)] so that events such as hardware failure and attacks against them can be detected and responded to effectively. For public networks, management software tools that communicate with devices shall use SNMP version 3 for network management. For private networks, management software tools that communicate with devices may use SNMP version 2 or version 3 for network management;

10. Review cybersecurity maintenance records on a regular basis to verify configuration settings, evaluate password strengths, and assess activities performed on the server (i.e., by inspecting logs);
11. Provide or arrange cybersecurity maintenance support for all equipment that is owned, leased, or licensed by CIHA;
12. Arrange support services through appropriate cybersecurity maintenance agreements or with qualified technical support personnel;
13. When cybersecurity maintenance support is provided by a third party, confidentiality agreements shall be signed by authorized representatives of the third party before any cybersecurity maintenance support is performed;
14. Schedule, perform, and document information system cybersecurity maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and organizational requirements and review those cybersecurity maintenance and repair records;
15. Maintain records of all cybersecurity maintenance activities;
16. Approve and monitor all cybersecurity maintenance activities to include routinely scheduled cybersecurity maintenance and repairs, as well as whether the equipment is serviced onsite, remotely, or moved to another location;
17. Ensure that before the information system or any of its components are removed from the facility for repair an appropriate official has approved it first;
18. Sanitize equipment when the information system or any of its components require offsite cybersecurity maintenance or repairs by following the proper procedure to remove all protected health information (PHI) and other Restricted or Highly Restricted information from associated media;
19. Verify the proper functionality of all potentially impacted security controls after cybersecurity maintenance is performed;
20. Restrict the use of root/administrator privilege to only when required to perform duties;
21. Establish normal change controls and cybersecurity maintenance cycles for all information technology resources (i.e. hardware, software, etc.);
22. Maintain cybersecurity maintenance records for the information system to include the following:
    a. Date and time of cybersecurity maintenance;
    b. Name of the individual performing the cybersecurity maintenance;
    c. Name of escort, if necessary;
    d. Description of the cybersecurity maintenance performed;
    e. List of equipment removed or replaced (including identification numbers, if applicable);

23. Employ automated mechanisms to schedule and conduct the cybersecurity maintenance as required and to create up-to-date, accurate, complete, and available records of all cybersecurity maintenance actions.

Cybersecurity Maintenance Tools
[NIST MA-3]

CIHA shall observe the following requirements for the use of cybersecurity maintenance tools:

1. Approve, control, and monitor the use of cybersecurity maintenance tools and maintain these tools on an ongoing basis;
2. Prevent the unauthorized removal of cybersecurity maintenance equipment, which can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers as follows:
    a. Verify that there is no CIHA data contained on the equipment;
    b. Sanitize or destroy the equipment;
    c. Retain the equipment within the facility; or
    d. Release to a third-party disposal facility upon management approval explicitly authorizing the removal of the equipment from the facility.

Cybersecurity Maintenance Tools - Inspect Tools:
[NIST MA-3(1)]

Inspect all cybersecurity maintenance tools that are carried into the facility by cybersecurity personnel, checking for unauthorized modifications or malicious code. Handle any such incidents by following the CIHA incident response policies and procedures.

Cybersecurity Maintenance Tools - Inspect Media:
[NIST MA-3(2)]

Check all media containing diagnostic and test programs for malicious code before they are used in the information system; Inspect media that contains cybersecurity maintenance diagnostic and test programs, and if the CIHA CISO or his/her designee determine that the media contains malicious code, handle the incident by following the CIHA incident handling policies and procedures.

Nonlocal Cybersecurity Maintenance
[NIST MA-4]

CIHA shall ensure that all nonlocal (remote access) cybersecurity maintenance and diagnostic activities of information systems conducted by individuals through either the internal or external network observe the following requirements:

1. Approve and monitor nonlocal cybersecurity maintenance and diagnostic activities;
2. Employ multi-factor authentication that combines at least two mutually independent factors such as challenge/response answers, biometrics, and tokens for nonlocal cybersecurity maintenance and diagnostic sessions to protect the integrity and confidentiality of communications;

3. Maintain records for nonlocal cybersecurity maintenance and diagnostic activities;
4. Terminate session and network connections when nonlocal cybersecurity maintenance is completed;
5. Allow the use of nonlocal cybersecurity maintenance and diagnostic tools and document which tool is being used for which purposes in the information system's security plan.

Cybersecurity Maintenance Personnel
[NIST MA-5]

CIHA shall ensure that all individuals performing hardware or software cybersecurity maintenance on CIHA information systems have the proper access authorizations needed to connect to networks in order to perform cybersecurity maintenance activities.

1. Establish an authorization process for cybersecurity maintenance personnel and maintain a current list of authorized cybersecurity maintenance organizations or personnel;
2. Ensure non-escorted personnel who perform cybersecurity maintenance locally or remotely have appropriate access authorizations to the information system allowing access to CIHA data. Unauthorized access would result in a compromise of confidentiality, integrity, or availability (CIA);
3. Designate personnel who are technically competent and possess the required access authorizations to supervise the cybersecurity maintenance activities of personnel who do not possess those access authorizations.

Timely Cybersecurity Maintenance
[NIST MA-6]

CIHA shall perform preventative cybersecurity maintenance and provide support for purposes of maintaining satisfactory operating conditions for equipment and facilities:

1. Predictive cybersecurity maintenance or condition-based cybersecurity maintenance is performed by periodically or continuously (online) monitoring the condition of equipment;
2. Where technically configurable, use automated mechanisms to transfer predictive cybersecurity maintenance data to a computerized cybersecurity maintenance management system;
3. The timely cybersecurity maintenance control is optional for Low-risk information systems.

Support for Operating Systems:

CIHA shall ensure that the operating systems employed to run the production environment are regularly monitored for security risks and maintained to support business operations. CIHA should consider the following issues when supporting operating systems:

1. New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities;

2. Periodic cybersecurity maintenance improves the performance of operating systems (i.e., hard drive defragmentation);
3. The operating systems on servers, minicomputers, and mainframes usually require daily cybersecurity maintenance tasks and routines that may be either initiated manually as a result of an alert or logged event or scripted to run automatically when a certain threshold or limit is exceeded;
4. Operating system cybersecurity maintenance logs should be reviewed regularly and compared to other system logs to ensure the following:
    a. Cybersecurity maintenance tasks continue to function as expected;
    b. Operating systems continue to operate within accepted thresholds;
    c. System security is not being compromised by cybersecurity maintenance tasks;
    d. Cybersecurity maintenance tasks do not adversely affect computer capacity or performance.

Operating System (OS) Software Upgrades:
OS upgrades shall be carefully planned, executed, and documented as a project. CIHA personnel involved in software upgrades to operating systems shall perform the following steps before commencement of the upgrade project:

1. Document whether system security controls will remain effective or will be modified to appropriately respond to the OS upgrade;
2. Locate change control processes and procedures;
3. Document written agreement of technical personnel and management to acceptance criteria;
4. Document that qualified personnel have certified the upgrade and that the upgrade has passed user acceptance testing;
5. Establish a rollback plan (a set of written steps to undo a release and restore the system to its original state) in the event the upgrade has unacceptable ramifications;
6. An OS failure can have a cascading adverse effect on other systems and possibly even the network;
7. System documentation and business continuity plans should be amended to reflect the OS upgrade;
8. Since OS upgrades typically affect many systems within CIHA, such upgrades should be part of the annual cybersecurity maintenance plan/budget. OS upgrade testing and review cycles should be included in this budget.

Managing System Operations and System Administration:
CIHA systems shall be operated and administered using documented procedures, maintained in a security folder in CIHA's Microsoft Teams repository, that are efficient and effective in protecting CIHA's data.

1. For system transaction records, which include access and audit logs related to the activities of IT systems, CIHA must establish and maintain an adequate system of controls;

2. CIHA shall employ and document controls to provide for the management of system operations and system administration. To minimize the risk of corruption to operating systems or integrated applications, the controls shall include, but are not necessarily limited to, the following:
    a. Develop and document daily operational security procedures;
    b. Assigned personnel shall perform updating of the operating systems and program/application backups;
    c. Operating system software patches shall be applied only after reasonable testing verifies full functionality;
    d. Physical or logical access shall be given to suppliers for support purposes only when necessary and with documented management approval. The suppliers' activities shall be continuously monitored;
    e. Vendor-supplied software used in the operating systems shall be maintained at a level supported by the vendor;
3. CIHA must clearly define the security responsibilities of system administrators who shall protect their assigned IT resources (i.e. hardware, software, etc.) and the information contained on those resources;
4. CIHA must, also, provide appropriate training for those system administrators;
5. System administrators shall do the following:
    a. Ensure that user access rights and privileges are clearly defined, documented, and reviewed for appropriateness;
    b. Consider the risk of exposure when administering system resources (i.e. hardware, software, etc.);
    c. Take reasonable actions to ensure the authorized and acceptable use of (1) data, (2) networks, and (3) communications transiting the system or network.

Scheduling System Operations:

CIHA shall ensure that modifications to information system operations are implemented and maintained properly.

1. Create, implement, and maintain documented operational procedures during system operations and take into consideration the following:
    a. Computer start up, shutdown, and recovery procedures;
    b. Scheduling requirements (length, time frame, etc.);
    c. Processes for handling errors and unforeseen issues that may arise during job execution;
    d. Contact lists;
    e. System restrictions;
    f. Instructions for handling output, including failed jobs;
    g. Proper media handling and storage;
    h. Incident handling and escalation procedures;
    i. Configuration management;
    j. Patch management;
    k. General system hardware and software cybersecurity maintenance;

2. All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy;
3. When special or emergency situations make it necessary to perform cybersecurity maintenance operations outside of the normal system operations schedule, the following must be done:
    - These situations must be documented;
    - Management must be notified;
    - The operation processes used must be recorded;
4. CIHA shall develop change control procedures to accommodate IT resources or events that require changes to be made to system operations;
5. Changes to system baselines require effective communication amongst the CIHA information technology team to ensure that information systems maintain secure operations and avoid lag due to processing consumption and to minimize downtime due to unforeseen problems during such changes;
6. Change control procedures must be documented and followed during the scheduled cybersecurity maintenance windows and take into consideration the following:
    a. Periods of maximum and minimum workflow;
    b. The approval and notification process;
    c. Interfaces with other applications, systems, or processes;
    d. External CIHA interdependencies;
    e. Change categories, risk, and type;
    f. The change request process;
    g. Rollback plans and the point of no return;
    h. Modifications to change control procedures for special or emergency circumstances;
7. All documentation shall be approved by management and reviewed on an annual basis for accuracy and relevancy;
8. Upon the completion of a baseline change, the audit change logs must be retained in accordance with CIHA retention requirements.

Managing and Maintaining Backup Power Generators:

CIHA's business requirements that demand uninterrupted information processing during power outages shall deploy backup power generators. When a backup generator is employed, CIHA shall observe the following requirements:

1. Regularly inspect the generator to ensure it remains compliant with both safety and manufacturer cybersecurity maintenance requirements and has an adequate supply of fuel;
2. Ensure the generator has the capacity to sustain the power load required by supported equipment for a prolonged period of time;
3. Ensure the generator is tested at least monthly according to the manufacturer's specifications;

4. A backup generator is usually combined with an uninterruptible power supply (UPS) to protect critical IT systems that demand high availability. Combinations as such include both:
    - Supporting an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss;
    - Providing continuous business operations if the cutover to the generator is too slow to provide power immediately with no interruption;
5. Contingency plans should include procedures that are to be followed in the event the backup generator fails.

Managing and Using Hardware Documentation:

In order for CIHA to effectively manage information assets, they shall develop and maintain additional documentation that details hardware placement and configuration and provides flowcharts, etc.

1. CIHA shall retain user documentation and technical specifications of IT hardware;
2. Documentation shall be secured from unauthorized use and made readily available to support system cybersecurity maintenance and system support personnel. CIHA shall identify and record its IT hardware assets in a formal hardware inventory/register;
3. CIHA shall develop a process to ensure that IT hardware is identified with unique-to-CIHA physical asset tags and that the inventory/register is kept up to date;
4. The formal hardware inventory should include only information that is available for public inspection.

Maintaining Hardware (On-Site or Off-Site Support):

1. CIHA shall provide or arrange cybersecurity maintenance support for all equipment that is owned, leased, or licensed by CIHA;
2. CIHA must arrange support services through appropriate cybersecurity maintenance agreements or with qualified technical support personnel;
3. When cybersecurity maintenance support is provided by a third party, confidentiality agreements shall be signed by authorized representatives of the third party before any cybersecurity maintenance support is performed;
4. Records of all cybersecurity maintenance activities shall be maintained;
5. To maintain the reliability of databases, cybersecurity maintenance must be performed on the operating system of the system that hosts the databases, or there is a greater possibility that the database itself will fail.

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 MAINTENANCE POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 3/15/2023

Revision Information:

Date	Section Updated	Change
3/15/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
3/15/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA"
3/15/2023	Information Box	Added "Last Reviewed" date
3/15/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
3/15/2023	Purpose	Added "North Carolina State departments, including the NCDIT," "NCDHHS," and "NC Medicaid" as the entities that we must meet compliance requirements with and deleted "NCDHHS/EBCI Tribal Option Contract"
3/15/2023	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
3/15/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"
3/15/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
3/15/2023	Policy	Added that a Maintenance Policy must be implemented and maintained in compliance

		with NIST and State departments and deleted "NCDHHS/EBCI Tribal Option Contract"
3/15/2023	Policy	Amended the title of the "*EBCI Tribal Option Maintenance Policy*" by deleting "EBCI Tribal Option" and replacing it with "CIHA"
3/15/2023	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
3/15/2023	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
3/15/2023	Policy	Added "development, documentation, dissemination, implementation, and maintenance of a maintenance policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Maintenance Policy*
3/15/2023	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"
3/15/2023	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"
3/15/2023	Procedural Guidelines	Updated NIST MA-1: Added the "Internal Controls" section on NIST MA-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
3/15/2023	Procedural Guidelines	Added that "CIHA Maintenance procedures must include the necessary controls" to facilitate the implementation of this Policy
3/15/2023	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
3/15/2023	Procedural Guidelines	Changed "IT security requirements" to "maintenance security procedures" when stating what CIHA will be in accordance with when performing maintenance of operating systems
3/15/2023	Procedural Guidelines	Deleted "EBCI Tribal Option" and added "CIHA" before all instances of "CISO"
3/15/2023	Procedural Guidelines	Changed "nondisclosure statements" to "confidentiality agreements" as the documents that must be signed by authorized representatives of a third party before any maintenance support is performed
3/15/2023	Procedural Guidelines	Deleted "the requirement [about employing automated mechanisms to schedule and conduct the information system security maintenance] that is only applicable for information systems with a High security categorization based on its impact on critical business processes and the sensitivity of the data contained within the system." Deleted the link that defined the security "categorization of High, Medium, or Low"

3/15/2023	Procedural Guidelines	Deleted “if consistent with EBCI Tribal Option policy” in regard to allowing the use of nonlocal maintenance and diagnostic tools
3/15/2023	Procedural Guidelines	Deleted “inappropriate” access and added “unauthorized access instead to reflect that it would result in a compromise of CIA
3/15/2023	Procedural Guidelines	Deleted the title heading for NIST MA-4(2) and its information because NIST MA-4(2) had been withdrawn according to the *NIST Special Publication 800-53 - Security and Privacy Controls for Information Systems and Organizations*
3/15/2023	Procedural Guidelines	Added “and unauthorized” access to “inappropriate access,” which would result in a compromise of CIA
3/15/2023	Procedural Guidelines	Deleted “in approved secure configurations” as a place where operating systems employed to run the production environment are maintained
3/15/2023	Procedural Guidelines	Deleted “EBCI Tribal Option GRC tool” and replaced it with “in a security folder in CIHA’s Microsoft Teams repository” as to where CIHA systems documented procedures are maintained
3/15/2023	Procedural Guidelines	Changed “IT transaction records” to “system transaction records” when discussing documented procedures that protect CIHA’s data systems
3/15/2023	Procedural Guidelines	Deleted the standard “for financial transactions and accounting records,” “addressed by the NC Office of the State Controller” as a documented procedure that operates and administers CIHA systems
3/15/2023	Procedural Guidelines	Changed “EBCI Tribal Option retention standards” to “CIHA retention requirements”

		as audit change logs must be retained in accordance with
3/15/2023	Policy Implementation/ Revision Information	Added policy revision information table
10/19/2023	Policy Title	Added “Cybersecurity” after “CIHA” in the title
10/19/2023	Information Box	Updated “Last Reviewed” date, and added “Policy Owner” and identified the role
10/19/2023	Staff Governed By This Policy	Added “/or” to “CIHA vendors and/or subcontractors”