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 Services Acquisition 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 Services Acquisition 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 Services Acquisition 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 SA 1]

Note SA = Acronym used by NIST for System and Services Acquisition

CIHA shall implement and maintain a Cybersecurity System and Services Acquisition 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 Services Acquisition Policy* shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a system and services acquisition policy and procedural guidelines;
- Assessment, determination, and documentation of information security requirements to adequately allocate all necessary resources;
- Management of information systems using System Development Life Cycle (SDLC) best practices;
- Requirements to be included in all information system acquisitions;
- Requirements for information technology service providers to provide a description of the functional properties of security controls to be employed;
- Requirements for information technology service providers to provide design and implementation information of the security controls employed;
- Requirements for information technology service providers to provide information on security-relevant external system interfaces, high-level design, low-level design, source code and hardware schematics;
- Requirements for information technology service providers to identify early in the SDLC the functions, ports, protocols, and services intended for use by CIHA;
- Assurance that relevant administrator documentation for the information systems, system components, and information systems services is obtained;
- Application of all necessary information system security engineering principles in the

specification, design, development, implementation, and modification of an information system;

- Compliance by external information system services with the CIHA information security requirements and employment of a formal Service Level Agreement (SLA);
- Requirement that providers of external information system services identify the functions, ports, protocols, and other services required for the use of such services;
- Performance of configuration management activities, along with documenting, managing, and controlling the integrity of changes to information systems;
- Performance of relevant testing and evaluation of information systems by external information technology services providers;
- Implementation of a comprehensive, defense-in-depth information security strategy, which protects against supply chain threats;
- Requirement that external information system services follow a documented development process that addresses information security requirements;
- Requirement that external information system services provide adequate training on the correct use and operation of security functions, controls, and mechanisms;
- Requirement that external information system services produce a design specification and security architecture that is consistent with and supportive of the CIHA security architecture.

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.

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 Services Acquisition Policy and Procedural Guidelines

[NIST SA-1]

Internal Controls:

All CIHA information assets must meet the required security controls defined in this Policy that are based on the NIST. This Policy addresses CIHA's requirements, which will be used to implement the system and services acquisition process and the family of system and services acquisition security controls. The system and services acquisition 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 Services Acquisition principles established in NIST, "System and Services Acquisition" control guidelines, as the official standards for this security domain. The "SA" designator identified in each control represents the NIST-specified identifier for the System and Services Acquisition 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 Services Acquisition 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 system and services acquisition 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.

Allocation of Resources

[NIST SA-2]

CIHA shall expediently allocate resources for information security, in order to provide rapid yet supervised allocation, ensuring that the organization is modernized and protected against emerging and ongoing threats. Funding shall include allocation of resources for the initial information system or information system service acquisition and funding for the sustainment of the system/service. CIHA shall accomplish this mission by doing the following:

a. Determine the information security requirements for the information system or service in each mission or business-process planning;
b. Identify, document, and allocate the appropriate amount of resources which are required to protect the information system or service as part of the capital planning and investment control process;
c. Establish discrete line items for information security systems or services within the budgeting process.

System Development Life Cycle

[NIST SA-3]

CIHA shall manage information systems using an SDLC that incorporates information security considerations:

a. Identify qualified individuals having information security roles and responsibilities that are involved in creating the SDLC. This may include the CIHA CIO, CIHA CISO, business owners, system administrators, security architects, security engineers, security analysts, etc. These personnel will ensure that the system life cycle activities meet the information security requirements for the organization;
b. Define and document information security roles and responsibilities throughout the SDLC;
c. Integrate the CIHA information security risk management process into SDLC activities;
d. CIHA shall require a business case justification of custom information system development projects. When proposing the development of custom software, CIHA shall make a strong business case that does the following:
   i. Supports the rationale for not enhancing current systems;

ii. Demonstrates the inadequacies of packaged solutions (software and/or services tailored to achieve a specific scope of work);
iii. Justifies the creation of custom software;

e. The organization shall implement a Change Management program, which enables system engineers, architects, and security analysts to expediently perform their necessary business functions, yet maintain a controlled, secure, and functioning environment. Examples of this program include multi-tiered deployments (Dev, Test, Quality Control, Production), which are capable of backing-up and rolling-back changes which are unsuccessful. Change control requirements are provided in the *CIHA Cybersecurity Configuration Management Policy*;

f. The organization will plan for End-of-Life (EoL) and End-of-Support dates (EoS) for information systems and services; this will ensure that systems and services are capable of receiving security patches and updates throughout the SDLC and that the organization is prepared to discontinue the system or service once no longer supported, or when security cannot be ensured;

g. Many SDLC models exist that can be used by an organization in developing an information system. A traditional SDLC is a linear sequential model. This model assumes that the information system will be delivered near the end of its life cycle. An SDLC should include the following phases:

i. Initiation;
ii. Acquisition / Development;
iii. Implementation / Assessment;
iv. Operations / Maintenance;
v. Sunset (disposition);

h. Each of these five (5) phases should include a minimum set of tasks to incorporate security in the information system development process. Including security early in the SDLC usually results in less expensive and more effective security than retrofitting security into an operational system;

i. The following questions should be addressed in determining the security controls that will be required for an information system:

i. How critical is the information system in meeting the organization's mission;
ii. What are the security objectives required by the system (e.g., CIA);
iii. What regulations, statutes, and policies are applicable in determining what is to be protected;
iv. What are the threats that are applicable in the environment where the system will be operational.

<u>Acquisition Process</u>

[NIST SA-4]

Security functional requirements are a part of the hardware, software, or firmware acquisition process. CIHA shall be capable of acquiring necessary solutions in an expedient manner.

CIHA shall ensure the following:

a. Security functional requirements shall include security capabilities, security functions, and security mechanisms;
b. Security strength requirements based on security categorization (i.e. Low or Moderate) associated with such capabilities, functions, and mechanisms shall include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass;
c. Security assurance requirements shall include the following:
    i. Development processes, procedures, practices, and methodologies;
    ii. Evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved;
d. Requirements for protecting security-related documentation;
e. Description of the information system development environment and environment in which the system is intended to operate;
f. Acceptance criteria requirements (a set of statements, each with a clear pass/fail result, that specify both functional and non-functional requirements) for assessing the ability of an information system component, software, or system to perform its intended function;
g. Proposed vendor hardware design complies with information security and other CIHA policies and standard security and technical specifications, such as the following:
    i. Vendors shall configure the information system with adequate capacity to fulfill the functional requirements stated in CIHA's design document;
    ii. Vendors shall configure hardware security controls to adequately protect data. (Optionally, the vendor may assist CIHA with the configuration of software security controls to provide adequate data protection on the vendor's hardware);
h. Information systems under consideration for acquisition are interoperable with the peripherals and systems currently in use;
i. Mitigation of risks of exploitation of covert channels by obtaining third-party applications from reputable sources and by protecting the source code in custom developed applications;
j. Non-security functional and technical requirements are also part of the hardware, software, or firmware acquisition process;
k. Procurement policies shall be followed when acquiring hardware to ensure that the purchase meets specified functional needs. CIHA shall include specific requirements for performance, reliability, cost, capacity, security, support, and compatibility in Request for Proposals (RFPs) to properly evaluate quotes;
l. Vendor compliance with CIHA security policies must be ensured and a Vendor Readiness Assessment Report (VRAR) from the vendor must be obtained prior to contract approval. This requirement is for both solutions hosted on CIHA infrastructure and those that are not hosted on CIHA infrastructure;
m. New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by CIHA;

n. The developer(s) of the information system, system component, or information system service is required to provide a description of the functional properties of the security controls to be employed. Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. **[Acquisition Process-Functional Properties of Controls NIST SA-4(1)]**;
o. The developer(s) of an information system, system component, or information system service is required to provide design and implementation information for the security controls to be employed that includes the following: security-relevant external system interfaces, high-level design, source code, or hardware schematics. **[Acquisition Process-Design and Implementation Information for Controls NIST SA-4(2)]**;
p. The developer(s) of an information system, system component, or information system service is required to identify early in the SDLC, the functions, ports, protocols, and services intended for CIHA use. **[Acquisition Process-Functions, Ports, Protocols, and Services in Use NIST SA-4(9)]**.

System Documentation

[NIST SA-5]

CIHA must obtain, or document attempts to obtain, administrator and user documentation for the information system, system component, or information system service. CIHA shall distribute such documentation to designated CIHA personnel that describes the following:

a. Secure configuration, installation, and operation of the information system, system component, or information system service;
b. Effective use and maintenance of security functions/mechanisms;
c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
d. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
e. Methods for user interaction, which enable individuals to use the information system, system component, or information system service in a more secure manner;
f. What responsibilities the end user has in maintaining the security of the information system (e.g. password protection, sharing information, etc.);

CIHA shall also do the following:

g. Ensure each new or updated information system includes supporting system documentation and technical specifications of information technology hardware, whether the system is developed or updated by in-house personnel or by a third-party vendor;
h. Create, manage, and secure system documentation libraries or data stores that are always available to only authorized personnel;
i. Ensure that system documentation is readily available to support the personnel responsible for operating, securing, and maintaining new and updated systems;

j. Control system documentation to ensure that it is current and available for purposes such as auditing, troubleshooting, and personnel turnover;
k. All documentation of operational procedures must be approved by CIHA management and reviewed at least annually for accuracy and relevancy.

Security and Privacy Engineering Principles

[NIST SA-8]

CIHA shall apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems. Security engineering principles shall be primarily applied to new development information systems or systems undergoing major upgrades. For legacy systems, internal departments and external organizations shall apply security engineering principles to system upgrades and modifications to the extent that it is technically configurable, given the current state of hardware, software, and firmware within those systems.

a. Security engineering principles shall include the following:
    i. Developing layered protections;
    ii. Establishing sound security policy, architecture, and controls as the foundation for design;
    iii. Incorporating information security requirements into the SDLC;
    iv. Delineating physical and logical security boundaries;
    v. Ensuring that information system developers are trained on how to build secure software;
    vi. Tailoring security controls to meet organizational and operational needs;
    vii. Performing threat modeling (a form of risk assessment that models aspects of the attack and defense sides for selected data within a system) to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;
    viii. Reducing risk to acceptable levels, thus enabling informed risk management decisions;

b. NIST SP 800-27, Revision A *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, shall be used as guidance on engineering principles for information system security. NIST SP 800-27 Revision A may be found at the following link: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27ra.pdf.

External System Services

[NIST SA-9]

a. CIHA shall require that third parties and providers of external information system services comply with CIHA information security requirements and employ to include (at a minimum) security requirements contained in applicable federal laws, executive orders, directives, policies, regulations, standards, and established SLAs;

b. CIHA shall define and document how external information system complies with CIHA information security controls to include user roles and responsibilities and compliance auditing and reporting requirements. CIHA must ensure vendor compliance with CIHA security policies and obtain a VRAR from the vendor prior to contract approval;
c. CIHA shall monitor security control compliance by external service providers on an ongoing basis;
d. CIHA shall restrict the location of information systems that receive, process, store, or transmit state and federal data to areas within the United States territories, embassies, or military installations;
e. CIHA, when outsourcing their information processing, must ensure that the service provider demonstrates compliance with state standards and procedures and industry quality standards;
f. Outsourcing agreements shall include the following:
    i. CIHA's course of action and remedy if the vendor's security controls are inadequate such that the CIA of CIHA's data cannot be assured;
    ii. The vendor's ability to provide an acceptable level of processing and information security during contingencies or disasters;
    iii. The vendor's ability to provide processing in the event of failure(s);
g. To support service delivery, the outsourcing agreements shall contain or incorporate by reference all the relevant information security requirements necessary to ensure compliance with CIHA information security policies and CIHA's record retention schedules, and business continuity requirements;
h. Services, outputs, and products provided by third parties shall be reviewed and checked, at minimum, annually;
i. To monitor third-party deliverables, CIHA shall do the following:
    i. Monitor third-party service performance to ensure service levels meet contract requirements;
    ii. Review reports provided by third parties and arrange regular meetings as required by contract(s);
    iii. Resolve and manage any identified problem areas;
j. Contracts with vendors providing offsite hosting or cloud services must require the vendor to provide CIHA with an annual third-party risk assessment report [Service Organization Controls (SOC) 2 Type II, International Organization for Standardization (ISO) 27001 (and subsequent revisions), Federal Risk and Authorization Management Program (FedRAMP) Moderate] to establish compliance. The assessment shall include, at a minimum, the following:
    i. The rate of compliance with the ISO 27001 (and subsequent revisions) and/or NIST SP-800-53;
    ii. An assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of CIHA funds for information technology security;

iii. Estimation of the cost to implement the security measures needed for CIHA to fully comply with state and federal regulations and industry standards;

k. Any changes to services provided by a third party must be approved by CIHA prior to implementation;

l. CIHA shall develop a process for engaging service providers and maintain a list of all service providers who store or share confidential data;

m. CIHA shall ensure that the SLA includes requirements for regular monitoring, review, and auditing of the service levels and information security requirements as well as incident response and reporting requirements. The SLA shall state how the service provider is responsible for data stored or shared with the provider;

n. CIHA shall perform the monitoring, review, and auditing of services to monitor adherence to the SLA and identify new vulnerabilities that may present unreasonable risk. CIHA shall enforce compliance with the SLA and must be proactive with third parties to mitigate risk to a reasonable level;

o. Changes to an SLA and services provided shall be controlled through formal change management;

p. CIHA must prohibit the use of non-CIHA-owned information systems, system components, or devices that receive, process, store, or transmit Highly Restricted data, including federal tax information (FTI), unless explicitly approved by the Office of Safeguards.

External System Services – Identification of Functions, Ports, Protocols, and Services

[NIST SA-9(2)]

CIHA shall require providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.

Developer Configuration Management

[NIST SA-10]

CIHA shall require the information system developer to create and implement a configuration management plan that does the following:

a. Performs configuration management during information system design, development; implementation, and operation for the following:

   i. Internal system development and system integration of commercial software;

   ii. External system development and system integration;

b. Documents, manages, and controls changes to the information system or configuration items under configuration management;

c. Implements only CIHA-approved changes to the system;

d. Documents approved changes to the system;
e. Tracks security flaws and flaw resolution within the system;
f. Mitigates risks of exploitation of covert channels by protecting the source code in custom developed applications.

Developer Testing and Evaluation

[NIST SA-11]

CIHA shall require the information system developer to test for software faults that pose security risks prior to being deployed into production. CIHA shall do the following:

a. Create and implement a security assessment plan:
    i. Testing requirements must be defined and documented for both information system development and system integration activities. The plan must include requirements for retesting after significant changes occur;
    ii. Perform security testing/evaluation:
        - Restricted or Highly Restricted data shall not be used for testing purposes;
        - CIHA may permit the use of production data during the testing of new systems or systems changes only when no other alternative allows for the validation of the functions and when permitted by other regulations and policies. CIHA shall use data anonymization or data masking tools, if they are available;
        - If production data is used for testing, the same level of security controls required for a production system shall be used;
    iii. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
    iv. Implement a verifiable flaw remediation process;
    v. Correct flaws identified during security testing/evaluation;
b. Teach and encourage software fault-reporting procedures through security training and awareness programs;
c. Designate a quality control team that consistently checks for faults and is responsible for reporting them to software support;
d. Use a formal recording system for the following:
    i. Tracks faults from initial reporting through to resolution;
    ii. Monitors the status of reported faults and confirms that satisfactory resolutions have been achieved;
    iii. Provides reports and metrics for system development and software support management;
    iv. Software faults shall be prioritized and addressed promptly to minimize the exposure resulting from the security vulnerability;
e. While faults are being tracked through to resolution, research shall also be conducted to ensure no security controls have been compromised and resolution activities have been appropriately authorized;
f. Perform unit, integration, and system regression testing/evaluation:

i. Require that information system developers/integrators perform a vulnerability assessment to document vulnerabilities, exploitation potential, and risk mitigations;
ii. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed;
iii. To maintain the integrity of CIHA information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an operational/production environment;
iv. Test data and accounts shall be removed from an application or system prior to being deployed into a production environment if the application or system does not have a dedicated testing environment;
v. Qualified personnel must certify that the upgrade or change has passed acceptance testing;
vi. A rollback plan must be established in the event the upgrade or change has unacceptable ramifications;

g. CIHA shall include the following issues and controls when developing acceptance criteria and acceptance test plans:
i. Capacity requirements - both for performance and for the computer hardware needed;
ii. Error response - recovery and restart procedures and contingency plans;
iii. Routine operating procedures - prepared and tested according to defined CIHA policies;
iv. Security controls - agreed to and put in place;
v. Manual procedures - effective and available where technically configurable and appropriate;
vi. Business continuity - meets the requirements defined in CIHA's business continuity plan;
vii. Impact on production environment - able to demonstrate that installation of new system will not adversely affect CIHA's current production systems (particularly at peak processing times);
viii. Training - of operators, administrators, and users of the new or updated system;
ix. Logs - logs of results shall be kept for a CIHA-defined period once testing is completed;

h. Implement a verifiable flaw remediation process to correct security weaknesses and deficiencies identified during the security testing and evaluation process;

i. Controls that have been determined to be either absent or not operating as intended during security testing/evaluation must be remediated.

Supply Chain Risk Management

[NIST SR Family]

CIHA shall ensure protection against supply chain threats to the information system, system component, or information system service by employing necessary safeguards as part of a comprehensive, defense-in-depth information security strategy.

Development Process, Standards, and Tools

[NIST SA-15]

CIHA shall require that the developer of the information system, system component, or information system service follows a documented development process that addresses information security requirements, identifies the standards and tools used in the development process, documenting the specific tool options and tool configurations used in the development process and documenting, managing, and ensuring the integrity of changes to the process and/or tools used in development. Additionally, CIHA shall review the development process, standards, tools, and tool options/configurations for ensuring satisfaction of all information security requirements.

Developer-Provided Training

[NIST SA-16]

CIHA shall require the developer of the information system, system component, or information system service to provide adequate training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Developer Security and Privacy Architecture and Design

[NIST SA-17]

CIHA is to require the developer of the information system, system component, or information system service to produce a design specification and security architecture that is consistent with and supportive of the organization’s security architecture, along with accurately and completely describing the required security functionality and the allocation of security controls. Additionally, CIHA shall express how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

CIHA CYBERSECURITY SYSTEM AND SERVICES ACQUISITION 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	Amended the Policy's title from "*Systems and Services Acquisition*" to "*System and Services Acquisition*" based on the *NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*
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 Services Acquisition 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,” “implementation,” and “maintenance of a system and services acquisition policy and procedural guidelines” as preventive and timely maintenance activities in the *CIHA Cybersecurity System and Services Acquisition Policy*
8/17/2023	Policy	Added the bullet “Requirement that providers of external information system services identify the functions, ports, protocols, and other services required for the use of such services” to the list of items covered in this 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 SA-1: Added the “Internal Controls” section on NIST SA-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 Services Acquisition 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 deleted “EBCI Tribal Option”

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 SA-1, 4(1), 4(2), 4(9), 5, 8, 9, 9(2), 11, and 17
8/17/2023	Procedural Guidelines	Added the word “information” before “security requirements,” “system developers,” “system,” “system development projects/process,” and “system service”
8/17/2023	Procedural Guidelines	Changed “organization” to “CIHA”
8/17/2023	Procedural Guidelines	SA-3: Item d(ii): Added a layman’s definition for “packaged solutions,” “acceptance criteria requirements,” and “threat modeling”
8/17/2023	Procedural Guidelines	SA-4: Deleted “N.C.G.S. 143B 1350, and any other applicable state or federal laws, directives, policies, regulations, standards, guidelines, and business needs” as CIHA being in accordance with when acquiring necessary solutions in an expedient manner Item f: Added a layman’s definition for “acceptance criteria requirements” Item l: Changed “companywide” to “CIHA”
8/17/2023	Procedural Guidelines	SA-8: Defined that it is “internal departments and external organizations” for legacy systems that shall apply security engineering principles to system upgrades and modification to the extent that it is technically configurable Item a(vii): Added a layman’s definition for “performing threat modeling”

8/17/2023	Procedural Guidelines	SA-9: Item g: Changed CIHA “information security standards” to CIHA “information security policies” when ensuring compliance, the outsourcing agreements shall contain or incorporate by reference all the relevant information security requirements necessary in order to support service delivery Item j(i): Added “(and subsequent revisions)” to ISO 27001 and changed “enterprise-wide security standards” to “ISO 27001 (and subsequent revisions) and/or NIST SP-800-53” as being the rate of compliance with Item j(iii): Added “state and federal regulations and industry” standards as CIHA being fully compliant with when estimating the cost to implement the needed security measures
8/17/2023	Procedural Guidelines	SA-11: Item a: In regard to the CIHA requirement for the information system developer to test for software faults that post security risks prior to being deployed into production, the item: “create and implement a security assessment plan” was deleted
8/17/2023	Policy Implementation/ Revision Information	Added policy revision information table