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 Communications Protection Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 8/17/2023

LAST REVIEWED: 11/20/2025

POLICY OWNER: CIHA Chief Information Security Officer

PURPOSE:

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

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

STAFF GOVERNED BY THIS POLICY:
This Policy applies to all:

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

POLICY:
CIHA shall implement and maintain a Cybersecurity System and Communications Protection Policy in compliance with National Institute of Standards and Technology (NIST) and State departments.

System and Communications Protection Policy and Procedural Guidelines
[NIST SC-1]
Policies and procedures are a critical component of CIHA's system of internal controls, which helps to ensure that all personnel have a clear understanding of roles, responsibilities, acceptable uses, and other important information that relates to system and communications protection in accordance with information security's best practices. As such, policies and procedures relating to the stated criteria herein are to be reviewed and updated annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary to ensure that their overall adequacy and sufficiency meets CIHA's needs.

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

The *CIHA Cybersecurity System and Communications Protection Policy* shall include preventive and timely cybersecurity maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a system and communications protection policy and procedural guidelines;
- Effective application partitioning to separate user functionality from information system management functionality;
- Isolation of security functions from non-security functions;
- Prevention of unauthorized and unintended information transfer via shared system resources;
- Ensuring adequate safeguards are in place for protecting the overall network against denial of service (DoS) attacks and distributed denial of service attacks (DDoS);
- Implementing a managed interface for every external telecommunication service;
- Ensuring information systems monitor and control communications at the external boundary of the system and at key internal boundaries within the system;
- Limiting the number of external network connections;
- Implementation of a Deny by Default/Allow by Exception model to data packets;
- Implementation of fail secure processes, which prevents systems from entering unsecure states in the event of an operational failure of a boundary protection device;
- Isolation of information system components;
- Prevention of split tunneling for remote devices;
- Protecting the CIA of transmitted information;
- Implementation of cryptographic mechanisms or alternate physical protection to prevent unauthorized disclosure of information;
- Ensuring that information systems terminate the network connection for communications sessions at the end of the session or after a defined time of inactivity;
- Establishing and managing cryptographic keys to ensure protection of information during transit;
- Ensuring the information systems prohibit remote activation of collaborative computing devices;
- Definition of signed and unsigned mobile code;
- Establishment of usage restrictions and implementation of Voice over Internet Protocol (VoIP) technologies;
- Ensuring that information systems provide additional data origin authentication and integrity verification artifacts;
- Implementation of secure name/address resolution services;
- Ensuring that name/address resolution services are fault-tolerant and implement internal/external role separation;

- Ensure protection of authenticity of communication sessions;
- Ensure the information stored in information systems "at rest" are protected;
- Ensure that information systems maintain a separate execution domain for each executing process.

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

The CIHA workforce, consistent with *Section 2.01 Applicability* of the CIHA Employee Handbook, includes all designated CIHA direct employees and contractors, volunteers, interns, trainees, students, third parties, non-employees, and others whose conduct, while performing work for CIHA or a business associate or covered entity, is under the direct control of CIHA and/or the business associate or covered entity, regardless of payment status.

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.

Separation of System and User Functionality

[NIST SC-2]

CIHA shall separate user functionality (including user interface services) from information system management functionality in application components.

a. For the application and database secure zones, a CIHA-approved firewall or other network segmentation mechanisms [e.g., micro-segmentation or virtual local area networks (VLANs)] is required to segregate web servers, application servers and database servers;
b. Information systems shall prevent the presentation of information system management-related functionality at an interface for non-privileged users;
c. CIHA's internal network infrastructures [i.e., CIHA local area networks (LANs)] shall be segregated into network zones to protect web servers, application servers, and database servers from the user LAN;
d. Production and non-production environments [e.g., test, development, quality assurance (QA), etc.] shall be segregated;
e. Wireless networks shall be physically and/or logically segregated from internal networks, such that an unknown external user cannot access a CIHA internal network;
f. Systems not able to adhere to the demilitarized zone [(DMZ) a perimeter network that protects and adds extra security to CIHA's local-area network from unauthorized traffic] and/or other security requirements of this Policy need to be in a special assembly zone. CIHA must document the rationale for developing a special assembly zone:
    i. An example of special assembly zones includes facility management systems, such as heating, ventilation, and air conditioning (HVAC), badge access, electrical generators, power distribution, water, and closed-circuit television (CCTV). These may be excluded from the network zoning requirements, provided those systems are not publicly accessible, are logically isolated (i.e., VLANs) from other networked systems and cannot access other shared systems/services, and have appropriate access control mechanisms in place;
g. Where technically configurable, CIHA shall separate virtual machines with Highly Restricted data from those with unrestricted data.

Security Function Isolation

[NIST SC-3]

CIHA must ensure that the information system isolates security functions from non-security functions because such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Security function isolation initiatives must include the provisioning of security kernels (hardware, software, and firmware components), enforcing least privilege in regard to access rights and other essential best practices.

Information in Shared System Resources

[NIST SC-4]

Information systems shall prevent unauthorized and unintended information transfer via shared system resources.

a. Information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) shall not be made available for object reuse nor shall residual information be made available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems;
b. Information systems shall prevent unauthorized information transfer via shared resources in accordance with CIHA information security policies when system processing explicitly switches between different information classification levels or security categories.

Denial-of-Service Protection

[NIST SC-5]

CIHA shall limit the effects of denial of service (DoS) attacks by appropriately securing all hosts that could be a potential target for a DoS or distributed denial of service (DDoS) attack, by doing the following:

a. Denying all inbound traffic by default, thus limiting the channels of network attacks;
b. Periodically scanning network and devices for bots (software robots) and Trojan horse programs;
c. Deploying authentication mechanisms wherever technically configurable;
d. Designing and implementing networks for maximum resiliency;
e. Developing specific plans for responding to DoS and DDoS attacks in the CIHA incident management procedure and the business continuity plan;
f. Managing excess capacity, bandwidth, or other redundancy to limit the effects of information flooding DoS attacks;
g. Providing detection and monitoring capabilities to detect indicators of DoS attacks against CIHA and to determine if sufficient resources exist to prevent effective DoS attacks;
h. Providing additional guidance, which is available in the NIST SP 800-61 *Computer Security Incident Handling Guide*.

Boundary Protection

[NIST SC-7]

CIHA shall do the following:

a. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with CIHA security architecture requirements. Managed interfaces include, for example, gateways, routers, firewalls, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks) **[Boundary Protection-External Telecommunications Services NIST SC-7(4)]**;

b. Establish a traffic flow procedure for each managed interface;
c. Document each exception to the traffic flow procedure with a supporting mission/business need and duration of that need;
d. Review exceptions to the traffic flow procedure annually and remove exceptions that are no longer supported by an explicit mission/business need;
e. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system **[Boundary Protection-Isolation of System Components NIST SC-7(21)]**;
f. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal CIHA networks;
g. Limit the number of external network connections to the information system. Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic **[Boundary Protection-Access Points NIST SC-7(3)]**;
h. Include at minimum the following protective controls:
    i. Positive source and destination Internet Protocol (IP) address checking to restrict rogue networks from manipulating CIHA's routing tables;
    ii. Firewalls must use an authentication mechanism that provides accountability for the individual and to ensure device configuration does not become corrupted with false entries;
    iii. Shield internal network addresses from external view;
    iv. Information systems at managed interfaces shall deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic system policy ensures that only those connections which are essential and approved are allowed **[Boundary Protection-Deny By Default-Allow By Exception NIST SC-7(5)]**;
i. Ensure the information system fails securely (preventing it from entering unsecure states) in the event of an operational failure of a boundary protection device **[Boundary Protection-Fail Secure NIST SC-7(18)]**;
j. Implement network routing controls to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal subnetworks ("subnets");
k. Develop web applications to use a minimum number of secure ports to allow for easy integration in traditional DMZ (DMZ-filtered subnet) environments;
l. Configure firewalls to the following specifications:
    i. Local user accounts shall be configured on network firewalls for the sole purpose of eliminating possible extended outages;
    ii. Local accounts shall be configured to only be used when the device cannot make contact with the central unit. During normal operation, the local account exists but is not used;
    iii. Passwords on firewalls shall be kept in a secure encrypted form, as is required by the *CIHA Cybersecurity Identification and Authentication Policy*;

iv. CIHA shall designate a minimum of two (2) authorized firewall administrators. At least one (1) of the designated firewall administrators will be a security specialist who is consulted before firewall rule set changes are approved and implemented;

v. For temporary or emergency port openings, CIHA process shall establish a maximum time for the port to be open, which shall not exceed five (5) days. CIHA authorized firewall rules set by administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening, reducing its vulnerability and the possibility of being compromised;

vi. System administrators shall configure the firewall so that it cannot be identifiable as such to other network(s) or, at most, appears to be just another router;

vii. Firewalls shall be installed in locations that are physically secure from tampering. Firewalls shall not be relocated without the prior approval of CIHA management;

viii. Firewall rule sets shall always block the following types of network traffic:

- Unauthorized scanning activity that originates outside of its network, within its network, and between information systems;
- Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself;
- Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall;
- Traffic inbound to the CIHA network containing Internet Control Message Protocol (ICMP) traffic will be blocked at the perimeter with the following exceptions: To allow testing initiated from internal IT support groups, ICMP echo replies, and ICMP time-to-live (TTL) expired will be permitted inbound to the CIHA network but will be limited to specific IP addresses or small subnets representing the internal support group. A ping point can be established at the perimeter for troubleshooting purposes, with the sole purpose and sole capability of responding to a ping;
- Inbound network traffic containing IP source routing information;
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0 and/or containing directed broadcast addresses;

ix. Logging features on CIHA network firewalls shall capture all data packets dropped or denied by the firewall, and CIHA personnel or the entity managing the firewall shall review those logs at least weekly;

x. CIHA's firewall rule sets shall be reviewed and verified by CIHA personnel at least quarterly. If an outside entity, manages the firewall, then that entity shall be responsible for reviewing and verifying the CIHA firewall rule sets at least quarterly;

xi. Firewall configurations and associated documentation must be treated as restricted information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel);

m. Ensure that information systems, in conjunction with a remote device, shall prevent the device from simultaneously establishing non-remote connections (i.e., split tunneling) with the system and communicating via some other connection to resources in external networks **[Boundary Protection-Split Tunneling for Remote Devices NIST SC-7(7)]**;

n. Require use of NIST SP 800-41 as guidance on firewalls and firewall rule sets;

o. Require use of NIST SP 800-189 as guidance on routers;

p. Require use of NIST SP 800-77 as guidance on Virtual Private Networks (VPNs);
q. Require use of NIST SP 800-94 as guidance on Intrusion Detection and Prevention Systems (IDPS).

Transmission Confidentiality and Integrity
[NIST SC-8]

CIHA shall protect confidentiality and integrity of transmitted information to ensure that the confidentiality and integrity of the data are maintained during the transfer process by doing the following:

a. Implementing safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling. CIHA must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized CIHA personnel;
b. Implementing network monitoring capabilities to detect and monitor for suspicious network traffic;
c. Deploying controls to ensure that CIHA's resources do not contribute to outside-party attacks. These controls include the following:
    i. Securing interfaces between CIHA-controlled and non-CIHA-controlled or public networks;
    ii. Standardizing authentication mechanisms in place for both users and equipment;
    iii. Controlling users' access to information systems;
    iv. Monitoring for anomalies or known threat signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDPS signatures shall be up to date;
d. Ensuring CIHA network users do not intercept or attempt to intercept data transmissions of any kind that they are not authorized to access;
e. Documenting and retaining on file a case-by-case risk management determination for each type of confidential information as to the appropriateness of its unencrypted transmission to a party not served by CIHA's internal network;
f. Addressing the risk involved in the transfer of different types of data and implement safeguards through the means of exchange used, such as through email, the Internet, or exchange of electronic media;
g. Using secure protocols, such as Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPsec), for secure network management functions;
h. Requiring that all communications that transfer confidential sensitive data between web clients and web servers must employ the most current secure transport protocol that includes the most recent version of TLS;
i. Requiring the use of NIST SP 800-52 as guidance on protecting transmission integrity using TLS;
j. Requiring the use of NIST SP 800-77 as guidance on protecting transmission integrity using IPsec;
k. Requiring the use of NIST SP 800-81 as guidance on Domain Name System (DNS) message authentication and integrity verification;
l. Requiring the use of NIST SP 800-113 as guidance on Secure Sockets Layer (SSL) VPNs;
m. Ensuring that instant messaging technologies, where allowed, must not be used to transmit any type of Restricted or Highly Restricted data;

n. Ensuring that the following types of transmission require enhanced protection (e.g., cryptography mechanisms) when integrity is an important consideration:
    i. Internal traffic within the information system and applications;
    ii. Internal traffic between two (2) or more information systems;
    iii. External traffic to or across the Internet;
    iv. Remote access;
    v. Email;
    vi. File Transfer Protocol (FTP) transmissions;
    vii. Web services;
    viii. VoIP;
    ix. Audio and video;
    x. Wireless client to host communications;
o. Implementing cryptographic mechanisms to prevent unauthorized disclosure of information and/or to detect changes to information during transmission unless otherwise protected by alternative physical safeguards **[Transmission Confidentiality and Integrity-Cryptographic Protection NIST SC-8(1)]**;
p. Protecting the confidentiality of data transmitted on the network from corruption or data loss by prohibiting the extending, modifying, or retransmitting network services, such as through the installation of new switches or other network devices, unless prior CIHA CIO or delegate approval is granted.

Network Disconnect
[NIST SC-10]
CIHA shall do the following:
a. Terminate all sessions that have had no activity for a period of fifteen (15) minutes or less, such that the user must re-authenticate their identity to resume the session;
b. Ensure that an absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the CIHA network;
c. Ensure that the information system must be configured to disconnect inactive remote VPN.

Cryptographic Key Establishment and Management
[NIST SC-12]
CIHA shall ensure electronic key systems are managed according to the following requirements:
a. Use of FIPS 140-3 (and subsequent versions) compliant encryption mechanisms when protecting Restricted or Highly Restricted data. Products and modules that have been validated by NIST as FIPS 140-3 (and subsequent versions) compliant and are currently listed as validated products list and may be found at: http://csrc.nist.gov/groups/STM/cmvp/validation.html;
b. CIHA assets that use key-based data encryption systems must implement a key escrow system to guarantee CIHA access to encrypted data when needed. Key escrow data shall be routinely backed up. Recovery procedures must be tested at least quarterly to ensure CIHA access and availability to encrypted data;

c. Only authorized personnel have access to keys used to access Restricted or Highly Restricted data. Encryption keys must be properly stored (separate from data) and available, if needed, for later decryption. CIHA must also ensure the following:
    i. Separation of duties or dual control procedures are enforced;
    ii. Any theft or loss of electronic keys results in the notification of management;
    iii. All keys are protected against modification, substitution, and destruction, and secret/private keys are protected against unauthorized disclosure;
    iv. Cryptographic keys are replaced or retired when keys have reached the end of their life or the integrity of the key has been weakened or compromised;
    v. Physical protection is employed to protect equipment used to synchronize, store, and archive keys;
    vi. An electronic key management and recovery system, including all relevant key escrow procedures, is documented and in place. This shall be handled through key escrow procedures;
    vii. Custodians of cryptographic keys formally acknowledge they understand and accept their key-custodian responsibilities;
    viii. Encrypted data are recoverable, at any point in time, even when the individual(s) who encrypted the data is no longer available;

d. Only digital certificates either issued by and/or approved by the CIHA CIO can be used to access the CIHA network, applications, and/or systems;

e. NIST SP 800-56A and NIST SP 800-56B must be referenced as procedures on establishing cryptographic keys;

f. NIST SP 800-57 must be referenced as guidance on managing cryptographic keys.

Cryptographic Protection
[NIST SC-13]

CIHA must implement cryptographic modules in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards.

a. CIHA shall document and retain on file a case-by-case risk management determination for each type of Restricted or Highly Restricted data as to the appropriateness of its unencrypted transmission to a party not served by CIHA's internal network;

b. All laptops that are used to conduct CIHA business shall use **full disk encryption** to protect all information stored on the laptop's storage device;

c. All other mobile computing devices and portable computing devices [e.g., smart phones, tablets, and portable storage devices, such as compact disks (CDs), digital video disks (DVDs), media players and flash drives], that are used to conduct CIHA business, shall use encryption to protect all Restricted and Highly Restricted data from unauthorized disclosure;

Device	Encryption Requirements
Laptops, Notebooks, etc.	All devices shall use Full Disk Encryption (FDE) using a FIPS 140-3 (and subsequent versions) Level 1 certified Advanced Encryption Standard (AES)-256 encryption algorithm.
Mobile and portable computing devices, such as tablets and smart phones. Removable media, such as CDs, DVDs, memory sticks (flash drives), electronic media, or any other portable device that stores data.	All Restricted or Highly Restricted data shall be encrypted using a FIPS 140-3 (and subsequent versions) Level 1 certified algorithm of at least a 128-bit strength. Note: Restricted and Highly Restricted CIHA data should only be stored on CIHA-issued and CIHA-owned media.

d. CIHA shall enforce procedures concerning the storage of CIHA's Restricted and Highly Restricted data on all portable and removable media devices;
e. For a list of validated cryptographic modules and products, refer to the following NIST publication: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

Collaborative Computing Devices and Applications
[NIST SC-15]
CIHA shall do the following when using collaborative computing devices:

a. Prohibit remote activation of collaborative computing devices, for example, networked white boards, cameras, and microphones;
b. Provide an explicit indication of use to users physically present at the devices. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Mobile Code
[NIST SC-18]
CIHA shall implement a tamper protection program for the information system, system component, or information system service to protect the CIHA network from mobile code that performs unauthorized and malicious actions. The following are categories of mobile code/active content:

a. Category 1/high risk mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, server, and remote system services and resources. These pose a significant risk to CIHA's information systems because they allow unlimited access to a user's computer. There are two (2) subgroups of Category 1 mobile code technologies:
    i. Category 1 technologies can differentiate between signed and unsigned mobile code. The technologies can also be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. Category 1 mobile code technologies may be used by CIHA when additional restrictions are implemented. The following are assigned to Category 1:
        - ActiveX controls;

- Shockwave movies (e.g., dcr, .dxr, .dir files), including Xtras, that execute in the Shockwave for Director plug-in;

ii. Category 1 consists of mobile code technologies that are prohibited from use on CIHA information systems beyond the local information system's authorization boundary, or to or from external entities because they cannot differentiate between signed and unsigned mobile code, nor can they be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code. The following are assigned to Category 1:
   - Mobile code scripts that execute in Windows Scripting Host (WSH) (e.g., JavaScript or VBScript downloaded via URL file reference or email attachments);
   - Hypertext Markup Language (HTML) applications (e.g., .hta files) that download as mobile code;
   - Scrap objects (e.g., .shs and .shb files);
   - Microsoft Disk Operating System (MS-DOS) batch scripts;
   - UNIX shell scripts;
   - Binary executables (e.g., .exe files) that download as mobile code;

iii. Category 1 mobile code must be obtained from a trusted source and must be signed with a CIHA approved Public Key Infrastructure (PKI) code-signing certificate;

iv. All CIHA information systems capable of executing mobile code must be configured to disable the execution of unsigned Category 1 mobile code obtained from outside the CIHA-managed boundary;

b. Category 2/medium risk mobile code technologies have full functionality, allowing mediated or controlled access to workstations, server, and remote system services and resources. Category 2 technologies can pose a moderate security threat to CIHA's information systems because they offer limited control by the user on what the code is allowed to do. They may be used when the Category 2 restrictions, as described, are implemented;

i. The following are assigned to Category 2:
   - Java applets and other Java mobile code;
   - Visual Basic for Applications (VBA) (e.g., Microsoft Office macros);
   - LotusScript (e.g., Lotus Notes scripts);
   - PerfectScript (e.g., Corel Office macros);
   - Postscript;
   - Mobile code executing in .NET Common Language Runtime;

ii. Category 2 mobile code may be used if it is obtained from a trusted source over an assured channel (i.e., TLS VPN, IPsec, or other approved secure channels);

iii. Unsigned Category 2 code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, or network connections other than to its originating host);

iv. Where technically configurable, Web browsers and other mobile code-enabled products must be configured to prompt the user prior to the execution of Category 2 code;

v. Where technically configurable, protections against malicious Category 2 technologies must be employed at end user systems and at system boundaries;

c. Category 3/low risk mobile code technologies support limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources. Category 3 mobile code may be freely used without restrictions in information systems. Category 3 technologies pose limited risk to CIHA's information systems because they are very restricted in the actions they can perform. The following are assigned to Category 3:

- JavaScript, including Jscript and European Computer Manufacturers Association (ECMA) Script variants, when executing in the browser;
- VBScript, when executing in the browser;
- Portable Document Format (PDF);
- Flash animations (e.g., .swf and .spl files) that execute in the Shockwave Flash plug-in;

d. Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and therefore have not been assigned to one (1) of the three (3) risk categories previously described. Emerging mobile code technologies must not be used unless approved by CIHA management. The download and execution of mobile code using emerging technologies must be blocked by all means available at the network boundary, workstation, host, and within applications.

Voice over Internet Protocol (VoIP)

[NIST SP 800-58]

a. CIHA shall establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously;
b. CIHA shall authorize, monitor, and control the use of VoIP within the information system.

Secure Name/Address Resolution Service (Authoritative Source)

[NIST SC-20]

CIHA information systems shall require the following for DNS:

a. Enable external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service using DNS servers;
b. DNS servers shall not be configured to allow zone transfers to unknown secondary servers:
   i. If CIHA maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers;
   ii. If CIHA maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only.

Secure Name/Address Resolution Service (Recursive or Caching Resolver)
[NIST SC-21]

a. CIHA information systems shall request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources using recursive resolving or caching DNS servers;
b. Recursion on an authoritative name server is prohibited;
c. NIST SP 800-81 must be used as guidance on secure domain name system deployment.

Architecture and Provisioning for Name/Address Resolution Service
[NIST SC-22]

CIHA information systems that collectively provide name/address resolution service for CIHA shall be fault-tolerant and implement internal/external role separation.

a. At least two (2) authoritative DNS servers shall be deployed to eliminate single points of failure and to enhance redundancy. One configured as the primary server and the other configured as the secondary server;
b. Servers shall be deployed in two (2) geographically separated network subnetworks (i.e., not located in the same physical facility);
c. DNS servers with internal roles shall only process name and address resolution requests from within CIHA (i.e., from internal clients);
d. DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet);
e. CIHA shall specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists);
f. Servers must be configured to provide redundancy, load balancing, and distributed access;
g. NIST SP 800-81 must be used as guidance on secure domain name system deployment.

Session Authenticity
[NIST SC-23]
CIHA shall do the following:

a. The information system must protect the authenticity of communications sessions. CIHA shall select and implement protection mechanisms to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission. Mechanisms include, but are not limited to, the following:
    i. Security services based on IPsec;
    ii. VPNs;
    iii. TLS;
    iv. SSL
    v. DNS;
    vi. SSH;
    vii. Digital signatures;
    viii. Digital certificates;
    ix. Digital time stamping;
    x. FIPS 140-3 (and subsequent versions) approved encryption technology;

b. The information system invalidates session identifiers upon user logout or other session termination to curtail the ability of adversaries from capturing and continuing to employ previously valid session IDs;
c. NIST SP 800-52 must be used as guidance on the use of TLS mechanisms;
d. NIST SP 800-77 must be used as guidance on the deployment of IPsec VPNs and other methods of protecting communications sessions;
e. NIST SP 800-95 must be used as guidance on securing web services;
f. NIST SP 800-113 must be used as guidance on SSL VPNs.

Fail in Known State
[NIST SC-24]
CIHA ensures the information system fails to a defined known state for defined failures, thereby preserving information as best as possible.

Protection of Information at Rest
[NIST SC-28]
a. CIHA information systems shall protect the confidentiality and integrity of all Restricted or Highly Restricted data at rest. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems;
b. Restricted and Highly Restricted data stored in non-volatile storage (i.e., disk drive) on all endpoints shall be encrypted with FIPS 140-3 (and subsequent versions) compliant encryption during storage (regardless of location);
c. CIHA shall consider increasing integrity protection of data by recording data onto hardware-enforced, write-once media. Write-once, read-many (WORM) media includes, for example, compact disk-recordable (CD-R) and digital video disk-recordable (DVD-R);
d. CIHA shall also consider storing data at rest on a physically separate non-mobile storage device (e.g., disk drive, electronic media) with cryptographic protections in place;
e. Whereas a virtual machine may store or process confidential data, the virtual machine image file shall use appropriate controls to protect the data at rest.

Process Isolation
[NIST SC-39]
CIHA ensures that the information system maintains a separate execution domain for each executing process.

As such, all CIHA Microsoft Windows systems that are in place support process isolation, as their virtual memory mechanisms essentially require it, and provide mechanisms for inter-process communication (IPC) via shared memory or local/remote sockets.

CIHA CYBERSECURITY SYSTEM AND COMMUNICATIONS PROTECTION POLICY:
POLICY IMPLEMENTATION/REVISION INFORMATION

Original Effective Date: 8/17/2023

Revision Information:

Date	Section Updated	Change
8/17/2023	Policy Header	Replaced "EBCI Tribal Option" with "Cherokee Indian Hospital Authority"
8/17/2023	Policy Title	Deleted "EBCI Tribal Option" from the title of the Policy and replaced it with "CIHA" and added "Cybersecurity" after "CIHA"
8/17/2023	Information Box	Added "Last Reviewed" date and added "Policy Owner" and identified the role
8/17/2023	All sections	Checked and amended grammar, numbering, and readability as needed and replaced all references of "EBCI Tribal Option" with "CIHA"
8/17/2023	Purpose	Added "North Carolina State departments, including NCDIT, NCDHHS, and NC Medicaid" as the entities that we must meet compliance requirements with and deleted "NCDHHS/EBCI Tribal Option Contract"
8/17/2023	Purpose	Changed "EBCI Tribal Option" to "State departments" in the following: In support of the purpose, this Policy has been developed to ensure CIA, privacy, and security of the information assets of CIHA, exceeding "State departments'" compliance requirements
8/17/2023	Purpose	Changed "employees or contractors" to "CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce)"
8/17/2023	Staff Governed By This Policy	Updated the "Staff Governed By" section with the appropriate parties
8/17/2023	Policy	Added that a Cybersecurity System and Communications Protection 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 communications protection policy and procedural guidelines" as preventive and timely maintenance activities in the *CIHA Cybersecurity System and Communications Protection Policy*
8/17/2023	Policy	Amended the preventative and timely maintenance bulleted items to match the information within the 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 SC-1: Added the "Internal Controls" section on NIST SC-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 Communications Protection 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 system and communications protection in accordance with information security's best practices. Added that these policies and procedures are to be reviewed and updated annually
8/17/2023	Procedural Guidelines	Added "NC" to all instance of "DHHS" and changed "State" to "NCDHHS"
8/17/2023	Procedural Guidelines	Amended the following heading titles to reflect those in the *NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*: NIST SC-2, 4, and 15 and added the headings for NIST SC-7(4), 7(21), 7(3), 7(5), 7(18), 7(7), 8(1), and 15 and changed NIST SC-19 to SP 800-58
8/17/2023	Procedural Guidelines	SC-2: Item a: Added "web servers" as an item for the application and database secure zones that a CIHA-approved firewall or other network segmentation mechanisms is required to segregate Item c: Added that "web servers" and "database servers" as items that will be protected from the user LAN through internal network infrastructures segregating them into network zones

		Item e: Added “and” to “Wireless networks shall be physically and/or logically segregated from internal networks” Item f: Provided a layman’s definition for DMZ and Changed “or” to “and” in “An example of special assembly zones includes facility management systems, such as heating, ventilation, and HVAC…”
8/17/2023	Procedural Guidelines	SC-3: Added examples of “security kernels” as “(hardware, software, and firmware components)”
8/17/2023	Procedural Guidelines	SC-4: Item b: Changed “companywide information security standards” to “CIHA information security policies”
8/17/2023	Procedural Guidelines	SC-5: Changed “incident management plan” to “CIHA incident management procedure”
8/17/2023	Procedural Guidelines	SC-7: Item a: Changed “companywide” to “CIHA” Items b, c, and d: Changed instances of “policy” to “procedure” Item h(i): Added “IP” to “Positive source and destination IP address checking to restrict rogue networks from manipulating CIHA’s routing tables Item h(iii): Changed “Screen” to “Shield” internal network addresses from external view Item i: Added “(preventing it from entering unsecure states)” as to why to ensure the information system fails securely Item k: Added “secure” to “Develop web applications to use a minimum number of secure ports to allow for easy integration in traditional DMZ environments” Item l(v): Added the explanation of what “CIHA authorized firewall rules set by administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening” does by adding “reducing its vulnerability and the possibility of being compromised” Item l(ix): Added “data” to better identify “packets” and changed “monthly” to “weekly” for the cadence of reviewing network firewalls logs Item l(xi): Deleted this line item, which was “Additional requirements for protecting FTI on networks are provided in IRS 1075 Section 9.4.10, Network Protections”
8/17/2023	Procedural Guidelines	SC-8: Item a: Deleted “(NC Electrical Code, Chapter8, Article 830) as a reference because it does not apply to CIHA in regard to network cabling and unauthorized interception of data transmissions Item c(iii): Changed “resources” to “systems” in “Controlling users’ access to information systems” Item c(iv): Added “threat” to “Monitoring for anomalies or known threat signatures” Item f: Deleted “exchange of tapes” as a means to transfer different types of data and implement safeguards through the means of exchange used Item p: Changed “CIHA CISO” to “CIHA CIO” as the role who grants prior approval for actions such as the installation of new switches, other network devices, etc.
8/17/2023	Procedural Guidelines	SC-10: Item a: Changed the time frame from when CIHA terminates all sessions that have had no activity for a period of “30 minutes” to “15 minutes” or less
8/17/2023	Procedural Guidelines	SC-12: Item a: Changed all instances of “FIPS 140-2” to “FIPS 140-3 (and subsequent versions)” Item b: Changed “annually” to “quarterly” as the cadence of testing recovery procedures Item d: Changed “Certification Authority” to “CIHA CIO” as the role that digital certificates are either issued by and/or approved by to access the CIHA network, applications, and/or systems
8/17/2023	Procedural Guidelines	SC-13: Item c: Deleted “MP3 players” as an example of a portable storage device because they are antiquated and mostly defunct and deleted “personal digital assistants” as an example of a mobile and portable computing devices because it is antiquated and mostly defunct and changed “tape media” to “electronic media” as an example of removable media
8/17/2023	Procedural Guidelines	SC-18: Item b(ii): Deleted “by NCDHHS” and added or other approved “secure channels” as an id est for “Category 2 mobile code may be used if it is obtained from a trusted source over an assured channel
8/17/2023	Procedural Guidelines	SP 800-58: Item b: Deleted the sentence because it is not applicable to CIHA, “Additional requirements for protecting FTI transmitted by VoIP systems are provided in Section 9.4.15, VoIP Systems of IRS 1075”
8/17/2023	Procedural Guidelines	SC-20: Item b(iii): Deleted this item because it is not applicable to CIHA, “When a domain has a US extension, the US Domain Registry requires the domain allow copies to be transferred to the US Domain Registry’s Master Server.

		Therefore, all domains registered with US Domain Registry will allow transfers of copies of their zones to the Master Server for the US Domain Registry"
8/17/2023	Procedural Guidelines	SC-23: Item a(iv): Identified and added "SSL" as a protection mechanism that ensures adequate protection of data integrity, confidentiality, and session authenticity in transmission
8/17/2023	Procedural Guidelines	SC-28: Item d: Changed "tape drive" to "electronic media" as an example of a non-mobile storage device
8/17/2023	Policy Implementation/ Revision Information	Added policy revision information table
9/20/2024	Policy	Added "cybersecurity" before "maintenance" to provide further clarification for readers
9/20/2024	Policy and Procedural Guidelines	Moved NIST SC-1 language from the Procedural Guidelines section and combined it with the NIST SC-1 language in the Policy section
11/20/2025	Policy Header	Updated CIHA seal
11/20/2025	Definitions	Amended the CIHA Workforce definition