# 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 Access Control Policy**

**REVIEWED AND APPROVED BY: CIHA Executive Committee**

**EFFECTIVE DATE: 2/15/2023**

**LAST REVIEWED: 2/15/2023**

**PURPOSE:**

To provide a security framework that ensures the protection of the Cherokee Indian Hospital Authority (CIHA) information 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 *Access Control 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 or subcontractors, who process, store, transmit, and have connectivity to the Information Technology (IT) infrastructure.

**POLICY:**
**[NIST AC-1]**
**Note AC = Acronym Used by NIST for Access Control**
CIHA shall implement and maintain an Access Control 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 Access Control Policy* shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of an access control policy and procedural guidelines;
- Management of accounts regarding access control to ensure only authorized users gain access to CIHA information systems;
- Identification and selection of information system accounts;
- Information systems enforcement of role-based access control;
- Information flow enforcement through deployment of mechanisms to control access;
- Separation of duties for access control, which helps mitigate conflicts of interest regarding access to CIHA information systems;
- Implementation of access rights for which permissions to perform certain operations are assigned to specific roles, and the concept of "least privilege" is to provide a user account with only those privileges, which are essential to that user's work;
- Authentication of parameters are set to require that a user's account be locked out upon the third invalid log-on attempt;
- Appearance of an approved system use notification message appears once users have been granted access to certain information systems;
- Concurrent session controls to define the maximum number of simultaneous sessions per user when accessing information systems;

- Termination of a session terminates all processes associated with a user's logical session, except those processes that are specifically created by the user to continue after the session is terminated;
- Instances of permitted actions without identification or authentication for ensuring the safety and security of CIHA's information systems;
- Remote access consisting of communication protocols and other supporting devices that ultimately ensure CIA of such connections, along with the organization's network;
- Wireless access consisting of communication protocols and other supporting devices that ultimately ensure CIA of wireless connections and the organization's network, requiring the use of secure connectivity protocols;
- Use and application of mobile devices that consist of communication protocols and other supporting devices that ultimately ensure the CIA of such devices and the information being stored, processed, or transmitted on them;
- Use of external systems that are outside of the authorization boundary;
- Sharing of information with a sharing partner;
- Publicly accessible content.

**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.

**Access Control Policy and Procedural Guidelines**

**[NIST AC-1]**

Internal Controls:

All CIHA information assets must meet the required security controls defined in this Policy that are based on NIST. This Policy addresses CIHA's requirements, which will be used to implement the access control process and the family of access control security controls. The access control 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 Access Control principles established in NIST, "Access Control" control guidelines, as the official standards for this security domain. The "AC" designator identified in each control represents the NIST-specified identifier for the Access Control control family. NIST outlines the Access Control requirements that CIHA must implement and maintain in order to be compliant with this Policy.

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:

i. This Policy to address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
ii. The Access Control procedures must 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 access control 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.

## Account Management

**[NIST AC-2]**

Management recognizes the vital importance of proper account management in regards to access control, which ultimately ensures that only authorized users gain access to CIHA information systems, ensuring the safety and security of organizational assets. Authorized personnel within CIHA are therefore responsible for a wide range of account management initiatives, beginning with supporting and properly identifying and documenting the relevant information system account to ensuring users are removed from account access as needed. As such, CIHA's account management initiatives consist of the following:

a. Identifies and selects the following types of information system accounts to support organizational mission essential functions (MEFs)/critical business functions:
    i. Individual;
    ii. Group;
    iii. System;
    iv. Application;
    v. Guest/Anonymous;
    vi. Temporary;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by managers and/or system owners for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with documented CIHA account management procedures;
g. Monitors the use of information system accounts;
h. Notifies account managers:
    i. When accounts are no longer required;
    ii. When users are terminated or transferred; and
    iii. When individual information system usage or need-to-know access changes;
i. Authorizes access to the information system based on:
    i. A valid access authorization;
    ii. Intended system usage; and
    iii. Other attributes as required by CIHA or associated MEFs/critical business functions;

j. Reviews user accounts quarterly, at minimum, and semi-annually for privileged accounts/roles to comply with account management requirements;
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

**Account Management – Automated System Account Management**
**[NIST AC-2(1)]**
Effective management of information system accounts includes the use of automated mechanisms for ensuring that all aspects of the access control lifecycle for users are monitored at all times from initial provisioning to subsequent de-provisioning of users. This monitoring ultimately helps to ensure the safety and security of CIHA information systems.

The following automated mechanisms are used by CIHA:

- **Email**
  Used for communicating and documenting all necessary activities within the access control lifecycle;
- **Telephone**
  Used for communicating all necessary activities within the access control lifecycle;
- **Internal Monitoring Systems Within the Directory Services**
  These systems effectively allow for the real-time monitoring of accounts, along with providing detailed information as to the account types, access rights afforded users, and other essential information.

**Account Management – Automated Temporary and Emergency Account Management**
**[NIST AC-2(2)]**
Both temporary and emergency accounts will be disabled immediately after no longer needed. Such accounts are often initiated for specific conditions; therefore, access to these accounts is revoked after the mandated time period, along with the removal of the accounts. In some cases, an emergency or break glass type account is meant to be used only once for a maintenance or recovery function. For these cases, the password is reset after use, so the account can be used again if needed.

**Account Management – Disable Accounts**
**[NIST AC-2(3)]**
User credentials that are inactive for a maximum of ninety (90) days are disabled, except as specifically exempted by a security administrator. All accounts that have been disabled for greater than three hundred sixty-five (365) days are deleted.

**Account Management – Automated Audit Actions**

**[NIST AC-2(4)]**

CIHA information systems automatically audit account creation, modification, and enabling, disabling, and removal actions, and document these changes in the IT provided ticketing system.

**Account Management – Inactivity Logout**

**[NIST AC-2(5)]**

CIHA requires that users and systems log out or lock their system(s) when inactive for fifteen (15) minutes.

**Account Management – Account Monitoring For Atypical Usage**

**[NIST AC-2(12)]**

CIHA monitors information system accounts for atypical use and reports atypical usage of information system accounts to the information security group including the CIHA CISO.

**Account Management – Disable Accounts for High-Risk Individuals**

**[NIST AC-2(13)]**

CIHA immediately disables accounts of users posing a significant risk to CIHA operations, data, and infrastructure upon initial discovery of the risk.

## Access Enforcement

**[NIST AC-3]**

CIHA information systems enforce a role-based access control policy over defined subjects and objects, as well as control access to the data based upon valid access authorization, intended system usage, and the authority to disclose data.

## Information Flow Enforcement

**[NIST AC-4]**

CIHA deploys mechanisms to control access to its network backbone and/or routed infrastructure. The CIHA network is configured to monitor and control communications at the external boundary of the network and internal boundaries at strategic locations.

The network only connects to external networks or information systems through managed interfaces, consisting of boundary protection devices (e.g., proxies, gateways, routers, firewalls, encrypted tunnels, web content filters, and data loss prevention) arranged in accordance with effective security architecture.

## Separation of Duties

**[NIST AC-5]**

Separation of duties is an essential initiative for access control as it helps ensure that conflicts of interest regarding access to CIHA information systems are mitigated to the fullest extent.

Effective separation of duties consists of implementing access control policies that provide varying access rights based on a user's needs. CIHA has implemented measures during the initial provisioning process for ensuring that users granted access rights to information systems do not result in a segregation of duty conflict.

Effective separation of duties consists of users of information systems having clear roles and responsibilities for various initiatives throughout the organization, which do not overlap with other responsibilities provided to other users. Examples include, but are not limited to, the following:

- Separating duties, where allowable, relating to network engineering for firewalls, routers, switches, and other network related devices;
- Separating duties, where allowable, relating to system administration of servers and other related information systems;
- Separating duties, where allowable, between development, staging, and production environments.

## Least Privilege

**[NIST AC-6]**

The concept of "least privilege," is known collectively as that of "least access," "need to know" access, or Role Based Access Control (RBAC). CIHA has implemented access rights for which permissions to perform certain operations are assigned to specific roles, resulting in users acquiring the permissions to perform particular functions on information systems within the organization. Therefore, privileges to these particular information systems are never to be assigned based on a specific employee's demands, requests, or preferences.

The principle purpose of the "least privilege" concept is to provide a user account with only those privileges, which are essential to that user's work. Thus, when applied to users, the terms "least user access" or "least- privileged user account" are also utilized. At all times, all user accounts should run with as few privileges as possible.

### Least Privilege – Authorize Access to Security Functions

**[NIST AC-6(1)]**

CIHA explicitly authorizes access to confidential information.

### Least Privilege – Non-Privileged Access for Nonsecurity Functions

**[NIST AC-6(2)]**

CIHA requires that users of information system accounts or roles with access to confidential information use non-privileged accounts or roles when accessing nonsecurity functions.

**Least Privilege – Network Access to Privileged Commands**

**[NIST AC-6(3)]**

CIHA authorizes network access to confidential information that is only used for organization-defined operational needs and documents the rationale for such access in the security plan for the information system.

**Least Privilege – Privileged Accounts**

**[NIST AC-6(5)]**

CIHA restricts privileged accounts on the information system to specific, organization-defined personnel or roles.

**Least Privilege – Log Use of Privileged Function**

**[NIST AC-6(9)]**

CIHA audits or reviews logs for the execution of privileged functions.

**Least Privilege – Prohibit Non-Privileged Users from Executing Privileged Functions**

**[NIST AC- 6(10)]**

CIHA prevents non-privileged users from executing privileged functions, which include disabling, circumventing, or altering implemented security safeguards/countermeasures.

**Unsuccessful Logon Attempts [NIST AC-7]**

Authentication parameters are set to require that a user's account be locked out upon the third invalid log-on attempt.

- The information system:
  i. Enforces a limit of minimum three (3) consecutive invalid log-on attempts by a user during a one hundred twenty (120)-minute period;
  ii. Automatically locks the account/node for a minimum of thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. The time the account/node is locked can be shortened if the end user successfully unlocks the account through a challenge question scenario, or a system administrator, security administrator, or an authorized help desk personnel member re-enables the user's account;
- Password parameters are set to require that once a user's account is locked out, it remains locked for a minimum of thirty (30) minutes or until a system administrator, security administrator, or authorized help desk personnel resets the account. Additionally, the session lock shows a system generated publicly viewable image (one that is deemed acceptable) once the system goes into lock mode.

**System Use Notification**
**[NIST AC-8]**

Once users have been granted access to certain information systems, an approved system use notification message appears on the screen, which users must read and acknowledge before receiving access. Because of the numerous information systems currently in place at CIHA, system use notifications will be tailored, as necessary, to the applicable environments for which users are being granted access to.

The minimum system use notification requirements for all systems are to include the following notifications and general information:

- A description of the type of information systems that are being accessed;
- Users are subject to system monitoring, recording, and auditing of all activity, if applicable;
- Unauthorized use of the accessed information systems is prohibited and subject to criminal and civil penalties.

For publicly accessible systems, the minimum use notification requirements are to include the following notifications and general information:

- System use information discussing specific conditions before granting further access;
- When accessing such systems, the user is subject to system monitoring, recording, and auditing of all activity, if applicable;
- A description of the authorized uses of the system.

Depending on operating system and browsers accessed via the Internet, the format of the system use notification will appear in banner format and may vary in size and depth.

**CIHA Information Systems:**

a. Display to users a system use notification message (provided in the next section of this Policy) before granting access to the system that provides privacy and security notices consistent with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance and state that:
    i. Users are accessing a secure information system;
    ii. Information system usage may be monitored, recorded, and subject to audit;
    iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties;
    iv. Use of the information system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on or further access the information system;

c. For publicly accessible systems:
    i. Display system use information before granting further access;
    ii. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;
    iii. Include a description of the authorized uses of the system.

**Current CIHA Notice and Consent Banner:**

CIHA has the right to monitor and access all aspects of the information systems, if deemed necessary, including an employee's email and Internet access to ensure compliance with Sec. 4.13. Use of phone, mail and office systems of the *CIHA Personnel Manual.* All applicable workforce is provided with a computer and a computer account to assist with the expected job performance. All workforce should not expect personal privacy in regard to anything created, sent, received, or downloaded on a CIHA information system by the employee.

The information systems belong to CIHA and should be used for business purposes only. CIHA reserves the right to monitor the operation of these systems, to access all records within them, and to retain or dispose of those records, as deemed necessary.

All messages created, stored, sent, or received by any member of the workforce shall remain the property of CIHA, regardless of if any member of the workforce uses a personal password or code to access information systems.

CIHA reserves the right to monitor its network for any user misconduct, abuse and misuse, or any type of insider threat activity. If any of the aforementioned activities are detected, CIHA may use digital forensics to capture data to present as evidence in a court of law.

## Concurrent Session Control

**[NIST AC-10]**

Concurrent session control allows CIHA to define the maximum number of simultaneous sessions per user when accessing information systems. Although each user has a respective account, restricting the number of concurrent sessions ensures that multiple users can no longer share an individual's user account. The goal of CIHA's concurrent session control initiative is to ensure the safety and security of information systems while allowing flexibility regarding necessary access to such systems.

## Session Termination

**[NIST AC-12]**

A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session

termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. When accessing CIHA information systems, session terminations will be invoked for the following reasons:

- Session inactivity by a user;
- Time-of-day restrictions;
- Information systems configured to terminate a session because of any perceived or actual breach that could impact the CIA of CIHA information systems;
- The information system automatically terminates a user session after thirty (30) minutes of inactivity. For certain higher risk information systems, the requirement for a session idle timeout may be more stringent as determined by CIHA policy, industry standard, or other regulations.

**Permitted Actions Without Identification or Authentication**

**[NIST AC-14]**

Identification and authentication serve as one of the underlying best practices for ensuring the safety and security of CIHA's information systems, and such measures will be utilized at all times. However, there are instances for which such measures may be bypassed, which consist of the following when accessing:

- Information made available on public web servers, such as URL addresses that can be accessed by the general public;
- Marketing material, such as brochures, press releases, press statements, pamphlets, newsletters, etc.;
- Public records, such as court orders and rulings, local, state, and federal filings [U.S. Securities and Exchange Commission (SEC) filings, incorporation filings, etc.];
- Any other data and information for which actions can occur without invoking identification or authentication measures as determined by CIHA.

**Remote Access**

**[NIST AC-17]**

Remote access consists of communication protocols and other supporting devices that ultimately ensure the CIA of such connections, along with the organization's network. This is achieved by using secure connectivity methods that utilize appropriate levels of encryption, such as Secure Sockets Layer (SSL) and Internet Protocol Security Virtual Private Network (IPsec VPN) tunneling and other approved methods. Remote access platforms that do not meet these minimum requirements are strictly forbidden.

The use of remote access is a privilege assigned only to authorized individuals with a justified business need for such access and only after comprehensive analysis and subsequent approval procedures have been undertaken by applicable supervisory personnel and all necessary IT authorities.

Remote access configuration and connection requirements do not allow remote access client software – if residing on a user's device – to be altered in any way. Additionally, users are not to initiate remote access sessions from untrusted end-user devices that are not owned, operated, maintained, and controlled by CIHA or pose a credible security threat. Common examples include the following: mall kiosks that offer Internet services, hotel business/computer rooms offering PCs for use, office supply/mailing stores providing computers for printing, faxing, scanning services, etc.

Users are forbidden from engaging in dual connectivity/concurrent connectivity, whereby a user is connected to the CIHA network while also connected to another network. Furthermore, this demonstrates why it is necessary to implement MFA to gain remote access.

Remote access is a privilege, whereby all authorized users are only permitted to utilize services for business use only, performing no personal or questionable activities. "Business use only" implies the following:

- Facilitating all required duties for a stated job function;
- Communicating with other authorized parties (e.g., employees, providers, patients, contractors, etc.);
- Conducting research applicable to one's job duties. Data and information accessed are often highly sensitive and confidential, requiring due professional care at all times, which means no "comingling" with personal activities that could jeopardize the safety and security of CIHA assets.

**Remote Access – Monitoring and Control**

**[NIST AC-17(1)]**

The information system monitors and controls remote access using automated monitoring tools.

**Remote Access – Protection of Confidentiality and Integrity Using Encryption**

**[NIST AC-17(2)]**

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

**Remote Access – Managed Access Control Points**

**[NIST AC-17(3)]**

CIHA's information system routes all remote accesses through managed network access control points. Limiting the number of access control points for remote accesses reduces the likelihood of a cyberattack on CIHA.

**Remote Access – Privileged Commands and Access**

**[NIST AC-17(4)]**

CIHA authorizes the execution of privileged commands and access to security-relevant information via remote access only for business use, as well as documents the rationale for

such access in the security plan for the information system.

**Wireless Access**

**[NIST AC-18]**

Wireless access consists of communication protocols and other supporting devices that ultimately ensure the CIA of wireless connections and the organization's network, requiring the use of secure connectivity protocols. Wireless access platforms that do not meet these minimum requirements are strictly forbidden.

Configuration and connection requirements for wireless access require an assessment of operational, performance, security, and any applicable legal/regulatory issues. Additionally, wireless access platforms will be provisioned and hardened accordingly, which includes changing basic default settings on all wireless devices, removing unnecessary and insecure services, utilizing the strongest encryption algorithm available, and other necessary security best practices.

Administrative access rights to CIHA wireless platforms are limited to authorized personnel only, such as systems administrators, network engineers, and other individuals responsible for the overall design, configuration, implementation, maintenance, and monitoring of wireless access points. End user access rights include all employees and other applicable third parties as designated by CIHA.

Additionally, all workforce access must include a log-in session where certain information is requested, such as a password for the wireless Service Set Identifier (SSID) that is being broadcasted. CIHA currently uses Wi-Fi Protected Access 2 (WPA2) with strong pre-shared keys.

**Wireless Access – Authentication and Encryption**

**[NIST AC-18(1)]**

The information system protects wireless access to the system using authentication of users and devices with FIPS-140-2 (and subsequent versions) compliant encryption.

**Wireless Access – Restrict Configurations by Users [NIST AC- 18(4)]**

CIHA identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

**Wireless Access – Antennas and Transmission Power Levels**

**[NIST AC-18(5)]**

CIHA selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

## Access Control for Mobile Devices

**[NIST AC-19]**

The use and application of mobile devices consists of communication protocols and other supporting devices that ultimately ensure the CIA of such devices and the information being stored, processed, or transmitted on them.

All mobile devices used for sending, receiving, and storing information are to have encryption enabled at all times. Because it is quite common to lose, have stolen, or misplace a mobile device, sensitive CIHA and client information is never to be stored on such devices without proper approval, and if approval is granted, the data must be encrypted at rest for adequate protection mechanisms.

These devices must contain features for entering certain credentials (e.g., usernames, passwords, biometrics, etc.), allowing them to be used by authorized personnel. Lost, stolen, or misplaced devices can immediately be accessed by unauthorized parties without such security provisions in place. Additionally, mobile devices must be configured in accordance with CIHA password parameters and must store all user-saved passwords in an encrypted password format for ensuring their CIA.

Moreover, administrative access rights to CIHA mobile devices are limited to authorized personnel only, such as systems administrators, network engineers, and other individuals responsible for the overall design, configuration, implementation, maintenance, and monitoring of mobile devices. End user access rights include all employees and other applicable third parties as designated by CIHA. All access must include a username and password to help prevent unauthorized access to CIHA mobile devices.

Users of mobile devices are fully expected to have a satisfactory understanding of the use and application of such devices. If users feel they do not have adequate knowledge for using such devices, they must seek immediate assistance. Educating oneself via an accompanying training manual and/or requesting additional training from an internal resource at CIHA or an external resource, such as an online training video or a consultant who can provide greater understanding of one's mobile device, making it a more safe and secure device.

CIHA establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for CIHA-controlled mobile devices. CIHA authorizes the connection of mobile devices to CIHA information systems with manager approval.

### Access Control for Mobile Devices – Full Device or Container-Based Encryption

**[NIST AC-19(5)]**

CIHA employs encryption to protect the confidentiality and integrity of information on mobile devices, which is achieved by the following:

a. Establishing usage restrictions, configuration requirements, connection requirements, and implementation guidance for CIHA-controlled mobile devices;
b. Authorizing the connection of mobile devices to CIHA information systems with manager approval.

CIHA personal mobile devices (e.g., cell phones) only have access to the CIHA exchange web services but no direct access to the production network.

## Use of External Systems

**[NIST AC-20]**

External information systems are information systems or components of information systems that are outside of the authorization boundary. These are established by organizations typically having no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. As such, the term "external information systems," consists of the following systems and environments used to implement security measures for CIHA:

**Home Computing:**

Many employees work from home, which means they store, process, and transmit sensitive and confidential CIHA information over their personal networks, which can pose significant security risks, as home networks are clearly within the scope of "external information systems." As such, when accessing CIHA information systems, employees must adhere to the following best practices:

- Use endpoint protection (i.e., antivirus software);
- Use strong passwords;
- Use a personal firewall;
- Be cautious online;
- Change SSID;
- Enable message authentication code (MAC) filtering;
- Change default wireless access to router;
- Do not allow household members to use CIHA systems.

**Personally Owned Information Systems/Devices:**

Securing personally owned information systems/devices [e.g., notebooks, smart phones, tablets, etc.] at all times is extremely critical, and it requires comprehensive measures regarding its physical security, while also protecting all electronic data residing on it. From travelling for meetings to connecting to open public wireless access points, personally owned information systems/devices are a constant source of target, so beware. Take the following precautions for securing these most important possessions:

- Use encryption tool;
- Use endpoint protection (i.e., antivirus software);
- Turn on firewall;

- Use strong passwords;
- Secure it physically;
- Keep a watchful eye.

**Privately-Owned Computing Devices Residing in Commercial Facilities:**

Ensuring the safety and security of privately owned computing devices (i.e., also known as personally owned information systems/devices) in commercial facilities requires great care in regard to one's environment. Do not leave a laptop, tablet, etc. unattended for any amount of time. For example, it is not wise to leave a privately owned laptop unsupervised while going to the bathroom in a coffee house. For a CIHA owned laptop, verify with the IT department that the serial number has been recorded, and for a personal laptop, personally record the serial number.

**Use of External Systems – Limits on Authorized Use**

**[NIST AC-20(1)]**

CIHA only permits authorized individuals to use an external information system to access the CIHA information system or to process, store, or transmit CIHA-controlled information when CIHA:

a. Verifies the implementation of required security controls on the external system as specified in CIHA's information security policy and security plan; or
b. Retains approved information system connection or processing agreements with CIHA hosting the external information system.

**Use of External Systems – Portable Storage Devices – Restricted Use**

**[NIST AC-20(2)]**

CIHA restricts the use of CIHA-controlled portable storage devices by authorized individuals on external facing information systems. Refer to the *CIHA Media Protection Policy*.

## Information Sharing

**[NIST AC-21]**

Sharing information with a sharing partner requires CIHA to implement comprehensive access rights for ensuring the safety and security of information systems. A sharing partner can be defined as either:

- An internal individual, group, or departmental level within CIHA or an entity that is associated with CIHA, legally and/or administratively; or
- An external individual, group, organizational level, or entity that has a legitimate business need for accessing CIHA information systems. As such, information sharing with a sharing partner requires the following:
  - A formalized and documented business justification as to the reason for

allowing information sharing for any internal and/or external individual, group, or entity, as well as identifying which systems. This information is kept on file in the applicable department, as necessary:

- For internal information sharing requirements, the documentation can be kept on file with Human Resources, IT, or any other department at CIHA, as needed;

- For external information sharing, such documentation should be encompassed into all legal documents for such providers, such as contractual material, Statements of Work (SOW), Master Services Agreements (MSAs), Service-Level Agreements (SLAs), etc. Adherence to all applicable CIHA access control policies, procedures, and processes by both internal and external sharing individuals, groups, or entities is a requirement to help ensure the CIA of CIHA information systems.

**Publicly Accessible Content**

**[NIST AC-22]**

CIHA's CISO ensures that business owners do the following:

a. Authorize designated individuals to post information on to publicly accessible information systems;
b. Train designated individuals to ensure that publicly accessible information does not contain non-public information;
c. Review the proposed content of publicly accessible information to ensure non-public information is not included prior to posting onto the information system;
d. Review content on the publicly accessible information system for non-public information, and if discovered, remove any such information;
e. Review content quarterly at a minimum for the identification and removal of non-public data.