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 Identification and Authentication Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 4/18/2023

LAST REVIEWED: 4/18/2023

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Identification and Authentication 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 *Identification and Authentication Policy* has been developed to ensure the confidentiality, integrity, availability (CIA), privacy, and security of the information

assets of CIHA through the establishment of safeguards to prevent theft, abuse, and misuse while exceeding State departments' compliance requirements.

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

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

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

POLICY:
[NIST IA -1]
Note IA = Acronym used by NIST for Identification and Authentication
CIHA shall implement and maintain an Identification and Authenticity 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 Identification and Authentication Policy* shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of an identification and authentication policy and procedural guidelines;
- Management adoption of a formalized access control lifestyle;
- Management of identification and authentication for CIHA users;
- Multifactor authentication (MFA) use for network access to privileged accounts;
- MFA for local access to privileged accounts;
- MFA use for network access to non-privileged accounts;
- Implementation of replay-resistant authentication mechanisms;
- MFA for remote access to privileged and non-privileged accounts that require at least one (1) factor to be provided by a separate device;
- Incorporation of password parameter requirements;
- Password-based authentication requirements;
- Implementation of re-authentication requirements;
- In-person or trusted third-party authorization for registration of users;
- Feedback of authentication information must be obscured to protect the information from possible exploitation/use by unauthorized individuals;
- Implementation of cryptographic modules for authentication;
- Management of identification and authentication for non-CIHA users.

DEFINITIONS:

Access to Organizational Information Systems

Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., non-local access).

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.

Non-Privileged Account
Generally defined as a standard user account that does not have elevated privileges, such as administrator access to a system.

Privileged Account
Generally defined as a system administrator account. Privileged accounts have elevated permissions than those of a non-privileged user account.

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.

Identification and Authentication Policy and Procedural Guidelines
[NIST IA-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 identification and authentication process and the family of identification and authentication security controls. The identification and authentication 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 Identification and Authentication principles established in NIST, "Identification and Authentication" control guidelines, as the official standards for this security domain. The "IA" designator identified in each control represents the NIST-specified identifier for the Identification and Authentication 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 Identification and Authentication procedures include the necessary controls to facilitate the implementation of this Policy.

Policies and procedures are a critical component of CIHA's system of internal controls, which helps to ensure that all personnel have a clear understanding of roles, responsibilities, acceptable uses, and other important information that relates to identification and authentication 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.

Management Adoption:
Management recognizes the vital importance of implementing a documented and formalized access control lifecycle for all users accessing CIHA information systems. All necessary financial, operational, and technical support will consist of the following measures:

Financial:
Financial resources will be allocated for purchasing all products, services, and goods necessary for developing, implementing, and maintaining an effective access control lifecycle. These products, services, and goods include, but are not limited to, the following:

- Hardware;
- Software;
- Maintenance and service agreements;
- User training (administrative and end-user);
- Consulting services.

Operational and Technical:
Operational and technical resources will be allocated for implementing and maintaining an effective access control lifecycle. These resources include, but are not limited to, the following:

- Assigning internal personnel key roles and responsibilities within the access control lifecycle that they must perform as part of their job function. These duties will include provisioning of accounts, establishing access rights, creating password complexity rules, ensuring segregation of duties, monitoring of accounts, de-provisioning/off-boarding, and any other necessary measures for users having access to CIHA information systems;
- Assigning internal personnel key roles and responsibilities regarding the initial development and continued adoption, implementation, and success of an effective access control lifecycle platform. CIHA will utilize all necessary technology resources for ensuring the appropriate and secure network design and configuration for the described platform.

Management Enforcement:
Management is aware of the enforcement measures that must be in place for its access control lifecycle and will enact all necessary initiatives to promote adherence to these guidelines. Enforcement measures can range from predetermined guidelines created for users who will access CIHA information systems for their respective job requirements to the system administrators and privileged users responsible for establishing general access rights within those information systems for end-users.

Enforcement:
Enforcement guidelines have been adopted to ensure that CIHA continues to maintain all aspects of its access control lifecycle, which will include, but is not limited to, the following measures:

- Providing financial and operational technical resources and support, as necessary and as previously described;
- Adhering to the policies and procedural guidelines as stated within this document.

Provisioning - On-Boarding Process:

The user provisioning - on-boarding process is such a critical component of the access control lifecycle that comprehensive measures will be implemented to ensure that only authorized users are provisioned with access to CIHA information systems. As such, before any new users (e.g., employees, contractors, guests, etc.) are provisioned with access to CIHA information systems, they will undergo a series of new hire procedures consisting of, but not limited to, the following measures:

- Completion and submittal of application for employment;
- Reference and background checks for work experience and overall character;
- Criminal background checks;
- Drug testing;
- Acceptance of job offer by CIHA;
- Assignment of any necessary CIHA property.

Identification and Authentication (Organizational Users)

[NIST IA-2]

CIHA information systems and those operated on behalf of CIHA shall be configured to uniquely identify and authenticate users (or processes acting on behalf of users), following these processes:

a. System owners shall not allow the use of shared accounts [credentials used by more than one (1) individual] within their system unless a risk assessment determines that the CIA of information or information systems are not at risk. The sharing of user accounts makes it difficult to uniquely identify individuals accessing an information system, as well as provide detailed accountability of user activity within an information system;

b. Identification and authentication mechanisms shall be implemented at the application level, as determined by a risk assessment, to provide increased security for the information system and the information processes. This shall be in addition to identifying and authenticating users at the information system level (e.g., when initially logging into a desktop, laptop, or mobile device);

c. Access to non-privileged accounts, privileged accounts, and all local accounts shall be authenticated with passwords, personal identification numbers (PINs), tokens, biometrics, or in the case of MFA, some combination thereof;

d. CIHA information systems shall use MFA for the following conditions **Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Privileged Accounts [NIST IA-2(1)]**:

   i. Local access to information systems for all users using privileged accounts;

   ii. Remote access to information systems for all users using privileged accounts;

iii. Remote network access for all users with privileged and non-privileged accounts for information systems that receive, process, store, or transmit Highly Restricted data **Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Non-Privileged Accounts [NIST IA-2(2)]**;

iv. Remote access for all users with privileged and non-privileged accounts such that one (1) of the factors is provided by a device separate from the system gaining access. Factors are:

- **Something you know:**
  Includes passwords, passphrases, numerical PINS, or some other type of knowledge that is known by the user;
- **Something you have:**
  Includes some type of physical attribute provisioned to a user, such as a swipe card, badge reader, key fob, smart card, dynamically generated unique identifier, or any other type of utility owned by the user;
- **Something you are:**
  Generally includes a unique physical attribute of the user, commonly known as biometrics. Many devices read a user's biometrics for purposes of authentication, which may include, but is not limited to, a fingerprint scanner;

By requiring the use of a device that is separate from the information system to gain access and use one (1) of the MFA factors, the risk of compromising stored authentication credentials on the system is reduced **Identification and Authentication (Organizational Users) – Access to Accounts - Separate Device [NIST IA-2(6)]**;

e. CIHA information systems shall implement replay-resistant authentication mechanisms for network access to privileged accounts, if technically configurable **Identification and Authentication (Organizational Users) – Access to Accounts-Replay Resistant [NIST IA- 2(8)]**. Authentication processes resist replay attacks (valid data transmissions that are maliciously or fraudulently repeated or delayed) if it is impractical for an attacker to replay previous authentication messages and thus achieve unauthorized access. Replay-resistant techniques include, for example, protocols that use challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators (one-time passwords).

Identification and Authentication – Acceptance of Personal Identity Verification (PIV) Credentials:
[NIST IA-2(12)]
CIHA does not utilize PIV credentials.

Identification and Authentication (Organizational Users)

[NIST IA-2]

The concept of "identification" is incorporated into the access control lifecycle, which shall include the following initiatives:

- Establishing a valid and credible set of identification measures;
- Defining the different types of identification for all users who are authorized to gain access to information systems, such as employees, vendors, guests, contract workers, and other third parties;
- Defining the different types of provisioning/on-boarding process for all users who are authorized to gain access to information systems, such as employees, vendors, guests, contract workers, and other third parties;
- Implementing a documented and formalized provisioning /on-boarding process that includes:
    1. Request and approval;
    2. Validation;
    3. Creation of an identity for all users who are authorized to gain access to information systems, such as employees, vendors, guests, contract workers, and other third parties;
- Implementing all necessary forms, checklists, and other as-needed documentation for aiding and facilitating the user identification and provisioning process.

Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Privileged Accounts

[NIST IA-2(1)]

MFA is invoked for all users having network access to privileged accounts. MFA is thus defined as meeting two (2) of these three (3) conditions:

- Something you know;
- Something you have;
- Something you are.

Local access and network access will consist of the following measures:

- **Local Access**

  Any access to organizational information systems by users or processes acting on behalf of users where such access is obtained by direct connections without the use of networks;
- **Network Access**

  Any access to organizational information systems by user or processes acting on behalf of users where such access is obtained through network connections not deemed local, thus nonlocal;

- **Privileged Accounts**

  Accounts that allow users to perform various tasks, which are deemed privileged in nature and not allowable for use by all users. Such accounts include, but are not limited to, the following:
  - Administrator Accounts;
  - Root Accounts.

Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Non-Privileged Accounts

[NIST IA-2(2)]

MFA is invoked for all users having network access to non-privileged accounts. MFA is thus defined as meeting two (2) of these three (3) conditions:

- Something you know;
- Something you have;
- Something you are.

Local access and network access will consist of the following measures:

- **Local Access**:

  Any access that users or processes acting on behalf of users obtain through direct connections without using networks to organizational information systems;

- **Network Access**:

  Any access that users or processes acting on behalf of users obtain through network connections not deemed local (nonlocal) to organizational information systems;

- **Non-Privileged Accounts**:

  Accounts that allow users to perform various tasks that are not restricted by a number of conditions.

Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Privileged Accounts

[NIST IA-2(1)]

MFA is invoked for all users having local access to privileged accounts. MFA is thus defined as meeting two (2) of these three (3) conditions:

- Something you know;
- Something you have;
- Something you are.

Local access and network access will consist of the following measures:

- **Local Access**:

  Any access to organizational information systems by users or processes acting on behalf of users where such access is obtained by direct connections without the use

of networks;

- **Network Access**:

  Any access to organizational information systems by users or processes acting on behalf of users where such access is obtained through network connections not deemed local, thus nonlocal;

- **Privileged Accounts**:

  Accounts that allow users to perform various tasks, which are deemed privileged in nature and not allowable for use by all users. Such accounts include, but are not limited to, the following:

  - Administrator Accounts;
  - Root Accounts.

Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Non-Privileged Accounts
[NIST IA-2(2)]

The organizational information system implements MFA for local access to non-privileged accounts.

Identification and Authentication (Organizational Users) – Access to Accounts – Separate Device
[NIST IA-2(6)]

The information system implements MFA for remote access to privileged and non-privileged accounts, such that one (1) of the factors is provided by a device separate from the system gaining access. By requiring the use of a device that is separate from the information system to gain access and use one (1) of the MFA factors, the risk of compromising stored authentication credentials on the system is reduced.

Identification and Authentication (Organizational Users) – Access to Accounts – Replay Resistant [NIST IA-2(8)]

The information system shall implement replay-resistant authentication mechanisms for network access to privileged accounts, if technically configurable. Authentication processes resist replay attacks (valid data transmissions that are maliciously or fraudulently repeated or delayed) if it is impractical for an attacker to replay previous authentication messages and thus achieve unauthorized access. Replay-resistant techniques include, for example, protocols that use challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators (one-time passwords).

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Device Identification and Authentication

[NIST IA-3]

To protect the CIHA network from vulnerabilities that can be introduced when users access the network with unmanaged devices (e.g., personal computing devices), CIHA shall require that all users accessing the network adhere to and not attempt to deviate from required security configurations for their devices, including required patches and updated antivirus signature files on those devices. In order to protect CIHA data, the following steps are required:

a. Procedures that verify node authentication measures (techniques used to ensure that the managing server and data collectors communicate in a secure manner) shall be developed;

b. CIHA shall use only approved procedures, mechanisms, or protocols for host or device authentication. Approved mechanisms and protocols include, but are not limited to, the following:
   i. Media Access Control (MAC) address filtering, which provides basic filtering based on Open Systems Interconnection (OSI) Layer 2 (Data Link Layer) address information;
   ii. Vendor-specific solutions, which provide basic identification and authentication for devices in a wired network on a per-port basis;
   iii. Wi-Fi Protected Access 2 (WPA2) in combination with MAC filtering;
   iv. Institute of Electrical and Electronics Engineers (IEEE) 802.1x;
   v. Network Access Control (NAC) technology, which is most commonly built on the foundations of 802.1x;

c. Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks (also known as "subnets").

Identifier Management

[NIST IA-4]

CIHA shall ensure that all information systems, to include cloud provided services (like infrastructure, applications, and storage), have the following properties in place:

a. Receive authorization from a designated CIHA representative (e.g., system administrator, technical lead, or system owner) to assign individual, group, role, or device identifiers;

b. Select and assign information system identifiers that uniquely identify an individual, group, role, or device. These assignments shall ensure that no two (2) users or devices have the same identifier;

c. Prevent reuse of identifiers for seven (7) years;

d. Disable identifiers after one hundred twenty (120) days of inactivity, except as specifically exempted by CIHA management;

e. Delete or archive identifiers that have been disabled more than three hundred sixty-five (365) days.

Password Management Standards:

Non-Privileged Accounts

A non-privileged account is generally defined as a standard user account that does not have elevated privileges, such as administrator access to a system. For example, non-privileged accounts cannot make configuration changes to an information system or change the security posture of a system. CIHA information systems that use password-based authentication shall ensure the following:

a. Passwords have a minimum lifetime of one (1) day and a maximum lifetime of ninety (90) days. Password lifetime restrictions do not apply to temporary passwords;

b. Password reuse is prohibited for twelve (12) generations.

Privileged Accounts

A privileged account is generally defined as a system administrator account that allows users to perform various tasks deemed privileged in nature and not allowable by all users. For example, privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router management. Privileged accounts have the following properties:

a. Privileged accounts are generally used for performing administrative functions (e.g., configuration changes, system/software upgrade, and patch installations) and/or developing software;

b. Privileged accounts shall have passwords with a minimum lifetime of one (1) day and a maximum lifetime of thirty (30) days, whenever technically configurable, but must not exceed sixty (60) days.

Service Accounts

A service account is a non-interactive account created by system administrators for automated use by an application, operating system, or network device for business purposes. Service accounts shall be managed by the following:

a. Granting only the minimum level of access required to run a process;

b. Being dedicated solely to their business purpose and not being shared by an end user;

c. Separating privileged and non-privileged accounts;

d. Appropriately logging the account activity of all service accounts, as specified by CIHA. The application/device owner must audit the service account usage quarterly, at a minimum;

e. Having service account passwords change intervals, whenever technically configurable, appropriate to the level of risk posed by a potential compromise of the system. At a minimum, change intervals shall not exceed three hundred sixty-five (365) days;

f. Changing a service account password immediately after any potential compromise or any individual who knows the password leaves CIHA or changes roles within CIHA;

g. Seeking preapproval from CIHA management and the security liaison for special service accounts where an application or system is *specifically designed* to use 'non-expiring' passwords to complete their business purpose. CIHA approved controls, policies, and procedures must be in place to closely monitor and mitigate the risk of non-expiring passwords.

Authenticator Management – Password-Based Authentication
[NIST IA-5(1)]

The information system for password-based authentication:

a. Enforces minimum password complexity of eight (8) characters, a mix of upper-case letters, lower-case letters, numbers, and special characters;
b. Stores and transmits only cryptographically protected passwords;
c. Enforces password minimum and maximum lifetime restrictions;
d. Prohibits password reuse for twelve (12) generations;
e. Provides a temporary password for a system logon, allowing the user to immediately enter a permanent password.

Authenticator Management – Public Key-Based Authentication
[NIST IA-5(2)]

CIHA does not use Public Key Infrastructure (PKI)-Based Authentication.

Identity Proofing – In-Person Validation and Verification
[NIST IA-12(4)]

CIHA requires that the registration process for authentication be conducted in person or by a trusted third party with authorization from the CIHA Chief Information Officer (CIO).

Authenticator Management
[NIST IA-5]

The information system for hardware token-based authentication employs mechanisms that satisfy organization-defined token quality requirements.

a. CIHA manages information system authentication requirements. Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Related to the management of the system authentication requirements, CIHA:

i. Develops a set of secure log-on procedures to be applied to all network components, operating systems, applications, and databases that implement a user identification and authentication mechanism. These procedures shall

be designed to minimize the risk of unauthorized access;

ii. Verifies, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator **Identity Proofing – In-Person Validation and Verification [NIST IA-12(4)]**;

iii. Establishes initial authenticator content for authenticators defined by CIHA;

iv. Ensures that authenticators have sufficiently strengthened mechanisms for their intended use;

v. Establishes and implements administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators;

vi. Changes default content of authenticators, such as the default password, prior to information system installation;

vii. Requires individuals to have devices implement specific security safeguards to protect authenticators from unauthorized disclosure and modification;

viii. Changes authenticators for group/role accounts when membership to those accounts changes;

ix. Requires information systems to display a message to users before or while they are being prompted for their user identification and authentication credentials that warns against unauthorized or unlawful use. Refer to the **System Use Notification [NIST AC-8]** section of the *CIHA Access Control Policy* for the standard approved banner;

b. The log-on process should not be validated until user inputs all correct log-on data. Failing the process as each input field is completed will provide an attacker with information to further the attack;

c. Only generic "log-on failed" messages should be displayed if the user does not complete the log-on process successfully. Do not identify in the message whether the user identification, password, or other information is incorrect;

d. CIHA configures systems to limit the number of consecutive unsuccessful log-on attempts. If the number of consecutive unsuccessful log-on attempts exceeds the established limit, the configuration shall either force a time delay before further log-on attempts are allowed or shall disable the user account such that it can only be reactivated by a system or security administrator or an authorized help desk staff member;

e. All newly assigned passwords are changed the first time a user logs in to the information system;

f. Where technically feasible, passwords shall be at least eight (8) characters for access to all systems and applications;

g. Passwords shall have at least one (1) number, one (1) special character, and a mixture of at least one (1) uppercase and one (1) lowercase letter **Authenticator Management – Password-Based Authentication [NIST IA-5(1)]**;

h. Passwords shall not contain number or character substitutes to create dictionary words (e.g., d33psl33p for deepsleep);

i. Account passwords shall not traverse the network or be stored in clear text. All stored passwords shall be encrypted using FIPS-140-2 (and subsequent versions) encryption. FIPS-140-2 (and subsequent versions) is a set of standards used in designing, implementing, and operating cryptographic modules using appropriate levels of security with each level building on the lower level;

j. Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption;

k. Information systems may allow the use of a temporary password for a system logon as long as the temporary password is immediately changed to a permanent password upon the next log-on attempt;

l. Passwords shall be different from all other account passwords held by that user;

m. CIHA may use password management tools provided by the IT Department and approved by senior leadership Approved password managers must be installed and managed locally on the user's machine (not offsite or in the "cloud"), must securely store passwords with a master key or key file, and must encrypt the password list with FIPS 140-2 (and subsequent versions) encryption;

n. Passwords shall not be revealed to anyone, including supervisors, IT help desk personnel, security administrators, family members, or co-workers;

o. Users shall enter passwords manually for each application or system, except for simplified/single sign-on systems that have been approved by the CIHA CIO;

p. Passwords shall be changed whenever there is the suspicion or likelihood that the password or system is compromised;

q. CIHA shall validate the identity of an end user who requests a password reset. Initial passwords and subsequent password resets shall utilize a unique password for each user account.

Authentication Feedback

[NIST IA-6]

CIHA shall ensure that all information systems, including those operated on behalf of CIHA, execute the following:

a. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals;

b. Mask passwords upon entry (e.g., displaying asterisks or dots when a user types in a password) and not display passwords in clear text.

Cryptographic Module Authentication

[NIST IA-7]

a. CIHA shall ensure that the information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication;

b. Validation of cryptographic modules provides assurance that when CIHA implements cryptography, the encryption functions have been examined in detail and will operate as intended;

c. All encrypted electronic transmissions must be encrypted using FIPS 140-2 (and subsequent versions) validated cryptographic modules. NIST maintains a list of validated cryptographic modules on its website at: https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

Identification and Authentication – (Non-Organizational Users)

[NIST IA-8]

Identification and Authentication for Non-CIHA Users security control typically applies to CIHA information systems that are accessible to the general public (e.g., public-facing websites). CIHA shall ensure that the following for all non-CIHA users accessing information systems, including those operated on behalf of CIHA:

a. Approved third-party credentials must meet or exceed the set of minimum state and federal technical, security, and privacy requirements and CIHA maturity requirements;

b. CIHA information systems shall be configured to uniquely identify and authenticate non-CIHA users or processes acting on behalf of non-CIHA users;

c. CIHA information systems shall uniquely identify and authenticate non-CIHA users for all access other than those accesses explicitly identified and documented as exceptions in the *CIHA Access Control Policy* regarding permitted actions without identification and authentication.

Note: For any non-employee users being provisioned with access to CIHA resources, such as vendors, guests, or any other third parties, the following due diligence procedures include:

- **Vendors:**
  - Confirmation from authorized personnel that vendor has a valid business justification and reasoning for accessing CIHA information systems;
  - General business due diligence checks conducted on vendor;
  - Reference and background checks conducted on specific user employed by or representing the vendor;
  - Any other due diligence procedures deemed necessary.
- **Guests:**
  - Confirmation from authorized personnel that guest user has a valid business justification and reasoning for accessing CIHA information systems;
  - General business due diligence checks conducted on guest user;
  - Reference and background checks conducted on specific guest user;
  - Any other due diligence procedures deemed necessary.

Upon successful completion of the previous measures, all users are required to complete and submit the "Authorization Form for New Users" document, which provides all necessary details regarding the user who is being provisioned to access the CIHA information systems. Additionally, three (3) different "Authorization Form for New Users" documents have been developed to ensure that all provisioning procedures are documented accordingly with all required information for the user groups. This allows CIHA to capture, record, and ultimately assess all user provisioning information as necessary for each of the following three (3) user groups:

- **New Employees:**
  Includes individuals who have been hired by CIHA as full-time or part-time employees, thus considered "new users."
- **Vendors:**
  Includes service providers and other entities that require access to CIHA information systems for performing a specific function.
- **Guests:**
  Includes contract workers and all other third parties not listed within the scope of these three (3) documents.

Re-Authentication

[NIST IA-11]

All users of information systems are required to re-authenticate once the session expires, locks, or is terminated by the user or by other means. Additionally, re-authentication measures will be taken when the following conditions apply:

- When authenticators change;
- When roles change;

- When security categories of information systems change;
- When the execution of privileged functions occurs;
- After a fixed period of time.

Appropriate Security Measures:

Passwords will be protected at all times using the appropriate security measures that have been established for each system resource, having the ability to store passwords and authenticate a user's password.

Passwords:

The following password properties will be incorporated into the user identity, provisioning, and access rights lifecycle, which shall include the following initiatives:

- Frequency for changing passwords;
- Complexity requirements (password length and alphanumeric requirements);
- Previous password usage;
- Account lockout, reset, and idle time parameters;
- Password resets;
- First-time passwords;
- Employing password protection best practices for ensuring the safety and confidentiality of a user's password(s) during transit and storage;
- Employing all necessary hashing and encryption measures for protecting passwords that are stored in CIHA information systems and when using a password during authentication;
- Implementing all necessary forms, checklists, and other as-needed documentation for aiding and facilitating the stated password policies and procedures.

Password Parameters:

Password Parameters are set to require the following:

- Users to change passwords at least every sixty (60) days;
- Passwords to be at least eight (8) characters;
- Passwords to contain both numeric and alphabetic characters;
- New passwords cannot be the same as the previous twelve (12) generations.

Device Lock [NIST AC-11] and **Device Lock – Pattern-Hiding Displays [NIST AC-11(1)]**

The information system:

a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user and retains the session lock until the user reestablishes access using established identification and authentication procedures;

b. System configuration settings are set to require that system/session idle timeout features have been set to a period of thirty (30) minutes or less;

c. Ensures a user requesting a password reset who is not in the physical presence of appropriate and designated IT personnel must undergo a verification process through verbal confirmation, which consists of one (1) of the following activities:
    - Providing vital statistics to intended party who may reset their password. This verbal confirmation may consist of a supervisor's name and/or phone number or some other unique identifier;
    - Supplying employment data, such as length of employment;
    - Offering some other unique identifier developed by CIHA;

d. First-time passwords for new users and reset passwords for existing users are set to a one (1)-time unique value and become invalid after each use.

Password Protection Best Practices:

Passwords used for authenticating CIHA information systems are to adhere to the password parameters previously stated, which have been designed, approved, and implemented by authorized personnel. Accessing information systems is a privilege, and as such, great care is to be taken by all users for protecting the confidentiality of personal password(s), which includes, but is not limited to, the following measures:

- Users are prohibited from writing down passwords and displaying them on or around the workstation vicinity;
- Users are prohibited from asking for other users' passwords for the purposes of accessing CIHA information systems;
- Users are prohibited from transmitting passwords via unsecure messaging technologies, such as instant messaging platforms, facsimile, unencrypted email, or any other untrusted form of data transmission;
- Users are prohibited from having passwords reset if they failed to undertake the necessary and required password reset protocols as stipulated.

Password Protection Measures:

Passwords used for authenticating to CIHA information systems will employ appropriate security measures for ensuring the security of the password during transit over the network. Unsecure network protocols are prohibited from being used, as passwords can be intercepted. Storing passwords within CIHA information systems requires appropriate security measures to be employed, such as hashing and encryption.

Unsecure network protocols, which include, but are not limited to, the following, will transfer password and related data in clear text and are, therefore, prohibited from being used:

- HTTP (Hypertext Transfer Protocol);
- FTP (File Transfer Protocol);
- SMTP (Simple Mail Transfer Protocol);
- POP3 (Post Office Protocol 3);
- Telnet.

Thus, secure network protocols that employ Transport Layer Security (TLS) and SSL protection will be used when passwords are in transit of the network. These protocols consist of the following:

- HTTPS (Hypertext Transfer Protocol Secure);
- SFTP (Secure File Transfer Protocol);
- SSH (Secure Shell);
- TLS.

Privileged Users:

Users identified as having elevated, super user, root, or other type of administrative or privileged access credentials are to have their accounts regularly monitored and audited to ensure access rights are commensurate and appropriate for users' respective roles and responsibilities within CIHA. Privileged users have the ability to exploit information systems by engaging in malicious and unethical activities that may be difficult to identify or stop. These actions can lead to any number of security breaches within CIHA (e.g., theft of sensitive CIHA data, destruction of vital electronic assets, etc.). As such, the following measures regarding privileged users and their access rights will be implemented:

- Execute effective monitoring and auditing processes, as necessary;
- Eliminate shared accounts and employ effective segregation of duties among privileged users;
- Ensure all default privileged accounts on all information systems have been appropriately identified, assigned, and/or locked down, as necessary;
- Utilize effective automated Privileged User Management (PUM) software applications, as necessary.

Dormant Accounts:

Accounts within CIHA's information systems that have been identified as dormant and inactive pose significant threats to CIHA assets and are to be removed immediately. Dormant accounts can be used by former workforce, hackers, and other malicious individuals to gain unauthorized access to information systems. As such, the following measures regarding the timely removal of dormant accounts will be implemented:

- Develop and implement custom scripts that can be used to determine user activity for all accounts;
- Employ comprehensive user off-boarding/de-provisioning procedures, as necessary;

- Implement effective monitoring and auditing measures, as necessary.

Stale Privileges:

Stale privileges are access rights granted to current users, which are no longer needed or necessary to perform respective job functions. User access rights often change because different resources within CIHA require authorization as a condition of job performance. These actions result in significant changes to access rights to various information systems. As such, the following measures to ensure that stale privileges are eliminated from user accounts are to be implemented:

- Require all users who seek changes in user access to complete an "Access Rights Change Control" document, which details all access rights afforded to that specific user, while ensuring that all previous privileges, where applicable, are effectively removed;
- Implement effective monitoring and auditing measures.

Database Access Rights:

CIHA considers database security to be of extreme importance due to the enormous amount of confidential information held within these systems and the growing number of data breaches and exploitations reported within other organizations. Of the many domains related to database security, access rights are considered a critical area where effective security must be in place to ensure the CIA of the database environments.

Overall, CIHA ensures that only properly authenticated (authentication) users will perform authorized (authorization) actions. As such, the following measures, which ensure appropriate database access rights, are to be implemented:

- Implement effective access control procedures, such as RBAC, where applicable, along with Discretionary Access Control (DAC), whereby flexibility and discretion are allowed when granting subjects (i.e., users) access to items within the database environments;
- Designate authorized IT personnel as the Database Administrator, whereby this user is given a super user account for a large number of privileged commands and is ultimately responsible for establishing effective access control mechanisms for ensuring the safety of databases;
- Implement programmatic methods, such as stored procedures, for users accessing databases for purposes of retrieving information, performing queries, and other user actions;
- Restrict the number of users that have privileged accounts within databases, thus limiting users, where applicable, to only querying databases;

- Implement effective monitoring and auditing measures.

Access Rights Change Control:

Users requesting access changes to information systems within CIHA are to complete an "Access Rights Change Control" document to include a comprehensive documentation process and subsequent provisioning and, if necessary, de-provisioning procedures.

User De-Provisioning and Off-Boarding:

CIHA has a documented de-provisioning/off-boarding process that includes:

- Request and Approval;
- Validation;
- Disabling of or deletion of accounts;
- Implement measures for ensuring that all critical accounts (e.g., email, voicemail) previously used by the de-provisioned and off-boarded user are appropriately maintained as needed by CIHA;
- Implement all necessary forms, checklists, and other as-needed documentation for aiding and facilitating the user identification and provisioning process.

This process is for all users who have been terminated from CIHA, resulting in the removal of access to information systems. These users include, but are not limited to, employees, vendors, guests, contract workers, and all other third parties.

CIHA has developed and implemented a comprehensive user de-provisioning/off-boarding process, which encompasses the following categories and supporting activities listed in the next section of this Policy. CIHA will fully enforce these policy directives to ensure that the user authentication initiatives are executed in a formal manner and on a consistent basis for all information systems that CIHA deems critical.

De-Provisioning and Off-Boarding Process:

The user de-provisioning and off-boarding process is a critical component of the user identity, provisioning, and access rights lifecycle, and as such, comprehensive measures are to be implemented to ensure that all terminated users are appropriately removed from having access to any CIHA information systems. Failure to enact these measures could potentially result in a breach of security within CIHA, as terminated users may still be able to gain authorized access to CIHA information systems. Thus, the following procedures to be undertaken include the following:

- Complete a Separation Form and contact (via email, telephone, or in person) all appropriate personnel responsible for terminating users from all CIHA information systems;

- Obtain signatures on the aforementioned Form from all individuals directly involved in the actual de-provisioning/off-boarding procedures for the terminated users;
- Confirm that terminated users have been effectively removed from system access to all CIHA information systems, to include undertaking the following procedural guidelines:
  - Inspect all information systems and supporting utilities for which authentication and authorization rights were initially established for terminated users;
  - Obtain the appropriate evidence (i.e., system screenshots and other system settings, as necessary) from the information systems that resulted in the user's termination and effective access removal and attach the applicable documentation to the Separation Form.

Critical Accounts:

Critical accounts for de-provisioned and off-boarded users will be appropriately maintained by authorized personnel for ensuring that correspondence, such as emails, voicemails, and other forms of communication are addressed in a timely manner by CIHA. As such, the following critical accounts will be monitored following the de-provisioning/off-boarding process for terminated users:

- Email accounts;
- Voicemail/Private Branch Exchange (PBX);
- Cellular devices;
- Any other forms of communication.

Authentication:

The concept of "authentication" is incorporated into the user identity, provisioning, and access rights lifecycle, which shall include the following initiatives:

- Requiring users to utilize a username with a password, passphrase, or some other type of commonly employed method of "authentication" to legitimately authenticate to the specified information system.

  Note: Users are to employ one (1) of or a combination of the following three (3) factors for authentication, depending on the type of authentication:
  - Something you know;
  - Something you have;
  - Something you are;
- Establishing password, passphrase, and other as-needed authentication complexity rules and parameters for authenticating to information systems;
- Utilizing appropriate security measures for password protection;

- Implementing all necessary forms, checklists, and other as-needed documentation for aiding and facilitating the user authentication process.

Methods of Authentication:

Authentication to CIHA information systems is encrypted by utilizing one (1) of or a combination of the following three (3) stated factors:

- Something you know;
- Something you have;
- Something you are.