Scope

The Statewide Information Security Polices are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (Agency CIO) to establish an agency wide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law. This security policy is consistent with applicable laws, executive orders, directives, regulations, other policies, standards, and guidelines.

Material Superseded

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.

Responsibilities

All covered personnel accessing or using IT resources are responsible for adhering to this policy and with any local Identification and Authentication requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated agency officials at the senior leadership level are assigned the responsibility for the continued development, dissemination, implementation, operation and monitoring of the Identification and Authentication process.
Agency Security Liaisons	Agency Security liaisons are responsible for ensuring that adequate user identification and authentication controls are present in all agency computing environments including those managed by agencies or by third parties.
Information System Owner	The Information System Owner (SO) is responsible for ensuring that identification and authentication controls for the system are implemented in coordination with agencies, information owners, security system administration, and the information system security officer, and functional "end users."
Information Owner	The information owner is the individual with operational responsibility and authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Provides input to information system owners (ISO)s regarding security requirements and security controls for the information

	system(s) where the information resides. Decides who has access to the information system and with what types of privileges or access rights.
Covered Personnel	Covered personnel are responsible for following the approved identification and authentication processes and the supporting controls.
Third Parties	Third party service providers with systems interconnected to the agency network are responsible for managing identification and authentication actions in accordance with this policy.

IA-1 – Policy and Procedures

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the requirements set forth by the State to implement the family of Identification and Authentication security controls at the organization, process and/or system level for all information assets / State data. This policy provides requirements for the identification and authentication process which is required to assure that information systems are designed and configured using controls sufficient to safeguard the State's information systems.

The State has adopted the Identification and Authentication principles established in NIST SP 800-53, "Identification and Authentication" control guidelines as the official policy for this security domain. The "IA" designator identified in each control represents the NIST-specified identifier for the Identification and Authentication control family. The following subsections in this document outline the Identification and Authentication requirements that each agency must implement and maintain in order to be compliant with this policy. This policy and associated procedures shall be reviewed and updated annually, at a minimum. They shall also be updated following agency-defined events that necessitate such change.

This policy and the associated procedures shall be developed, documented, and disseminated by the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level.

IA-2 - Identification and Authentication Authorized Users

Information systems shall be configured to uniquely identify and authenticate users (or processes acting on behalf of users). Access to information systems is defined as either local access or network access. Local access is any access to 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 information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (e.g., nonlocal access).

a. System Owners shall not allow the use of shared accounts (credentials used by more than one individual) within their system. The use of shared 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 multifactor authentication (MFA), some combination thereof. **Note:** See IA–5 - Authenticator Management for definitions of privileged and non-privileged accounts.

IA-2 (1) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts

MFA shall be implemented for access to privileged accounts.

IA-2 (2) – Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-Privileged Accounts

a. MFA shall be implemented for remote network access with privileged and non-privileged accounts for information systems that receive, process, store, or transmit Restricted or Highly Restricted data.

b. MFA for remote access with privileged and non-privileged accounts shall be implemented such that one of the factors is provided by a device separate from the system gaining access. The purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system.

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

Information systems shall implement replay-resistant authentication mechanisms for network access to privileged accounts, if technically configurable. Authentication processes resist replay attacks 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).

IA-2 (12) - Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

Organizations shall accept and electronically verify Personal Identity Verification-(PIV) compliant credentials.

IA-3 - Device Identification and Authentication

To protect State resources from vulnerabilities that can be introduced when users access the network with unmanaged devices, such as personal computing devices, all users accessing those resources shall adhere to required security configurations for devices, including required patches and updated anti-virus signature files on those devices.

a. Procedures that verify node authentication measures shall be developed.

b. Only approved procedures, mechanisms, or protocols shall be used 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 (“subnets”).

IA–4 - Identifier Management

All information systems, to include cloud provided services, shall do the following:

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

b. Select and assign information system identifiers that uniquely identify an individual, group, role, service, or device. Assignment of individual, group, role, service, or device identifiers shall ensure that no two users or devices have the same identifier.

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

d. Disable identifiers after ninety (90) days of inactivity, except as specifically exempted by agency management.

e. Delete or archive identifiers that have been disabled more than 365 days.

IA-4 (5) Identifier Management | Identify User Status

Procedures shall be implemented to ensure that individual identifiers are managed by uniquely identifying each individual's credentials, such as employee, contractor, active, inactive, lock or disabled.

IA–5 - Authenticator Management

Information system authentication requirements shall be managed. Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. The following shall be required:

a. Develop 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.

b. Verify, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.

c. Establish initial authenticator content for authenticators issued by the organization.

d. Ensure that authenticators have sufficient strength of mechanism for their intended use.

e. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

f. Change default content of authenticators, for example, the default password immediately after system install.

g. Require individuals to take, and have devices implement, specific security safeguards to protect authenticators from unauthorized disclosure and modification.

h. Change authenticators for group/role accounts when membership to those accounts changes.

i. Information systems shall display a message to users before or while they are prompted for their user identification and authentication credentials that warns against unauthorized or unlawful

use. Refer to the Access Control policy AC-8 - System Use Notification for the standard State approved banner.

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

k. 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.

l. Systems shall be configured 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 service desk staff member.

m. For systems that store, transmit, or process FTI, the agency shall password-protect the system initialization (boot) settings.

n. All newly assigned passwords shall be changed the first time a user logs into the information system.

o. Where technically configurable, passwords shall be at least fourteen (14) characters long for access to all systems and applications.

p. Passwords shall consist of at least one (1) numeric, at least one (1) uppercase, at least one (1) lowercase letter, and at least one (1) special character.

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

r. Account passwords shall not traverse the network or be stored in clear text. All passwords stored shall be encrypted using FIPS-140-2 encryption.

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

t. Information systems may allow the use of a temporary password for system logons if the temporary password is immediately changed to a permanent password upon the next logon attempt.

u. Passwords shall be different from all other accounts held by that user.

v. Agencies may use password management tools approved by the Enterprise Security and Risk Management Office (ESRMO). 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 encryption.

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

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

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

z. The identity of an end user shall be validated when a password reset is requested. Initial passwords and subsequent password resets shall utilize a unique password for each user account.

aa. Passwords that are at least fourteen (14) characters long shall not be reused until five (5) additional passwords have been created. If passwords are less than fourteen (14) characters long, they must not be reused until twenty-four (24) additional passwords have been created.

bb. Passwords shall not have a minimum lifetime when used as an initial password or during a reset where a temporary password is provided. Use of this type of password shall be configured to require an immediate change on first use.

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 instance, non-privileged accounts cannot make configuration changes to an information system or change the security posture of a system. Information systems that use password-based authentication shall do the following:

a. Passwords shall have a minimum lifetime of one (1) day and a maximum lifetime of one year with MFA and one hundred eighty (180) days without MFA. For directory-based accounts, where the account can be used multiple places, MFA must be enforced for all instances to qualify for “with MFA”.

b. While the State is transitioning to the new standard stated above, passwords less than fourteen (14) characters long for non-privileged accounts shall have a maximum lifetime of ninety (90) days.

c. Passwords for citizens and business users are recommended to be changed at least annually.

Password Management Standards – Privileged Accounts

A privileged account is generally defined as a system administrator account. Privileged accounts have elevated permissions that allow them to do certain tasks a non-privileged user account cannot. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router management.

a. Privileged accounts are generally used for performing administrative functions, such as configuration changes, system/software upgrade, 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 one hundred eighty (180) days with MFA and ninety (90) days without MFA. For directory-based accounts, where the account can be used multiple places, MFA must be enforced for all instances to qualify for "with MFA".

d. While the State is transitioning to the new password lifetime standard stated above, passwords less than fourteen (14) characters long for privileged accounts shall have a maximum lifetime of thirty (30) days.

Password Management Standards—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 their business purpose. Service accounts shall be managed by the following:

a. Service accounts shall only be granted the minimum level of access required to run a process.

b. Service accounts must be dedicated solely to their business purpose and not shared by an end user.

c. Service accounts shall be separate from privileged and non-privileged accounts.

d. All service accounts must have appropriate logging as specified by the agency of account activity. The application/device owner must audit the service account usage semi-annually, at a minimum.

e. Whenever technically configurable, service account passwords must have change intervals appropriate to the level of risk posed by a potential compromise of the system. At a minimum, change intervals shall not exceed 364 days (1 year).

f. A service account password must be changed immediately after any potential compromise or any individual who knows the password leaves the organization or changes roles within the organization.

g. In the special case where an application or system is *specifically designed* for service accounts to use 'non-expiring' passwords to complete their business purpose, these accounts must be preapproved by agency management and the agency's security liaison. Agency approved controls, policies, and procedures must be in place to closely monitor and mitigate the risk of non-expiring passwords.

IA-5 (1) Authenticator Management | Password-based authentication

The following shall be done for password-based authentication:

a. Utilize a list of commonly used, expected, or compromised passwords that is regularly updated. The list should be reviewed at an organization defined frequency.

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-5(1)(a);

c. Transmit passwords only over cryptographically protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the composition and complexity rules defined in IA (5).

IA-5 (6) Authenticator Management | Protection of Authenticators

Authenticators shall be protected commensurate with the security category of the information to which use of the authenticator permits access.

IA-6 - Authenticator Feedback

All information systems including those operated on behalf of the agencies shall ensure the following:

i. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

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

IA-7 - Cryptographic Module Authentication

a. Mechanisms shall be implemented for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

b. Validation provides assurance that when an organization 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 validated cryptographic modules. NIST maintains a list of validated cryptographic modules on its website at http://csrc.nist.gov/.

IA-8 – Identification and Authentication (Non-Agency Users)

This control typically applies to information systems that are accessible to the general public, for example, public-facing websites. The following shall be done for all non-agency users accessing information systems, including those operated on behalf of the agencies.

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

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

c. Information systems shall uniquely identify and authenticate non-agency users for all access other than those explicitly identified and documented as exceptions in the Access Control Policy SCIO-SEC-301 regarding permitted actions without identification and authentication.

IA-9 - Service Identification and Authentication (Optional)

This control is optional for Low and Moderate risk information systems.

IA-10 - Adaptive Identification and Authentication (Optional)

This control is optional for Low and Moderate risk information systems.

IA-11 - Re-Authentication

Organizations may require users to re-authenticate during the following circumstances / situations:

a. When an account changes and necessities re-authentication,
b. When a privileged function occurs,
c. When the user's role changes,
d. After an agency defined fixed period of time.

IA-12 Identity Proofing

Organizations shall ensure the following:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

d. This control is optional for LOW risk information systems.

IA-12 (2) Identity Proofing |Identity Evidence

Evidence of individual identification such as documentary evidence or a combination of documents and biometrics must be presented to the registration authority. A registration authority refers to the department, team and/or role that owns the process of validation and verification of an identity. If required, this authority could use external sources/services for completion of the validation and verification of the individual's identity.

IA-12 (3) Identity Proofing | Identity Evidence Validation and Verification

The presented identity evidence shall be validated and verified through agency defined methods of validation and verification. Depending on the type of position and the risk of the job role/position, defined methods include the validation and verification of the following documentation:

a. ID card issued by Federal, state, or local government

b. US Passport

c. Birth Certificate

d. Permanent Resident Card

e. School ID card with a photograph

IA-12 (5) Identity Proofing | Address Confirmation

A registration code or a notice of proofing must be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Approved: DocuSigned by: James Weaver 372C8D237E5547A... 1/19/2022 | 11:34 AM EST

Secretary of Department of Information Technology (DIT