Policy #:	Title:	Effective Date:
x.xxx	Identification and Authentication Policy	MM/DD/YY

PURPOSE

To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116; Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. IDENTIFICATION AND AUTHENTICATION
   IT Department shall:

   a. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of [entity] users.

   b. Ensure that information systems implement multifactor authentication for network access to privileged accounts.

   c. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.

   d. Ensure that information systems implement multifactor authentication for local access to privileged accounts.

   e. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.

   f. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

g. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.

2. DEVICE IDENTIFICATION AND AUTHENTICATION
   IT Department shall:

   a. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

3. IDENTIFIER MANAGEMENT
   IT Department, through department information systems owners, shall:

   a. Ensure that the [entity] manages information system identifiers by receiving authorization from [entity defined personnel or roles] to assign an individual, group, role, or device identifier.

   b. Select an identifier that identifies an individual, group, role, or device.

   c. Assign the identifier to the intended individual, group, role, or device.

   d. Prevent reuse of identifiers for 90 days.

   e. Disable the identifier after 30 days of inactivity.

4. AUTHENTICATOR MANAGEMENT
   IT Department shall:

   a. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

   b. Establish initial authenticator content for authenticators defined by the organization.

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

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

   e. Change default content of authenticators prior to information system installation.

f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.

g. Change/refresh authenticators every 90 days.

h. Protect authenticator content from unauthorized disclosure and modification.

i. Require individuals and devices to implement specific security safeguards to protect authenticators.

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

k. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.

l. Ensure passwords must contain characters from three of the following five categories:

   i. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);

   ii. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);

   iii. Base 10 digits (0 through 9);

   iv. Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and

   v. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

m. Require passwords to have a minimum length of 8 characters.

n. Enforce at least one changed character when new passwords are created.

o. Store and transmit only cryptographically-protected passwords.

p. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.

q. Prohibit password reuse for 12 generations.

r. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

s. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

t. Enforce authorized access to the corresponding private key.

u. Map the authenticated identity to the account of the individual or group.

v. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

w. Require that the registration process to receive [entity defined types of and/or specific authenticators] be conducted in person or by a trusted third party before [entity defined registration authority] with authorization by [entity defined personnel or roles].

x. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy [entity defined token quality requirements].

5. AUTHENTICATOR FEEDBACK
IT Department shall:

a. Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

6. CRYPTOGRAPHIC MODULE AUTHENTICATION
IT Department shall:

a. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

7. IDENTIFICATION AND AUTHENTICATION
IT Department shall:

a. Ensure that information systems uniquely identify and authenticate non-entity users or processes acting on behalf of non-entity users.

b. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.

c. Ensure that information systems accept only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials.

d. Ensure that the organization employs only FICAM-approved information system components in [entity defined information systems] to accept third-party credentials.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY