Policy and Procedure 9-7
Information Security: Identification and Authentication

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	7/1/2024
Effective Date:	June 6, 2024		
Codes/Mandates:	Code of Virginia, §2.2-2005 Creation of Agency; appointment of Chief Information Officer Code of Virginia: §2.2-2007 Powers of the CIO		
References:	Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00, Commonwealth ITRM Standard SEC502: Audit Security Standard Commonwealth ITRM Standard SEC530: Information Security Standard		
Forms:	N/A		

CONTENTS

PURPOSE

The purpose of this policy and procedure is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that Department of Forestry develops, disseminates, and updates the Identification and Authentication policy and procedure. This policy and procedure establishes the minimum requirements for the Identification and Authentication controls.

This policy and procedure is intended to meet the control requirements outlined in SEC-530, Section 8.7 Identification and Authentication Family, Controls IA-1 through IA-12, to include specific requirements for the Commonwealth of Virginia.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all Department of Forestry information and information systems including systems used or operated by contractors and other third parties on behalf of Department of Forestry.

DEFINITIONS and ACRONYMS

"Agency" and **"DOF"** means the Virginia Department of Forestry.

"Information security officer" and **"ISO"** means the agency employee who is designated by the state forester to develop and manage the agency's information security program, as required in the Commonwealth's Information Security Standard, SEC530.

"System administrator" means the agency employee who implements, manages, and/or operates a system at the direction of the system owner or data owner.

"System owner" means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

ACRONYMS

BIA:	Business Impact Analysis
CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DOF:	Department of Forestry
DRP:	Disaster Recovery Plan
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC530:	Information Security Standard 530
VCCC:	VITA Customer Care Center
VITA:	Virginia Information Technology Agency

BACKGROUND

The identification and authentication program at Department of Forestry is intended to ensure that necessary security controls are integrated into systems and processes within the Department of Forestry. This policy directs that the Department of Forestry meet the requirements as stipulated by COV ITRM Security Standard SEC530 and security best practices.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describes 4 role specific activities:

- Responsible (R) – Person working on activity
- Accountable (A) – Person with decision authority and one who delegates the work
- Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
- Informed (I) – Person who needs to know of decision or action

	User	User Manager	System Owner	System Admin	Information Security Officer

Tasks					
Configure information systems to uniquely identify and authenticate organizational users.			A	R	I
Manage information system identifiers			I	R	A
Configure two-factor authentication for network-based administrative access.			A	R	I
Manage information system authenticators.			R	R	A
Map individuals to accounts				R	A
Establish initial authenticator content.				R	A
Establish procedures for authenticator distribution.					A/R
Change default content authenticators.			A	R	I
Protect authenticators from unauthorized disclosure.	A				I
Configure system to enforce authenticator best practices.			A	R	R
Train users on password best practices.					A/R
Ensure that unencrypted static authenticators are not embedded in applications.			A	R	R
Store hardware passwords securely.			A	R	R
Protect authenticators on internet-facing systems.			A	R	R
Configure or verify that system obscures feedback of authentication information.			A	R	R
Configure the information system to use mechanisms for authentication to a cryptographic module.			A	R	R
Configure the information system to uniquely identify and authenticate non-organizational users.			A	R	R

STATEMENT OF POLICY

In accordance with SEC530, IA-1 through IA-12, all users of Department of Forestry IT resources will be assigned a unique identity to securely authenticate to the systems that they have been authorized to access. The ISO will develop, disseminate, and review/update the Identification and Authentication Policy and Procedure at least on an annual basis and following an environmental change.

Identification and Authentication (Organizational Users) (IA-2)

The ISO will require that:

1. The system administrator will configure the information system to uniquely identify and authenticate organizational users and associate processes acting on behalf of those users.

   Note: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees.

2. Users must be uniquely identified and authenticated for all access other than those accesses explicitly identified and documented as exceptions regarding permitted actions without identification and authentication.
3. Group or shared accounts are not permitted.
4. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics or in the case of multifactor authentication, some combination thereof.
5. When possible, multi-factor authentication for remote access to privileged accounts and non-privileged accounts will be implemented such that:

   a. One of the factors is provided by a device separate from the system gaining access.

   b. The device meets organization-defined strength of mechanism requirements.

6. Replay-resistant authentication mechanisms are required.
7. Provide a single sign-on capability for organization-defined system accounts and services when possible.

Identifier Management (IA-4)

1. The system administrator will manage information system identifiers for users and devices by:
   a. Receiving authorization from a supervisor to assign an individual, group, role, service or device identifier.
   b. Selecting an identifier that identifies an individual, group, role, service or device.
   c. Assigning the identifier to the intended individual, group, role, service, or device.
   d. Preventing reuse of identifiers for at least one year.
   e. Maintain the attributes for each uniquely identified individual, device or service in organization-defined protected central storage.

Authenticator Management (IA-5)

The ISO or designee will require that:

1. System administrators manage information system authenticators for users and devices by:

   Note: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices and ID badges

   a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.
   b. Establishing unique initial authenticator content for authenticators defined by the organization.
      - **Note:** Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length).
   c. Ensuring that authenticators have sufficient strength of mechanism for their intended use.
   d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators and for revoking authenticators.
   e. Changing default content of authenticators upon information system installation.
      - **Note:** Default content of authenticators (i.e., passwords provided for initial entry to a system) must be changed by the system administrator before implementation of the information system or component (e.g., routers, switches, firewalls, printers, workstations, servers).
   f. Delivering the initial/temporary password must be delivered to the IT system user in a secure and confidential manner, if the system is sensitive (e.g., in person, secure email, etc.).
   g. Protecting authenticator content from unauthorized disclosure and modification.
   h. Requiring individuals to take and having devices implement, specific controls to protect authenticators.
   i. Changing authenticators for group or role accounts when membership to those accounts change.
2. DOF users must protect account identifiers by:
   a. Protecting authenticator content from unauthorized disclosure and modification.
   b. Maintaining exclusive control and use of their passwords by not loaning or sharing authenticators with others.
   c. Protecting them from inadvertent disclosure to others.
   d. Posting or displaying passwords is prohibited.

e. Reporting lost or compromised authenticators immediately to their supervisor, DOF IT Help Desk and the VCCC, in the case of COV passwords, as a security event.

3. The system owner shall confirm that software and/or hardware upgrades, updates and patches have not reinstalled default passwords.
4. For all DOF password-based authentication, the following enhancements are required:
   a. Maintain a list of commonly used, expected, or compromised passwords and update the list at least on a quarterly basis and when organizational passwords are suspected to have been compromised directly or indirectly.
   b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords
   c. Access to files containing passwords or password hashes must be limited to the IT system and its administrators.
   d. Transmit passwords only over cryptographically protected channels.
   e. The use of cached authenticators is prohibited.
   f. Store passwords using an approved salted key derivation function, preferably using a keyed hash.
   g. Require immediate selection of a new password upon account recovery.
   h. Passwords (other than initial) must be chosen by users, not assigned by system administrators or help desk staff.
   i. Allow user selection of long passwords and passphrases, including spaces and all printable characters.
   j. Passwords must have a minimum lifetime of 1 day(s) and a maximum lifetime of 42 days.
   k. Enforce the following composition and complexity rules:
      i. When a password is the only authenticator:
         a. At least 14 characters in length.
         b. Utilize each of the following four:
            i. Special characters
            ii. Alphabetical characters
            iii. Numerical characters
            iv. Combination of upper case and lower-case letters
         c. Password reuse is prohibited for 24 generations.
         d. Authenticators must be changed at least every 42 days.
      ii. When used as a component of multi-factor authentication:
         a. At least 8 characters in length.
      iii. For smart phones or tablets accessing or containing COV data, a password with a minimum of 6 characters is required.
5. Devices must be configured to safeguard authenticators (e.g., certificates, passwords).
6. Changing authenticators for group or role accounts when membership to those accounts change.
7. Developers and installers of system components are required to provide unique authenticators or change default authenticators prior to delivery and installation.
8. For internet facing web applications, the minimum password length must be fourteen characters and meet the following requirements:

a. Enforces password minimum and maximum lifetime restrictions of 24 hours minimum and 42 days maximum.

b. Prohibits passwords and PINs from being displayed when entered.

c. Requires that the IT system user change the initial/temporary password upon his/her first successful login.

d. Enforces Account Lockout using the following parameters:

i. The account lockout is enabled, the threshold is three invalid attempts, and the duration is at least 15 minutes.

ii. Accounts that are unused for 90 consecutive days must be disabled.

e. Enforces password protected screen saver lock after a period of no more than 15 minutes of inactivity.

f. Requires that forgotten initial passwords be replaced rather than reissued.

9. For Internet-facing systems containing sensitive data provided by private citizens, which is accessed by only those citizens who provided the stored data, the system owner shall:

a. Determine the appropriate validity period of the password, commensurate with sensitive and risk.

b. Determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitivity and risk.

c. Allow the citizen to continue to use the initial password so long as the agency provides a mechanism to the citizen that allows the citizen to create a unique initial password.

d. Provide the account holder with information on the importance of changing the account password on a regular and frequent basis.

Authenticator Feedback (IA-6)

1. The information system must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

a. Passwords must be masked upon entry (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text.

2. The feedback from the information system must not provide information that would allow an unauthorized user to compromise the authentication mechanism.

Cryptographic Module Authentication (IA-7)

1. The system administrator will configure the information system to use mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, directives, policies, regulations, standards and guidance for such authentication.

Identification And Authentication (Non-Organizational Users) (IA-8)

1. The system administrator will configure the information system to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users) insuring that:

a. Profiles for identity management conform to standards described in the Enterprise Architecture Standard: Enterprise Solution Architecture: Identity Access Management.

b. Accept only external authenticators that are NIST-compliant.

c. Document and maintain a list of accepted external authenticators.

Service Identification And Authentication (IA-9)

The system administrator will configure the information system to uniquely identify and authenticate on system services and applications before establishing communications with devices, users or other services or applications.

Re-Authentication (IA-11)

The system administrator will require users to re-authenticate when organization-defined circumstances or situations require re-authentication such as when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed period of time or periodically.

Identity Proofing (IA-12)

1. The system administrator will configure the information system to:
    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.
    c. Collect, validate, and verify identity evidence.
    d. Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.
    e. Require evidence of individual identification be presented to the registration authority.
    f. Require that the presented identity evidence be validated and verified through methods as described in the Enterprise Architecture Standard: Enterprise Solution Architecture: Identity Access Management.
    g. Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.
    h. Accept externally proofed identities at organization-defined identity assurance level.

AUTHORITY

This policy and procedure is issued by the Virginia state forester.

INTERPRETATION

The director of information technology and the chief of administration are responsible for the interpretation of this policy and procedure.

APPROVAL

I certify that this policy and procedure is approved and ready for publication.

Parik Patel	DocuSigned by: Parik Patel 3448F7C5388F457...	6/10/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature	
Amanda Davis	DocuSigned by: amanda davis C2CCAB60F85A4A6...	6/27/2024
Chief of Administration Name (Print)	Chief of Administration Signature	

Version History

Version History			
Date	**Version**	**Details**	**Author/Contributors**
June 6, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO