**Identification and Authentication Policy Template**

# PURPOSE

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

This policy is intended to meet the control requirements outlined in SEC-501, Section 8.7 Identification and Authentication Family, Controls IA-1 through IA-8, to include specific requirements for the Commonwealth of Virginia.

# SCOPE

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

# ACRONYMS

CIO: Chief Information Officer

ISO: Information Security Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

VCCC: VITA Customer Care Center

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The identification and authentication program at “YOUR AGENCY NAME” is intended to ensure that necessary security controls are integrated into systems and processes within “YOUR AGENCY NAME”. This policy directs that “YOUR AGENCY NAME” meet the requirements as stipulated by COV ITRM Security Standard SEC501 and security best practices.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Process section. The following Roles and Responsibility Matrix describe 4 activities:

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Roles** | 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 |  | R |  |  | A |
| 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 SEC501, IA-1 through IA-8, all users of “YOUR AGENCY NAME” IT resources will be assigned a unique identity to securely authenticate to the systems that they have been authorized to access. “YOUR AGENCY NAME” will develop, disseminate, and review/update the Identification and Authentication Policy at least on an annual basis:

1. **Identification and Authentication (Organizational Users)**
2. The System Administrator will configure the information system to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

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

* 1. 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.
  2. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity.

1. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.
2. The System Owner ensures that all network-based access used to perform administrative functions on servers or multi-user systems employ two-factor authentication and are audited.

Note: Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection.

1. The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by an asset separate from the information system being accessed, for example using an external token-based device or client-based certificate.
2. **Identifier Management**
3. The System Administrator will manage information system identifiers for users and devices by:
   1. Receiving authorization from the ISO to assign a user or device identifier;
   2. Selecting an identifier that uniquely identifies an individual or device;
      1. The system administrator will assign user identifiers to ensure that no two users have the same identifier, to ensure user accountability.
   3. Assigning the user identifier to the intended party or the device identifier to the intended device;
   4. Preventing reuse of user or device identifiers for the period up to three years after the account has been deleted; and
   5. Disabling the user identifier after 90-days of inactivity.
4. **AUTHENTICATOR MANAGEMENT**
5. The ISO or designee will manage information system authenticators for users and devices by:

Note: User authenticators include, for example, tokens, Public Key Infrastructure (PKI) certificates, biometrics, passwords, and key cards (“smart cards”).

* 1. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
     1. The System Administrator will map the authenticated identity to the user account.
  2. Establishing initial authenticator content for authenticators defined by the organization;
     1. The System Administrator shall establish unique initial authenticator content for user and device authenticators.

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).

* 1. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
  2. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
     1. If a user knows or suspects that their password has been compromised, they shall immediately:
        1. Notify their supervisor,
        2. Report a known or potential security breach to the VCCC,
        3. Request the VCCC to reset or change their password or if self- service password mechanisms are used, immediately change their own password, and
        4. 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.).
  3. Changing default content of authenticators upon information system installation;
     1. 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).
     2. The System Owner shall confirm that software and/or hardware upgrades, updates, and patches have not reinstalled default passwords.
  4. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
     1. Passwords must have a minimum lifetime of 1 day(s) and a maximum lifetime of 90 days.
        1. Unless authorized by the System Owner, passwords cannot be changed in less than one (1) day.
        2. Authenticators must be changed at least every 90 days.
     2. Password reuse is prohibited for 24 generations.
        1. Password history must be set with a history of at least 24 passwords, so a user cannot quickly re-use a previous password.
  5. Protecting authenticator content from unauthorized disclosure and modification;
     1. Passwords (other than initial) must be chosen by users, not assigned by system administrators or help desk staff.
     2. Access to files containing passwords or password hashes must be limited to the IT system and its administrators.
  6. Requiring users to take, and having devices implement, specific measures to safeguard authenticators;
     1. Users shall protect authenticators by:
        1. Maintaining exclusive control and use of their passwords by not loaning or sharing authenticators with others,
        2. Protecting them from inadvertent disclosure to others,
        3. Posting or displaying passwords is prohibited, and
        4. Reporting lost or compromised authenticators immediately to their supervisor and the VCCC as a security event.
     2. Devices must be configured to safeguard authenticators (e.g., certificates, passwords).
  7. Configuring information systems, for password-based and PIN-based authentication, to enforce the following:
     1. Enforces minimum password, including initial password, complexity of:
        1. At least eight characters in length; and
        2. Utilize at least three of the following four:
           1. Special characters,
           2. Alphabetical characters,
           3. Numerical characters, and
           4. Combination of upper case and lower case letters.
        3. For internet facing web applications, the minimum password length must be 9 characters.
     2. Enforces password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum;
     3. Prohibits password reuse for 24 generations;
     4. Prohibits passwords and PINs from being displayed when entered;
     5. Requires that the IT system user change the initial/temporary password upon his/her first successful login;
     6. Enforces Account Lockout using the following parameters:
        1. The account lockout is enabled, the threshold is 10 invalid attempts, and the duration is at least 15 minutes.
        2. Accounts that are unused for 90 consecutive days must be disabled.
     7. Enforces password protected screen saver lock after a period of no more than 30 minutes of inactivity;

1. “YOUR AGENCY NAME” devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced.
   * 1. Encrypts passwords and PINs when stored and transmitted; and
        1. The transmission of identification and authentication data is prohibited without the use of acceptable industry encryption standards.
     2. Requires passwords with a minimum of four characters on smart phones or PDAs accessing or containing “YOUR AGENCY NAME” data.
        1. Passwords are required on mobile devices (i.e., PDAs and smart phones) issued by the agency. For mobile phones, use a pin with a minimum of 4 alphanumeric characters. The account lockout parameters (see Account Lockout Parameters section) must be applied as practical.
   1. Requiring that users be trained on password best practices, including:
      1. Passwords must not contain any of the following:
         1. Dictionary words (e.g., computer, work) or common names (e.g., Betty, Fred, Rover).
         2. Portions of associated account names (e.g., user ID, login name).
         3. Consecutive character strings (e.g., abcdef, 12345).
         4. Simple keyboard patterns (e.g., QWERTY, asdfgh).
         5. Generic passwords (i.e., password consisting of a variation of the word “password” [e.g., P@ssw0rd1]).
      2. At least 50% of total password content must be changed when a new password is created.
      3. Passwords must have no personal significance (e.g., names of spouses, friends, favorite sports, pets, hobbies and so on).
   2. Ensuring that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys;
      1. Passwords must not be included in any type of batch login file, clear text file, script or procedure. The use of an “auto-login” feature to automatically log a PC onto the network is strictly prohibited, unless the IT system is functioning as a kiosk.
   3. Requiring that forgotten initial passwords be replaced rather than reissued;
      1. Replacement passwords shall be created using complexity requirements set forth is this policy.
   4. Requiring passwords to be set on device management user interfaces for all network-connected devices; and
   5. Documenting and storing hardware passwords securely.
2. 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:
   1. Determine the appropriate validity period of the password, commensurate with sensitive and risk.
   2. Determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitivity and risk.
   3. 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.
      1. The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.
3. **AUTHENTICATOR FEEDBACK**
4. 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.
   1. 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.
5. The feedback from the information system must not provide information that would allow an unauthorized user to compromise the authentication mechanism.
6. **CRYPTOGRAPHIC MODULE AUTHENTICATION**
7. 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.
8. **IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**
9. 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).

Note: Non-organizational users include all information system users other than organizational users explicitly covered by statement of policy section A.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 01/13/2004 | Original |
| 2 | 08/13/2004 | For “YOUR AGENCY NAME” systems accessed via Web and systems without Web access, reduced history of the number passwords that must be retained for each domain user from 24 and 12, respectively, to 4. |
| 3 | 09/28/2007 | Substantive changes related to system sensitivity. |
| 4 | 06/11/2008 | In sections (C) and (D) the minimum age of a password was changed from 5 days to 1 day and the history of passwords retained was changed from 4 to 12 or more. |
| 5 | 03/01/2010 | Changes made to subsection 2.3.12 to be in compliance with the Information Security Standard – SEC501 (Revision 5) dated 8-11-2009 regarding password age. The format in this document differs from previous documents by decomposing the decimal numbering scheme to three places. |
| 5.1 | 09/27/2010 | Administrative changes. |
| 5.2 | 10/29/2010 | Administrative changes. |
| 6 | 01/22/2013 | Administrative changes. |
| 7 | 07/01/2014 | Complete rewrite of the Password Usage Policy based on Information Security Standard SEC501 Revision 8 with Role Matrix added. |
| 8 | 11/21/2021 | Formatting changes |