I. Policy Statement

User Authenticators provide for a secure authorization when access is needed to any University information systems by any Faculty, Staff, or Student. Proper management of these authenticators help to maintain secure and reliable connections within the University information systems.

II. Purpose

This control establishes the University’s policy for maintaining and managing information systems authenticators for users and devices.

III. Requirements

NSU manages information system authenticators for users and devices by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;

2. Establishing initial authenticator content for authenticators defined by the organization;

3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost-compromised or damaged authenticators, and for revoking authenticators;

5. Changing default content of authenticators upon information system installation;

6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);

7. Changing/refreshing authenticators at least every 90-days;
8. Protecting authenticator content from unauthorized disclosure and modification; and

9. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

10. Requiring passwords with a minimum of four characters on smart phones or PDAs accessing or containing COV data.

11. Requiring that forgotten initial passwords be replaced rather than reissued.

12. Requiring passwords to be set on device management user interfaces for all network-connected devices.

13. Documenting and storing hardware passwords securely.

When sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, NSU may:

1. Determine the appropriate validity period of the password, commensurate with sensitivity 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.

The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.

Supplemental Guidance: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The information system supports user authenticator management by University-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for
temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

**Control Enhancements for Sensitive Systems:**

1. The information system, for password-based authentication:
   a. **Enforces minimum password complexity of:**
      i. At least eight characters in length; and
      ii. Utilize at least three of the following four:
         1. Special characters,
         2. Alphabetical characters,
         3. Numerical characters,
         4. Combination of upper case and lower case letters;

         **Enhancement Supplemental Guidance:** This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does not apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

   b. Encrypts passwords in storage and in transmission;

   c. Enforces password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum; and

   d. Prohibits password reuse for 24 generations.

2. **NSU requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery.**

   **Enhancement Supplemental Guidance:** This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators for those components prior to delivery to the University. Unique authenticators are assigned by vendors and/or manufacturers to specific information system components (i.e., delivered information technology products) with distinct serial numbers. This
requirement is included in acquisition documents prepared by the University when procuring information systems and/or information system components.

3. NSU protects authenticators commensurate with the classification or sensitivity of the information accessed.

4. NSU ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

   Enhancement Supplemental Guidance: NSU exercises caution in determining whether an embedded or stored authenticator is in encrypted or unencrypted form. If the authenticator in its stored representation, is used in the manner stored, then that representation is considered an unencrypted authenticator. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

4. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

5. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.