Purpose:
To establish a standard for user account and password management. User authentication is a means to control who has access to an IT Resource. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to HSC.

References:
2. Standard GP0003.02: Information Classification.

Standard:
1. Shared accounts and passwords shall not be used. The Unit Information Security Manager may approve exceptions in the following circumstances:
   a. If multiple administrative accounts cannot be established, the account/password may be shared. In such case, procedures must exist for safeguarding the shared account/password.
   b. Multi use workstations/devices may have a generic account and password for access to the device only. Access to the network or application systems must have unique accounts and passwords that conform to this Standard.
      i. Multi use workstations must not have locally stored shared files containing Restricted or Sensitive information.
   c. When a shared account and password is the appropriate method for providing emergency access.
2. Accounts providing access to the network and accounts providing access to applications containing Restricted or Sensitive information shall have an automatic logoff feature that terminates an electronic session after a predetermined time of inactivity. Reasonable and appropriate alternatives may be used but the rationale must be documented and retained within the Unit.
3. Unnecessary pre-configured or default accounts that have generic or nonexistent passwords must be removed or changed.
4. Passwords to necessary default accounts must be changed before attaching the system to the network.
5. For situations involving the use of passwords as an authentication mechanism, UF HSC Units must adopt a password configuration reflective of the nature of the information or information resource accessed (see Standard GP0001: Information Classification).
   a. Passwords must be safeguarded.
   b. Passwords must have an expiration schedule.
   c. Passwords must not be shared except in circumstances specified in 1 above.
6. Stored passwords shall be encrypted or otherwise safeguarded.
7. Users must not circumvent password entry with auto logon, use of applications remembering passwords, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (such as automated backup or single sign-on) with the documented authorization of the Unit ISM. In order for an exception to be approved there must be a procedure to change the password.
8. Login banners (http://www.ciac.org/ciac/bulletins/j-043.shtml) shall be used where technically feasible.

**Guidelines:**

1. All passwords, including initial passwords, should be constructed and implemented according to the following HSC guidelines:
   a. All initial passwords for user accounts should require the user to change it to a private value at the initial login.
   b. Passwords should be at least 6 characters/numbers in length and contain at least three of the four character sets (alpha, numeric, symbol and shift characters).
   c. Passwords should not be anything that can easily be associated with the account owner such as: user name, social security number, nickname, relative’s names, birth date, etc.
   d. Passwords should not be dictionary words or acronyms.
   e. Reuse of a password in fewer than eight changes should be prevented when possible.
   f. User account passwords should not be divulged to anyone.
   g. In the event a system administrator must open an account, the system administrator should change the password such that the account owner will know that his account has been accessed. If the account is to remain active, the system administrator should notify the account owner as soon as practicable of the change and reset the password to an initial value and state requiring the user to re-store it as a private value at their next login.

2. Passwords should be resistant to computer programs that check previously used
passwords or easily compromised passwords.

3. All Administrator Special Access account passwords should:
   a. Be at least 8 characters long.
   b. Be changed at least every 90 days.
   c. Have a unique password, different from all other accounts held by that user.

4. All user account passwords should be changed at least every 180 days.

5. Passwords should not be inserted into non-secure electronic communication.

6. Application owners are responsible for implementing the password policy for the associated application.

7. Whenever possible, automatic password aging should be enforced.

8. Password change procedures should require user authentication.

9. Technical staff with administrative right must not circumvent the User Account and Password Management Policy for the sake of ‘ease of use’.