S-6 Security SOP - User Accounts

4–12. Password control
b. The IAM or designee will manage the password generation, issuance, and control process. If used, generate passwords in accordance with the BBP for Army Password Standards. (AR 25-2, 24 Oct 2007)

h. **IAMs and SAs will remove or change default, system, factory installed, function-key embedded, or maintenance passwords**. (AR 25-2, 24 Oct 2007)

k. SAs/NAs will conduct weekly auditing of service accounts for indications of misuse. (AR 25-2, 24 Oct 2007)

Unit Password Security Standard Operating Procedures:

1. All system or system-level passwords and privileged-level accounts (e.g., root, enable, admin, administration accounts, etc.) will be a minimum of 15-character case-sensitive password changed every 60 days.

2. All user-level, user-generated passwords (e.g., email, web, desktop computer, etc.) will change to a 14-character (or greater) case-sensitive password changed every 60 days.

3. Password history will be set to a minimum of 10.

4. Set the Observation Window for Account lockout settings to no more than 60 minutes. Set the LockoutDuration setting (also known in Group Policy as the Account lockout duration setting) to 0 and the LockoutThreshold setting (also known in Group Policy as the Account lockout threshold setting) to 3. This allows no more than two unsuccessful logon attempts within a 60 minute period and requires a system administrator to unlock the account.

1. When supported, enable that system capability to notify the user of last successful and unsuccessful logon time and date. Users will notify administrative and security personnel when discrepancies are identified.

2. The password will be a mix of uppercase letters, lowercase letters, numbers, and special characters with a minimum of characters as follows:

- Contains at least 2 uppercase characters: A, B, C etc.
- Contains at least 2 lowercase characters: a, b, c, etc.
- Contains at least 2 numbers: 1,2,3,4,5,6,7,8,9,0
- Contains at least 2 special characters, i.e. ! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , . /

Passwords will not have the following characteristics:

Is a word found in any dictionary, thesaurus, or list (English or foreign)

Is any common usage word or reference such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Common words such as; "sanjose", "sanfran" or other derivative.
- Birthdays, addresses, phone numbers, or other personal information.
- Word or number patterns like; aaabbb, qwerty, mypassword, abcde12345.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- Social security numbers (SSNs).
- USERID
- Military slang, acronyms, or descriptors or call signs.
- System identification.

WINDOWS SERVICE ACCOUNTS:

3. Verify the use of AT LEAST a 15 character password for all Windows Service Accounts.

4. Windows Service Account passwords manually generated and entered by an administrator should be changed yearly or upon loss of system administrator that had knowledge of password, whichever is earlier.

Windows Service Account passwords randomly generated and automatically entered into systems do not have to be changed as frequently.

1. Many Windows Services do not require accounts to operate effectively. System implementations should minimize usage of Windows Service Accounts unless required. As legacy applications are upgraded to current COTS versions that do not require Windows Service Accounts, this should be accounted for during system implementations.

2. Privileged-level account passwords will differ from their normal-user account passwords.

Share authenticators only when required for trusted operations or authorized; such as group helpdesk accounts, network operations, or watch-standing environments, when alternative logging measures are implemented.

3. Stored password mnemonics files on ANY computer system (including Palm Pilots or similar devices) utilize NIST certified AES encryption (non-reversible) with at least a 128 bit key.

4. All temporary passwords issued must be expired immediately when input, forcing the user to choose another acceptable password known only to the user before the logon process is completed

5. If any account or password is suspected of having been compromised, report the incident to the SA/NA immediately. SA/NA will report account compromises to the IA personnel chain, the chain of command, the Installation DOIM, and the appropriate RCERT supporting your organization. Change all account passwords when directed; from a known secure system. Do not use your computer system until an investigation has been completed and the system has been rebuilt from the compromise.

6. If a privilege-level account has been compromised by an intruder, all passwords on that system will be immediately changed, and the privileged account disabled on the entire network until completion of the forensic investigation. Consideration must be given to the credibility of any and all accounts created within the suspected time frame, and all user accounts should be considered compromised. Re-issuance of new passwords or accounts may be required.

7. Users and supervisors are responsible for notifying SAs or IAMs when an individual's access is no longer required. User access will be terminated within 1 day following notification that a user no longer requires access to any IS. Any group account authenticators for which a departing individual had access will be changed immediately.

8. SAs will disable user accounts immediately upon identification of unauthorized activity by the user or the user notifies SA personnel that the account is being used illegally.

9. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "TheTrafficOnTheI95WasMiserableThisMorning"

All of the rules above that apply to passwords apply to passphrases.

10. SA/NAs will perform password cracking or guessing on a quarterly basis with Command authorization within their authority when passwords are used as the authenticator. If a password is guessed or cracked during one of these scans, the user will be required to change it. Never attempt to audit password files on an operational network.

11. Manage, enforce, and audit all account passwords, permissions, inactivity, and suspension policies.