

PASSWORD CONTROLS

A. User Requirements

- (1)** A user ID and password combination may be considered a legal signature and the user may be held accountable for any system activities that occur against it. Users are prohibited from sharing or disclosing their IDs and passwords with other individuals. It is the user's responsibility to protect passwords from loss or disclosure and to change it in accordance with system guidelines.
- (2)** Users are prohibited from attempting to access information in a system beyond the level to which they have been authorized.
- (3)** Users should change passwords frequently and at least every 90 days. When changing a password, at least two characters must be unique. Reuse of the same password with a different suffix (such as 1, 2, 3) is not permitted.
- (4)** Users should immediately notify their IITSMs and appropriate system administrators if they suspect that their passwords have been compromised.
- (5)** Users should choose passwords that consist of a minimum of eight characters, at least two of which must be non-alphabetic characters. Common items like names, birthdays, etc. should be avoided.
- (6)** Generic user IDs like "Admin" or "Temp" are prohibited under all circumstances. Other generic IDs are permitted for circumstances related to business reasons, such as an office with a high turnover of daily volunteers. All such exceptions must be documented in writing by the local manager, who accepts the associated risk and must ensure that complete audit logs showing who had access to those IDs on specific days and times are maintained.
- (7)** Generic passwords like "default" are prohibited.
- (8)** Scripts that allow user access to servers or automated information systems by automatic password entry are prohibited.

B. System Controls

- (1)** Use of group IDs may only be used under extremely limited circumstances. If group IDs are used, managers must submit written documentation to the BITSM identifying the reason for the use of group IDs and full explanation why the use of individual user IDs is not possible or practical.
- (2)** Initially assigned passwords should not be generic words like "default" nor any other standard string.

- (3) Systems should require passwords to consist of at least eight characters, at least two of which must be non-alphabetic characters.
- (4) Systems should force password changes at least every 90 days and prevent reuse of passwords for at least 8 changes. System Administrator passwords will be changed every 60 days. Passwords may not be reused until 180 days have passed since their last usage.
- (5) An account will be locked out after three consecutive failed password entries and can only be cleared by the IT Security manager or his/her delegated authority.
- (6) A password will be disabled immediately upon written notification from management that the person no longer requires access.
- (7) Passwords for contractors and others working on temporary details should be issued for specific time periods and be disabled thereafter.
- (8) Passwords are considered to be sensitive information and should be protected. Unencrypted password files are prohibited.
- (9) Systems should include audit logs that capture information about attempts to login by unauthorized users, or login as some other user, or to gain access to information outside the scope of granted access. Network administrators and/or IITSMs should monitor audit logs frequently and report unusual action as necessary to the BITSM.