Password configuration process checklist (section 3.6.4)
Account Management #3 & #4

March 31, 2011

The left column indicates whether the standard is listed in the Information Security Plan as a **M**ust or **S**hould. A justification must be written for any standard not followed in the department procedures. The justification must be approved by the IT Manager for items listed as a **S**hould and also reviewed with the IT Security Office if the item was listed as a **M**ust. The IT manager must review, sign and date, all exceptions every six months to indicate that the exception is still necessary.

M/S	Item	Y/N
S	1. Document process for technical configuration of all operating system and application accounts managed by the department. a. Include password creation settings. b. Include password expiration settings every 90 days or semester. Document any exceptions to this standard. c. Include password reuse settings. d. Include account lock out settings. e. Include password reset procedures (automatic and manual). Which includes proper identification of the individual, strong temporary password unique to each reset and unpredictable, forced password change by individual to password they select. f. Include any procedures to test account passwords by system administrators.	
S	2. Document instructions to users not to share passwords.	
S	3. Document exceptions for account sharing (such as read only lookup accounts), assignment of the shared account and regular password changes for the account.	