Account Management #1 checklist (section 3.6.1)

Excludes 3.6.1.3

July 6, 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
M	1. Account creation and maintenance according to authorized process	
M	a. Creating and assigning accounts	
M	b. Accessing another user's account(s)	
M	c. Reviewing, disabling, reassigning, or deleting accounts	
M	2. Passwords uniquely associated with user	
M	3. Passwords not shared	
S	4. Managers not request user passwords	
S	5. Accounts have only privileges/permissions to achieve job function/responsibility	
S	6. Privilege users also have standard user account for non-admin use	
S	7. Privilege accounts also uniquely associated with user	
M	**8. Privileged accounts must be reviewed and re-approved annually**	
M	9. Pre-created accounts (generic) are assigned to manager to reassign as needed	
M	a. User assigned account must choose password	
M	b. Manager change password when released from use	
M	c. Manager document assigned user, dates, and times for account	
S	10. Read only group accounts can have a longer password expiration period	
M	11. Shared accounts reviewed & re-approved annually	
M	12. Generic accounts justified/approved by IT manager	
M	13. Accessing someone else's account approved by manager	
M	a. Change password first	
M	b. AVP's of Faculty Affairs & Administration approve access without user notification	