Account Management #2 checklist (section 3.6.2)

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
S	1. Managers notify users about account usage (not system accounts)	
M	a. Keep password confidential	
M	b. Not access another user account	
M	c. Not embed password into programs	
M	d. Secure passwords that are written down	
S	e. Schedule resource-intense job off-peak hours	
S	f. Used for University-related activities	
S	g. Authorized software installed with account	
S	i. Not include peer-to peer	
S	ii. Not include personal software (screen savers, games, utilities)	
S	iii. Not include instant messaging	
S	2. User accounts auto password lock in 15 minutes or less inactivity	
S	3. Admin users confirm account usage	
S	a. patch/update desktops within 2 days of release	
S	b. Not install unauthorized software	
S	c. Browse trusted sites	
S	d. Use secure protocols when connecting to servers	
	4. Special privileged accounts (root, admin, power user, enable, oracle, etc.)	
S	a. Avoid direct login (sudo, run as)	
S	b. Password changed every 3-6 months or immediately for terminated/separated employee	
S	c. Not auto lock console login	
S	d. Auto lock remote access	
M	e. Reviewed annually and re-approved	
S	5. Default accounts (guest, etc.) disabled, password changed, login disallowed	