The Information Classification Standard implemented checklist (section 3.1.2) DT/LT/Mobile Device Security #1

December 5, 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. At least three times a year review authorized access to Protected level 1 information.	
M	2. Each Manager providing access to PL1 information will review the memo "Determining access to Confidential Data".	
M	3. Each Manager proving access to information collected by their department will provide to their Associated Dean/Vice President:	
M	❖ List of employees they have given access to PL1 information (electronic and non-electronic).	
M	❖ Employee RedID.	
M	❖ Location of information (desktop, server name, file cabinet location, etc).	
M	❖ With a justification for access tied to the employees job duties.	
M	❖ Summary of information in a spreadsheet or table in a memo.	
M	❖ List of employees who have not completed CSU Security Awareness training (compare training report with list of employees with PL1 access).	