Laptop full disk encryption checklist (section 3.3.1)

DT/LT/Mobile Device Security #6

May 4, 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. Storage of PL1 information approved by the employee's Vice President or Dean	
M	2. Full disk encryption versus folder encryption	
S	3. Commercially supported version of full disk encryption	
S	4. FIPS-140 approved algorithm: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm	
S	5. Key escrow used select/store/recover passwords	
	6. Password/keys selected according to section 3.6 that are applicable:	
M	a. Unique to each laptop	
M	b. Modified when transferred to new user	
M	c. User reminded to keep confidential	
S	d. Passphrases or two factor	
M	e. Minimum 8 char with upper/lower alpha, digits, symbols	
S	f. Expire every 90 days/semester	
S	g. Not reusable	
S	h. Reset for laptop user only	
	7. Password/keys handled according to PL1 standards (Table 3-1):	
M	a. Attended at fax	
M	b. Encrypted during transmission	
M	c. Encrypted in email	
M	d. Not stored on personal computer	
S	e. Encrypted in database	
M	f. Encrypted on laptop	
S	g. Encrypted on key server	
M	h. Secured if stored in paper/electronic media	
M	i. Shredded for paper disposal	
M	j. Shredded/overwritten for media disposal	
M	k. Labeled as PL1 in any documents/media/container	
M	l. Left on password protected voice message	
M	m. Discussed verbally in private area	
M	n. In sealed container labeled "Confidential" if sent in campus/postal mail	
S	8. Password/key recoverable if forgotten or lost	