Application Security #1, #2, & #3 (section 3.1.1 & 3.7.1)

February 1, 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.

Protected Level 1 data consists of:

a. Account passwords or credentials.
b. PINs (Personal Identification Numbers).
c. Private key (digital certificate).
d. Name with credit card number.
e. Name with Tax ID.
f. Name with driver's license number, state identification card, and other forms of national or international identification.
g. Name with birth date combined with last four digits of SSN.
h. Medical records related to an individual (including disability information).
i. Psychological counseling records related to an individual.
j. Name with bank account or debit card information with any required security code, access code, or password that would permit access to an individual's financial account.
k. Name with personally identifiable information:
   - Mother's maiden name.
   - Employee net salary.
   - Employment history (including recruiting information).
   - Biometric information.
   - Electronic or digitized signatures.
   - Names of parents or other family member.
   - Birthplace (city, state, country).
   - Race and ethnicity.
   - Gender.
   - Marital status.
   - Personal characteristics.
   - Physical description.

M/S	Item	Y/N
M	1. For applications containing protected level 1 or mission-critical information, managers must ensure that the software development process is documented and approved before implementation.	
	2. Requirements Analysis:	
M	❖ IT support staff need to be able to state not only what the system should do but also what it should not do.	
S	❖ Specific security objectives need to be defined and translated into concrete requirements	
M	3. Design: The priority in the translation of requirements to application functionality is to ensure the incorporation of security principles	
M	❖ FIPS-140 approved algorithm for encryption.	
S	❖ Password key strength for encryption processes selected and changed	

	according to section 3.6	
S	❖ Key escrow including secure storage and recovery if key is lost or forgotten	
S	❖ Use of secure network protocols (such as IPSec, SSL, or Secure RPC)	
S	❖ Mechanisms for authentication and access control	
S	❖ Mechanisms for implementing the rules for all forms of information input and interaction	
	4. Implementation: controls need to be in place to catch improper implementation procedures	
S	❖ Error handling	
S	❖ Coding standards available to all developers	
S	❖ Input validation	
S	❖ Cross check code and unit testing	
S	❖ Prioritize defects and assign timelines for rewrite/retest	
	5. Testing: focused on what should not happen	
S	❖ Attention to the software's operating environment (network connections, configuration, and customized set up) as well as the functional testing of security components	
S	❖ Look for functionality that should not be there, such as unintentional side effects and behaviors that are not specified in the design or implementation test plans.	
	6. Deployment: Special attention to the software's operating environment (network connections, configuration, and customized set up)	
S	❖ Use security checklists to review configuration files	
S	❖ Review enabled services and open ports	
S	❖ Review access to sensitive files and directories	
S	❖ Ensure that logging is enabled for forensics and incident response	
	7. Maintenance: review proposed changes in terms of risks that they impose on the overall security of the system, and maintain documentation tracing back to the appropriate configuration management process.	
S	❖ Changes required be validated and verified through the Implementation, Testing & Deployment cycles	
S	❖ Change management procedures can be used to track & document changes	
S	❖ Consider a consulting company to perform code checks for potential vulnerabilities	
	8. Commercial or legacy systems	
S	❖ Ensure that IT support staff investigate security issues with implementation of commercial-off-the-shelf (COTS) software prior to procurement	
S	o Who will have access to the system and in what capacity	
S	o How the system will be used	
S	o Will the system contain protected information	
S	o What are potential threats to the system or system information	
	❖ IT support staff research security implementation of the COTS software	
S	o http://security.sdsu.edu/iso/pdfs/App_Attacks_and_Countermeasures.pdf	
M	o Not using default passwords	
S	o Securely configuring file and access permissions	
S	o Shutting down unneeded services	

	❖ IT Manager analyze the results of the security research and identify controls and countermeasures that may be required to lower risks	
M	o Contact the TSO if the assessment involves protected level 1 information	
S	o Ensure that the final controls and configurations are appropriately documented in the system/application build documentation	