Server Logging & Review checklist (section 2.8.2)
Server Security #4

June 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 Should 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. Retained for one year (locally, centrally, or on backups)	
M	2. Enable OS and application logging	
M	3. OS and application log successful/failed logins, password changes, anti-malware results	
M	4. Servers log root/admin privileged activity	
S	5. Critical servers copy logs sent to remote server	
S	6. Database applications log successful/failed login & privilege use	
S	7. Database servers with PL1 sent to centralized logger	
M	8. IT Managers ensure written log review procedures that document	
	a. Who reviews, how often, which logs	
S	b. Log retention	
S	c. Frequency of log reviews	
S	d. Alert process for suspicious events	
S	i. Login/logout outside of work hours	
S	ii. Login/logout suspicious sites	
S	iii. Attacks initiated by SDSU IP addresses	
S	iv. Other anomalies	