Patch Management process checklist (section 3.2.1 & 3.4.2)
Information Security #1

March 2, 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
M	1.	Include all forms of software revisions (patches, upgrades, hot fixes, and config changes)	
M	2.	Include all operating systems & standard applications	
M	3.	Include inventory of all systems (including desktops and laptops) (see contents 3.2.1.1)	
S	4.	Centralized due to volume	
S	5.	Meetings with IT Manager to discuss (as applicable) vulnerabilities, patch size, network throughput, system limitations, tools, special requirements or restrictions (at least monthly)	
	6.	Patch windows (Patch Tuesday for Microsoft, etc.	
	7.	Patch dependencies & special installation	
M	8.	Subscribe to sdsu-cert mailing list, and other notification mailing lists	
M	9.	Subscribe to vendor mailing list for vulnerability announcements	
S	10.	Daily review of vulnerability emails	
S	11.	Deployment schedule of patches (immediate if announced on sdsu-cert, within a day for remote exploit, otherwise within a week)	
	12.	Deployment hierarchy (test & then to all systems, or additionally tiered approach) See Samples 3.2.1.2	
S	13.	Check services after deployment to ensure no changes to configuration	
S	14.	Throttle deployment to minimize affect on the patch server	
M	15.	Derive optimal/maximum deployment sizes/rates to desktops	
S	16.	Auto updates for laptops/mobile devices (checking twice a day)	
M	17.	Review logs on patch server for errors	
S	18.	Patch recovery/rollback	
S	19.	Reporting	
S		❖ List of patches deployed since last report	
S		❖ List by computer of missing patches	
S		❖ Issues or concerns	
S		❖ Exceptions (signed by manager, reviewed every six months)	