Network Security #1 checklist (section 3.10.2 & 3.10.3)

November 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
S	1. Internal firewalls should be implemented for systems and networks that contain protected information or have privileged access to protected information.	
M	2. A complete firewall ruleset and system document must be in place before servers are placed into an internal firewall zone	
S	3. For firewall implementation details, visit: http://security.sdsu.edu/services/firewall/internal.html.	
M	4. IT support staff must have change management documentation for firewall rule requests.	
S	5. For firewall rule requests visit: http://security.sdsu.edu/services/firewall/rulesets.html	