Information Security
Patch Management Guidelines

Summary
Fresno State is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems. IT staff of the university provide appropriate protection against malware threats, such as viruses, trojans, worms, and software bugs which could adversely affect the security of university managed systems or the data entrusted on those systems. Effective implementation of this patch management procedure will limit the exposure and effect of common malware threats and vulnerability exploitation to the systems within this scope.

Scope
All individuals performing the roles of system, network or application administrators managing university managed services and systems. This procedure also applies to contractors, vendors and others managing such services and systems.

This procedure covers all university managed computers, servers, systems, applications and the network infrastructure.

This procedure is primarily for system, network or application administrators and technical staff, including Technology Services' staff who are responsible for the ongoing maintenance of services and systems. The scope also extends to anyone else who is similarly undertaking activities governed by this procedure.

Patch Management Procedures
All university managed computers, computer systems, computer networks and electronic communications devices must be updated with the latest but stable patches released by the respective vendors:

a. A system administrator or team must be identified for the overall patch management of each system, application or device.

b. Those responsible for each system, device and application must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

c. The system administrator or team is responsible for identifying and rectifying failed patch deployments. Compliance with approved patches must be verified at least on a weekly basis.

d. Patches must be obtained from a known trusted source.

e. The integrity of patches must be verified to ensure the patch obtained is the correct and unaltered patch.

f. Patches must be assessed before implementation in a production environment to ensure that there is no negative impact as a result.

g. A backup of the production systems must be available before applying any patch.

h. An audit trail of all changes must be created and documented. The system administrator must verify that the patches have been installed successfully. Patching must remove obsolete or multiple software versions.

i. System administrators on university sponsored systems that manage the security of their own systems are required to use patches in accordance with this procedure.

Patching Priority
Patches must be deployed, as per the below-mentioned category classification from the time of the patch being released:

	Patch Level Classification / Definition			
	Critical	**High**	**Medium**	**Low**
Internet Facing System (server, application, etc.)	3 days	7 days	Next Maintenance Window	Next Maintenance Window
Non-Internet Facing System (server, desktop, application, etc.)	7 days	30 days	Next Maintenance Window	Next Maintenance Window
Laptops / Desktops	10 days	14 days	Next Maintenance Window	Next Maintenance Window
Network Devices	14 days	30 days	Next Maintenance Window	Next Maintenance Window

Exceptions
Systems and devices which are not patched via the centrally managed System Center Configuration Manager (SCCM) or JAMF (i.e., Casper Suite) must be patched as per the section on patching priority. Where this is not possible, exceptions must be obtained from Information Security and/or the Chief Information Officer and appropriate compensating controls must be implemented to mitigate the risk. Failure to align with this procedure may result in the affected device or service being removed from the university network.

Patch Enforcement
Implementation and enforcement of this procedure is the responsibility of system administrators. The IT Security team will conduct random external and internal vulnerability assessments to ensure compliance with this procedure. Any system found in violation of this procedure shall require corrective action.

Monitoring and Reporting
All system administrators and teams responsible for the administration of systems defined within the scope above are required to maintain monthly reporting metrics that summarize the outcome of each patching cycle. These reports shall be used by IT Security to evaluate the current patching levels of all systems and to assess the current level of risk.

Definitions

Patch Rating Critical: A vulnerability whose exploitation could allow code execution or complete system compromise without user interaction.

Patch Rating High (Microsoft rating Important): A vulnerability whose exploitation could result in compromise of the confidentiality, integrity or availability of university data or recourses.

Patch Rating Medium (Microsoft rating Moderate): A vulnerability whose impact is mitigated by existing information security controls.

Patch Rating Low: A vulnerability that is unlikely to be able to be exploited.