Standard: Application Patch Management

Effective Date:	2019.05.26
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Director, Information Security and Compliance
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The Application Patch Management Standard describes the acceptable standards to ensure the security and integrity of university information and information technology resources by patching software installed on IT Support managed servers and workstations.

Who/what does the standard apply?

The requirements in this standard apply to all university owned servers and workstations.

Definitions

- **Baseline**: Outlines the minimum patch definitions that must be applied
- **IT Support:** All staff in a unit or faculty who are responsible for maintaining computer systems and hardware, and for making decisions pertaining to those systems.
- **Out of Band patching:** An out-of-band patch is a patch released at some time other than the normal release time
- **Workstation:** Specialized computers that operate within a client/server architecture to serve the requests of client computers on the network.

Compliance

The patching of IT Support managed servers and workstations must align to the requirements and specifications outlined within this standard. Where systems and applications are unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

Requirement	Specifications
Workstations and Servers will be patched to the IST baseline for each application.	IST will establish an application version baseline for workstations and servers. The baseline will be determined on a quarterly basis.

Application patches must be deployed according to the prescribed conditions	Monthly – consisting of cumulative patches for the month Quarterly – consisting of cumulative patches for that quarter Critical – this will be out-of-band patching for critical patches
New workstations and servers or re-imaged workstations and servers must meet the minimum baseline	All new workstations or re-imaged workstations must be brought up to the baseline or a higher patch level prior to deployment.
Patches must be deployed using a formal process	Patching is conducted in accordance with an approved and documented process.
Deferred Schedule	Patching for applications may be deferred to the following quarter if there is no desired enhancements or bug fixes that affect the proper functioning of the application; or the CVE scores for known vulnerabilities are Low (0.1-3.9) or Medium (4.0-6.9).
Information Security Recommendations	Information Security may advise that patching occurs more frequently than the prescribed conditions if the CVE scores are High (7.0-8.9) or Critical (9.0-10.0).

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Server Patch Management Standard	Workstation Patch Management Standard