FLORIDA	**OFFICIAL**
POLYTECHNIC	**TECHNOLOGY SERVICES**
UNIVERSITY	**STANDARD**

Subject/Title: Technology Services Patch Management Standard
Date Last Revised: 2019.12.24
Responsible Division/Department: Technology Services
Initiating Authority: Ben Beachy, Chief Information Officer

STANDARD OWNER

This standard is owned by the University Chief Information Officer.

STANDARD PURPOSE

This standard is to ensure that information technology systems used by the University are managed, updated and patched to reduce risks to the confidentiality, integrity, and availability of University data. This standard describes expectations for IT staff, University employees, and contractors.

STANDARD SCOPE

This standard applies to all information technology systems used for official University business. An information technology system is a combination of software, hardware, storage, telecommunication, and/or automated processes that generate value for the University.

STANDARD CONTEXT

Florida State law and FPU-1.0123P – University Public Records require that most University records be made available to public inspection. This legal requirement effectively dispenses with concerns for the confidentiality of public University records. Integrity and availability remain pertinent concerns, however; as does the confidentiality of those few records exempted from public disclosure. The requirements of this standard reflect this regulatory context.

STANDARD REVIEW

This standard must be reviewed at least once annually by the standard owner. It may be modified at any time by the standard owner. Any changes to this standard will be promptly reviewed with affected employees.

STANDARD

Patches

Patches are updates to information technology systems that address information security risks: system bugs and vulnerabilities. Patches are created, tested, and distributed by software vendors or, in rare cases, by technology services staff.

Changes that add or alter systems beyond what is necessary to address bugs and vulnerabilities are not considered patches—these must be deployed consistent with our current change management practices (FPU-TS Change Management Standards).

Patches must be applied as soon as practical, except as noted below. To this end, patches are exempt from change management requirements (FPU-TS Change Management Standards) except requirements for rollback and logging. Other change management requirements, particularly testing, should be practiced when they do not unduly delay patch deployment.

Vendor-managed systems

Where practical, the University transfers patch management responsibility to vendors managing Software as a Service (SAAS) or on-premises systems. These vendor's policies and practices are evaluated consistent with our current risk management practices. The details of vendors policies and practices must be maintained by the vendors and must be made available to the University upon request.

For workstation operating systems

University employees must be prompted to install operating system patches when they are released by the vendor:

- A testing group of employees must receive updates immediately upon release and must install them within three calendar days.
- All other employees must receive updates two days after release and must install them within seven calendar days.

Exceptions to this schedule may be made to address vulnerabilities actively being exploited within the University.

For workstation information security systems

Technology services staff must configure workstations to automatically receive updates to anti-virus software and other information security systems immediately after those updates are released by the vendor.

For other workstation systems

Technology services staff must monitor vendor communication and public vulnerability notifications to identify needed security patches.

University employees may request upgrades to workstation software for reasons other than information security. These requests must be evaluated consistent with our current risk- and change-management practices (FPU-TS Risk Management Standard; FPU-TS Change Management Standard).

For networking and telecommunications systems

Technology services staff must monitor vendor communication and public vulnerability notifications to identify needed patches.

For server operating systems

Servers must be configured to automatically download and install operating system updates when they are released by the vendor. To minimize disruption to operations, servers should be configured to reboot when necessary outside normal business hours.

For server software systems

When practical, servers must be configured to automatically download and install software updates when they are released by the vendor. To minimize disruption to operations, servers should be configured to restart services when necessary outside normal business hours.

When automatic updates are not practical technology services staff must monitor vendor communication and public vulnerability notifications to identify needed patches.

For computing classrooms and computer labs

Technology services staff must update computing classroom and computer lab systems at least twice annually. Technology services staff should work with faculty to determine the security and functional patches that need to be applied with each update—avoiding disruption to instruction and research. Computing classroom and lab computers must be configured to restore a fixed configuration after every reboot—i.e. must be ‘frozen’.

Exceptions to this schedule may be made to patch vulnerabilities actively being exploited within the University.

University employees may request upgrades to computing classrooms and computer labs for reasons other than information security. These requests must be evaluated consistent with our current risk- and change-management practices (FPU-TS Risk Management Standard; FPU-TS Change Management Standard).

RESPONSIBILITIES

Technology systems is responsible for patching systems to address information security risks and functional changes, except where such responsibility has been transferred to SAAS vendors (see above).

University employees outside technology services may be responsible for patching systems to address functional changes when these systems are not centrally managed and have been evaluated to have low intrinsic information security risk.

CHANGES

2019.12.24 Ben Beachy. First version.