UTSA Institutional Compliance
Office of Information Security

OIS 26 – Standard for Patch Management

I. STANDARD STATEMENT

This standard describes general principles addressing the appropriate testing and installation of operating system patches. Information Security Administrators, Information Technology Associates and others who manage servers and workstations are responsible for the maintenance of security patching on those computers.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. Microsoft, Apple and most other workstation and desktop operating system vendors routinely issue software updates. Security updates published by operating system vendors must be deployed within 30 days of their release if published within the vendor's patch release cycle, and within 15 days if published via an out-of-cycle update. If the patch addresses a critical time-sensitive issue, University Technology Solutions (UTS) will notify the departmental IT staff to install the patch immediately.

B. UTS will install the updates to the servers and workstations it manages. Departmental IT staff and end users are responsible for installing the updates to their computers. A period for testing is recommended for any patches received; pertinent procedures and guidelines can be found on the Information Security Website.

C. This standard is closely related to the Standard for Configuration and Asset Management.

Title: OIS 26 – Standard for Patch Management
Effective Date: January 5, 2012
Last Revised: August 3, 2020