UTC-S-IT0135 – UTC System & Information Integrity Standard

Objective:
To align University of Tennessee at Chattanooga (UTC) standards of practice with University of Tennessee System-wide policy for developing, maintaining and documenting a System & Information Integrity (a.k.a. Patch Management) program.

Scope:
This program applies but is not limited to employees, contractors, agents, and representatives accessing, using, or handling UTC information technology resources.

Principles:
This document is a UTC-specific Standard based on University System-wide policy. Each User of UTC resources is required to be familiar and comply with University policies, and acceptance is assumed if the User accesses, uses, or handles UTC information technology resources.

The Chief Information Officer (CIO) is the Position of Authority (POA) for Information Technology at UTC and responsible for IT security at the University of Tennessee Chattanooga.

Responsibilities:

1. The CIO has overall responsibility of the System & Information Integrity (SI) program at UTC and ensures:
    a. The program is developed, documented, and disseminated to appropriate UTC entities in accordance with University policy.
    b. The program is reviewed and updated annually.
1. The Chief Information Security Officer (CISO) is responsible for overseeing the implementation of the SI program and consults system owners to ensure effective procedures are established addressing the patching of UTC information systems.
2. System administrators are responsible for developing department-level procedures for their respective system(s).

Standard:

1. All business systems supporting mission-essential functions are included in UTC's System & Information Integrity program.
2. The IT Security Team must employ the appropriate/approved industry standard tools and techniques for Patch Management.
3. All system owners/administrators must:
    a. Regularly monitor and assess IT systems for flaws and malware, and address issues in a timely manner.
    b. Apply relevant software and firmware updates at the earliest appropriate maintenance cycle.
    c. Employ current malicious code protection and alerting mechanisms.

    d. Ensure appropriate and adequate records and logs are maintained in accordance with applicable federal and state laws, and University policies, standards, and requirements.
4. **Banner System** administrators must ensure:
    a. Banner Applications are upgraded minimally twice as year (fall and spring) to stay current with releases from the manufacturer.
    b. Additional patches/upgrades may be applied outside the two main upgrade periods as new functionality is requested by the functional offices, bug fixes are needed, or Financial Aid processing requirements are released.
    c. All patches/upgrades are applied to test systems first, and once approved they can be scheduled for move into the production environment.
    d. Banner Databases are patched as maintenance windows/testing cycles allow after security patches are applied to the operating system for each version, and whole versions are implemented as required by Banner Applications, and the support agreements and warranties for those applications.
5. **Data Center** administrators must ensure:
    a. Production servers are patched in a timely manner using vendor supplied patches.
    b. Windows development and testing servers are set to download and install vendor patches automatically.
    c. Departmentally-owned servers in the Data Center are maintained by their owners.
6. **Networking** administrators must ensure:
    a. Network device operating system patches applied once a month if available.
    b. Network application-specific updates are applied once every 6 months unless there is an announced vulnerability in the current version being used.
    c. Vendor supplied appliance patches are evaluated and/or applied every 6 months when bugs are fixed and critical vulnerabilities are announced.
7. **End-user** patch management. Client Services must ensure:
    a. Managed endpoints are assigned to an endpoint protection policy.
    b. Managed workstations will download and install the appropriate endpoint protection software.
    c. Endpoints are evaluated cyclically, and antimalware definitions are updated daily based on the endpoint Protection policy.

References:
UT Policy IT0135 – System and Information Integrity