



Operating Systems and Application Services Patch Management

Purpose

To define the procedure for the application of patches and updates for information resources.

Scope

This procedure applies to University of North Texas System Administration and Institutions. Failure to follow these procedures could result in removal of the information resources from network or other disciplinary action referenced in the UNT System Information Security Regulation.

Procedure

1. Industry best practices should be followed when applying patches.
2. Patches should be applied in a timely manner. Recommended schedules may be established by a vendor.
3. Patching should be centrally managed where possible.
4. Logs of updates and alerting for out-of-date systems should be implemented.
5. Patching should follow change management procedures.
6. Patches should be tested and evaluated prior to implementation.

References

University of North Texas System Information Security Regulation

Contact Information

Information Security Team
IT Shared Services
<http://security.unt.edu>
security@unt.edu
(940) 369-7800