



University of North Texas System

Firewall Exception Process

Purpose

This document provides direction and guidelines for managing access control of firewalls on Information Technology Shared Services (ITSS) managed networks. In order to protect the confidentiality, integrity, and availability of information and information resources, the UNT System Information Security Regulation requires the implementation of the principle of least privilege. Firewalls managed by ITSS will be configured in a “default deny” configuration for ingress traffic. Exception requests must support the mission of UNT System Administration or Institutions.

Scope

These procedures apply to networks managed by ITSS.

Procedure

1. In order to request an exception, a user shall submit a request to the appropriate IT Support personnel within the requesting department or college. The request must include a business case that justifies the request and evidence that the system is properly secured and maintained. IT Support personnel will submit a service request for the firewall exception to ITSS Information Security.
2. The Director of Information Security or their delegate will review the request. The criteria for granting an exception are:
 - a. The request must support research, teaching, or business operations at the institution
 - b. The request must be for a service that cannot be supported via use of the VPN
 - c. The requesting department must have an established plan for ongoing maintenance of the system
 - d. Maintenance of the system must be assigned to a responsible party and implemented according to the maintenance plan
 - e. The system will be required to pass a credentialed vulnerability scan if feasible
 - f. The system will be continuously monitored for security concerns by ITSS Information Security

3. An approval or rejection of the request will be sent to IT Support personnel via the IT Service Management system.
4. A denial may be appealed to the Chief Information Security Officer of the UNT System or Institution.
5. Exceptions shall be reviewed for continuation at the end of each fiscal year by the Director of Information Security.
6. An exception may be revoked at any time for security reasons by the Director of Information Security. A revocation may be appealed to the Chief Information Security Officer of the UNT System or Institution.

Contact Information

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

References

UNT System Security Regulation
Texas Administrative Code Chapter 202