**Improve the Security of University Data Assets by Limiting Firewall Exceptions**

**Background:**

- The Security Task Force recognizes the importance of maintaining the integrity and security of ASU technology assets. Firewall exceptions allow connections from outside the ASU-J network (the Internet) directly into the local computer network. These exceptions can be very specific or very broad depending on the level of access needed. The more exceptions created and the more broad the access the greater the risk of unauthorized access to the University's computer network.

**Summary:**

- Firewall exceptions will be closely scrutinized and periodically reviewed.
- Perimeter devices will be scanned for security issues and remediation must be made to vulnerabilities

**Consequences:**

- Failure to document and justify a University need for a firewall exception will result in the termination of the exception.

- Failure to remediate security vulnerabilities on a network device will result in the device being disabled.

# Firewall Exception Procedure

Firewall exceptions added to the ASU-J firewall must adhere to the following:

- Firewall exceptions (open ports) must be requested in writing
- Requests must be justified and approved by Chair/Dean/Dept. Head
- Requests must be reapproved every 6 months
- ITS may scan devices that can be accessed via open ports for security issues. All issues found must be corrected/justified in two weeks or the firewall exception will be closed
- ITS may close an open port at anytime for security reasons
- ITS may at its discretion decline to open a port
- ITS may require that a device be moved to the perimeter network (referred to as the DMZ which provides an additional layer of security) instead of opening a firewall port
- Maintaining devices in the perimeter network (DMZ) is the responsibility of the department that owns the device
- Devices in the perimeter network (DMZ) may be scanned by ITS for security issues and sensitive data
- ITS may disable access to a device in the perimeter network (DMZ) if it fails said scans
- Devices failing scans must be corrected/justified in two weeks or access to the device will be disabled