THE UNIVERSITY OF ARIZONA.

Standard Title: University Network Operational Security
Standard Number: IS-S600
Responsible Office: Information Security Office

The purpose of this standard is to establish requirements and procedures for safeguarding the *university network* from:

- Unauthorized access to university computers by unknown individuals
- Unauthorized and inappropriate use of computer disk space and CPU resources
- Unauthorized access to or acquisition of *confidential university data*
- Use of a computer for outward bound *attacks* on others on the Internet

These standards apply to the users of all *devices* connected to the *university network* for the transmission and reception of *electronic communications*.

1. Standards

1.1. Network Access

- The university will not offer any *network* access or services to the world at large unless those services have been authorized in advance. Network Technology Solutions (NTS) will work with *system administrators* to maintain a catalog of services that need an outward face to the off-campus Internet. Access to these identified services will be allowed through the network border, all other Internet services will be denied access to the *university network*.
- Users of the *university network* will need to authenticate when attempting to access the *university network*. Additionally, users will be required to have a university approved, updated *anti-virus software* package and current security related operating system *patches* installed. If a user's host is found not to meet these minimum admission criteria, then that host will be blocked from *university network* access until it meets the above minimum admission criteria.
- The university hosts several non-*university network* connections for simple peering with the university and for connection to the commodity Internet and where qualified, Internet 2. All such networks will be outside the university secure perimeter unless the connection would adversely impact the entities' relationship with the university. Any network that is connected inside the *university network* perimeter will adhere to the same standards as *university networks*.

1.2. Network Infrastructure

- All wireless access points must be approved or installed by an authorized university *network administrator*.

  All traffic destined for *university resources* using a wireless access point shall be *encrypted*. Use of *UAWiFi* (or an equivalently "secured" wireless access point) or the use of the university's *site-licensed VPN* to connect to unsecured wireless access points accomplishes this.

Additional standards relating to account management can be found in Wireless Deployment and Management Standards.

- *Networks* that house *confidential university data* must be:
  - isolated from other *networks* through the use of firewalls.
  - physically secured, only allowing access required to conduct the business of the university.
- The university will not allow non-centrally managed *network* gear to participate, speak, or propagate 802.1d, 802.1s, 802.1w (Spanning-Tree) protocols to the *university network*.
- The university will host all voice communications centrally. This includes Voice over Internet Protocol (VoIP) services. Unit PBXs are not authorized to be used on the *university network*, except where expressly permitted. All voice communications will be operated in accordance with all applicable laws and will meet Network Reliability & Interoperability Council (NRIC) best practices and standards (including but not limited to compliance with the 911 Act and the Communications Assistance for Law Enforcement Act).

2. Operational Rules

2.1. Authorization

NTS will work with *system administrators* to determine the need for required Internet services to be opened at the campus border via rules on a *firewall*. *System administrators* must describe what service is needed, the precautions taken to secure the device offering the services and the probable sources of requests for the service.

2.2. Scanning

The *UISO* may designate university entities to *scan* machines or whole subnets at both announced and unannounced times to look for *vulnerabilities* or *compromised* machines.

2.3. Port Throttling

Port throttling or blocking may occur to prevent or alleviate either *attacks* or excessive bandwidth consumption.

2.4. Service Disconnection

Devices or *networks* of *devices* are subject to service disconnection by the *UISO* designee(s) if such *devices*:

- pose a security threat to the *university network*
- significantly impact the functionality of the *university network* in a negative manner
- violate Federal or State law or university policy

Examples of grounds for service disconnection include, but are not limited to:

- rogue DHCP servers
- malware infected devices
- spam senders/relays
- unauthorized probing of other network devices

Common forms of service disconnection include, but are not limited to:

- by device or port,
- or in extreme circumstances, by VLAN, floor, or building.

If it becomes necessary to disconnect service to one or more devices behind a non-centrally managed *network address translation (NAT)* device, all *devices* behind that NAT device are subject to service disconnection due to technological constraints. In cases where there is a prior understanding that the NAT device serves a large or critical *network* behind it, all reasonable effort will be put into notifying the *device* administrator before service disconnection occurs.

2.5. Prohibited Protocols

Authorized off campus users needing to access services on campus must do so in a secure manner. Use of Microsoft Windows File Sharing (WFS) will be blocked at the campus border and NTS will enable a specific pass through for those users who need to use the service from identified locations.

For services needing *university network* access to facilities on campus a *VPN* connection to campus must be used. Using the *VPN*, a user will be authenticated on the *university network* before gaining access to the *university network* resources. When using the *VPN* the network address assigned to the user's computer will be within the Internet Address range of the university. This will allow *authorization* for access to campus services and follow the rules for network admittance to other campus networks and Internet services.

Related Guidance

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)

All *italicized* terms used in this standard are defined in the Information Security Terms Guideline (IS-G100).

Revision History

Initial Draft	05/24/06
Effective Date	05/27/08