

STANDARD ADMINISTRATIVE PROCEDURE

29.01.99.M1.12 Information Resources –Network Access

Approved July 18, 2005

Next Scheduled Review: Currently Under Review

Supplements [University Rule 29.01.99.M1](#)

1. GENERAL

The information resources network infrastructure in Bryan/College Station is provided by Texas A&M University for tenants of University facilities. It is important that the infrastructure, which includes media, active electronic equipment (i.e., multiplexers, hubs, routers, etc.) and supporting software, be able to meet current performance requirements while retaining the flexibility to allow emerging developments in high speed networking technology and enhanced user services. The purpose of the TAMU network access procedures is to establish the process for the access to the network infrastructure.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all university network information resources.

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with network access.

System administrators are the primary audience for this SAP.

3. DEFINITIONS

3.1 Anonymous write capability - the ability of people to save (on TAMU computers) information they create without their identity being known (**to system administrators**).

3.2 Anonymously originating network traffic - causing a (TAMU) computer system to send traffic via the network where the custodian/owner is not known.

3.3 Information Resources (IR): the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

4. PROCEDURES

4.1 Network aggregation devices (e.g., hubs, switches, routers) shall not be connected to network infrastructure without prior approval by Computing

and Information Services (CIS). Contact CIS Help Desk Central at consult@net.tamu.edu or (979) 845-8300.

- 4.2 Management of network addresses and name space may be delegated to system administrators. Users are permitted to use only those network addresses issued to them by their designated system administrator.
- 4.3 Network scans and network vulnerability scans of devices attached to the Texas A&M University network are occasionally necessary to ensure the integrity of TAMU computing systems. Network scans and network vulnerability scans may only be conducted by University employees designated by the organizational unit head responsible for the information resource. Guidelines for appropriate scanning can be found at http://nis.tamu.edu/Home/IT_Policy/Networking_Procedures_and_Guidelines/Network_Scanning_Guidelines.php.
- 4.4 Individuals controlling right-to-use for systems attached to the network infrastructure will ensure only authorized persons are granted access.
- 4.5 Allowing anonymous write capability to University systems or anonymously originating network traffic requires CIS permission.
- 4.6 Users shall not alter University owned network hardware in any way.

CONTACT: [Information Technology Issues Management of CIS](#)

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)