The University of North Texas at Dallas Policy Manual	Chapter 14.000
14.005 Network Access	**Information Technology**

Policy Statement. It is the policy of the University of North Texas at Dallas to manage the University's information resources as strategic assets of the State of Texas. It is important that the information resources network infrastructure, which includes media, active electronic equipment 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. This policy defines the process for the access to the network infrastructure.

Application of Policy. This policy applies to all University Users.

Definitions.

1. Information Resources. "Information Resources" mean the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data and administered both centrally and within individual departments, on-campus and remotely, on a mainframe and network servers, and for use by single and multiple users.

2. Anonymously Originating Network Traffic. "Anonymously Originating Network Traffic" means network activity causing a university computer system to send data via the university network where the custodian/owner of the data is not known.

3. Anonymous Write Capability. "Anonymous Write Capability" means the ability of university users to store information on University computers, information they create without their identity being known to system administrators.

4. University Users. "University Users" mean all faculty, staff, students, contractors, volunteers, and individuals that maintain a business relationship with the University that accesses the University's network infrastructure.   Information resources may also be included in this category.

PROCEDURES AND RESPONSIBILITIES.

1. **Network Infrastructure**.

    1.01. Network aggregation devices (e.g., hubs, switches, routers) shall not be connected to the University network infrastructure without prior approval by the Information Technology Department.

    1.02. Users shall not install network hardware or software.

    1.03. Users shall not alter University owned network hardware in any way.

    Responsible Party: All University Users/Information Technology

2. **Network Access Privileges**.

    2.01. Management of network addresses and name space may be delegated to authorized system administrators. Users are permitted to use only those network addresses issued to them by their designated system administrator.

    2.02. Individuals controlling right-to-use for systems attached to the network infrastructure will ensure only authorized persons are granted access.

    2.03. Remote users may only connect to the University's network through protocols established by the Information Technology Department.

    2.04. Non-University computer systems that require network connectivity must conform to the University information resources standards.

    2.05. Individuals shall not configure systems allowing anonymous write capability or anonymously originating network traffic.

    Responsible Party: All University Users/Information Technology

<u>References and Cross-references</u>.

Texas Government Code § 2054 – Information Resources

Texas Administrative Code, Chapter 202, Subchapter C and Department of Information Resources, Policy and Standards for Protecting Information Resources for Texas

Approved: 8/30/2010
Effective: 8/30/2010
Revised: