IT Network Connection Policy

The University of Texas at Tyler

Information Technology

The University of Texas at Tyler's technology environment is continuing to expand and evolve at a rapid pace. It is imperative that the infrastructure supporting UT Tyler's use of information technology remains sound, efficient, consistent, and reliable for all members of the UT Tyler community. The Information Technology department (IT) is responsible for the campus backbone network including, routing, switching, domain name service, etc. IT is the logical entity to coordinate all connections to the campus network.

Definitions:

Modem
A peripheral device that connects computers to each other or a server for sending communications via telephone lines.

Router
A special purpose computer that attaches to two or more networks and routes packets from one network to the other.

Server
A computer that shares its resources, such as printers and files, with other computers on the network.

Switch
A device that filters and forwards packets between LAN segments.

Wireless Access Point
In networking, wireless access refers to connecting to the network without the use of wires.

Workstation
In networking, workstations refer to any computer connected to a local area network.

Improperly configured servers, workstations, switches, and routers can cause serious problems for the entire network and may have vulnerabilities that can become security breaches. Therefore, the following procedures have been adopted and implemented to assure the continuing quality of information technology at The University of Texas at Tyler.

• Any of the above devices (servers, workstations, switches, modems, or routers) that are or will be connected to the UT Tyler network (local or Internet) must be reported to Information Technology and approved before connection is made to the UT Tyler network.

• The University maintains a DHCP server with IP addresses, which are assigned to UT Tyler by The UT System Office of Telecommunication Services (OTS). Any network devices (servers, workstations, routers, or switches) that are set up, either by design or by default, to use DHCP assigned IP addresses must be reported to the Department of

Continued

Information Technology and must follow the naming convention set forth by Information Technology.

• The department head and his/her designee will be responsible for ensuring that OS security patches and service releases are applied and maintained on a regular basis. For information on basic operating system security guidelines and released patches consult the following Information Technology web site: http://www.uttyler.edu/inforesources/NetworkSecurity.htm

• Information Technology retains the right to disconnect and/or block the device from the network without notice if it is determined by IT that the device is causing bandwidth or other problems on the UT Tyler network or if the device has known security vulnerabilities that have not been corrected by maintenance of the service releases and/or security patches by the department head and or his/her designee.

The following minimum-security requirements are mandatory for any device connected to the UT Tyler backbone:

Servers & Workstations:

• All security patches must be loaded before attaching server and/or workstations to network and each must be kept current with security patches as they are released.

• Server and workstations must have anti-virus protection software loaded and virus definitions must be set to download daily.

• All web servers must be reported to Information Technology and all security patches must be applied as they are released.

• All FTP servers must be secured with a password (no anonymous access).

• Default installations of operating systems are not inherently secure, therefore, it is recommended that any services, which are not necessary for the immediate use of the end-user, be disabled. For more information on basic operating system security guidelines and released patches consult the following Information Technology web site: http://www.uttyler.edu/inforesources/NetworkSecurity.htm

• Passwords:
  - Must have password set and must be a minimum length of 7
  - characters.
  - Must be set to expire no more than every 45 days.
  - Must limit invalid password attempts to no more than 5.

Continued

- Must not allow immediate reuse of same password.
- All Guest and Anonymous login accounts must be disabled.
- Disable Default user or make sure there is a password set for Default.
- Limit concurrent logins to one except for administrative purposes.
- User accounts that remain inactive for a period of more than 6 months must be disabled.

Modems:

• User must report any and all modems to Information Technology.
• User must sign Modem policy that states reason for modem and acknowledges that user abides by all of the University's security policies. Forms will be retained in the Office of Information Technology.
• Any program that is used for remote access via a modem (ex: PCAnywhere, Remotely Possible, etc.) must be secured with a password and the call-back feature must be disabled.

Wireless Access Point (WAP):

• All wireless networks must be reported to Information Technology and must follow designated security guidelines.