Network Usage Policies

Policy:
Usage of Baylor University's communication networks is restricted to activity that supports the work and mission of the University. The specifics of these restrictions are detailed in the topics below.

Topic Listing:
Prohibited Usage
VPN Access
Web Filtering
Wireless Frequencies

Related Policies and Legislation:
Technology Systems Usage Policy BU-PP 025
Incident Response Policy

Contact:
ITS Help Desk 710-4357

Sanction:
Sanctions may include but are not limited to suspension of technology privileges, termination of employment, referral to Student Judicial Services, and/or criminal prosecution. For additional information, please reference Technology Systems Usage Policy BU-PP 025

Date updated:
Updated – March 26, 2007

Prohibited Usage:

- Incidental use while allowed may not be supported and/or may be restricted if it interferes with the functionality of the network.

- Unauthorized networking equipment (such as routers and wireless access points, etc.) is prohibited from use on the network. Network services and wiring may not be modified or extended beyond their intended use.

- Users may not manually assign an IP address to any network device. Doing so may disrupt connectivity for other users.
Users of the Baylor University network may not provide access to resources on the local network to anyone outside of the Baylor community for any purpose unless accomplished by means approved by Information Technology Services (ITS).

Computer names, computer descriptions, and messages broadcast across the network should not be defamatory, lewd, or obscene.

Network users are responsible for any network activity linked to their BearIDs. BearID passwords should be secure, and should not be shared with anyone (including family, roommates, and friends). Users who believe that another person is using their account should notify Baylor University IT security immediately and change their password.

For security reasons, Baylor University requires users to log on to access the campus networks and Internet. Users are prohibited from attempting to circumvent the authentication systems. In addition, users should not attempt to hide their identity or impersonate another's identity while on the University network.

Users are responsible for security and privacy precautions to protect against computer viruses, computer attacks, and theft which may result in loss of data, unintentional release of personal information, or negative impact on Baylor University's technology services. Failure to take these prudent steps could result in the offending computer or account being removed from the network.

Files may be shared on the local network. All shared resources on Resnet, wireless and other workstation computers must be protected with a secure password. Any sharing of resources without a password must be authorized by ITS.

Federal law prohibits the transmission (sharing) of copyrighted materials without express written permission from the copyright holder. Copyrighted works (including but not limited to original writings, software, movies and music) may not be shared on the local network without written permission of the copyright holder.

Baylor University reserves the right to restrict access to any service or equipment detrimental to the Baylor University's technology resources. Attempts to bypass these restrictions will be considered a violation of this policy.

Baylor University does not allow network users to run unauthorized SMTP, DHCP, DNS, or directory services on any networks.

Audio, video and game servers are allowed on hardwire (non-wireless) networks. However due to network bandwidth concerns, these servers may be disconnected without notice if performance of the University's networks is adversely affected. In addition, all use must comply with existing copyright laws.

Unauthorized registration of a domain to a Baylor IP address is prohibited. This includes but is not limited to direct DNS resolution and DNS aliasing.

Unauthorized hardware and/or software used to detect and/or exploit network vulnerabilities are forbidden on Baylor University networks.

Forgery or other misrepresentation of one’s identity via electronic or any other form of communication is prohibited regardless of intent.

Personally-owned computers are only allowed on the AIRBEAR and Resnet networks.

VPN Usage:

VPN usage is targeted for faculty/staff access. Graduate students may receive VPN access at the request of a faculty sponsor.

Only VPN client software that is approved by and/or distributed by ITS networking services may be used to connect to Baylor University's network.
Baylor University ITS has created a VPN application for sponsored third parties such as software consultants or support personnel, to gain VPN access to support on campus systems. A Faculty/Staff sponsor and a signed non-disclosure agreement by the third party are required to obtain the account.

Currently VPN software is available for Windows 2000/XP and Mac OS X. Approved users are responsible for the installation of the VPN software.

Baylor University has configured the VPN service to prevent the bridging of networks (split tunneling). As a result, when connected to VPN, all network traffic from the user’s computer will travel through the Baylor University network which will not allow communication back to a device on the private network other than the computer making the original connection.

Only one active VPN connection is allowed per user and the VPN concentrator is limited to a total connection time of 8 hours per user in one session.

**Web Filtering:**

- Baylor University ITS filters web content as a mandate of the University regents.

- Inappropriate adult content will be filtered.

**Wireless Frequencies:**

- ITS reserves the right to control and restrict the operation of all devices using the 2.4/5.2 GHz bands within University property.

- Devices that utilize the 2.4/5.2 GHz frequencies and are necessary for instructional or research applications will be handled through Baylor University ITS.

Last modified March 26, 2007