BAPTIST HEALTH SCIENCES UNIVERSITY

Internet Access Requirements on University PC's

Access Control

1. The University encourages users to explore the Internet, but this exploration should be for business or educational purposes, and not personal use. Non-business or non-educational activities must be performed on personal time. Internet access in the workplace is a privilege, not a right, and is given to assist users in work-related or educational objectives.
2. All users wanting access to the Internet must authenticate themselves at a firewall, or approved internet service provider. These firewalls are selected, approved, installed and managed by Information Technology. Anyone connecting to the Internet without a firewall authentication is subject to loss of network privileges and disciplinary action up to and including termination. Direct access via a dial-up connect to an Internet service provider is prohibited unless explicitly required for your job. Prior approval, by University administration is required.
3. Unless prior approval is obtained from the Vice President, Business and Financial Services, users may not establish internal or other external network connections that could allow non-University users to gain access to University Information Systems and information. No incoming , Transmission Control Protocol (TCP) session calls will be permitted.
4. Approval for Internet access must be requested from the department Director/Dean. Internet connections will not be moved or transferred. The request should obtain reasonable business justification for access to an outside web site, and the URL of the web site(s) you are most likely to access.
5. Users should use sensible, reasonable judgment when transferring large amounts of data which may affect other users. Users should be sensitive to the needs of other users, both in the quantity and type of data you are accessing

Transfer of Information

1. Users must not place Baptist University of Health Sciences, (hereafter University materials (software, internal memos, etc.) on any publicly accessible Internet computer which supports anonymous FTP or similar services unless the posting has been approved in writing by the Vice President, Business and Financial Services,.
2. Secret, proprietary, or private information must not be sent over the Internet. Users must not publicly disclose internal information that may adversely affect University student relations, vendor relations, public image, or financial standing. Users must be careful to properly structure comments and questions posted to mailing lists, public news groups, and related public postings to ensure inadvertently providing sensitive information. If a user is involved with an unannounced project or related confidential matters, all related postings must be cleared with their manager prior to being placed in a public spot on the Internet. Users are prohibited from responding to vendor surveys presented on-line.
3. University software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-University party for any purposes other than business purposes expressly authorized by management.

4. Unless approved by the Vice President, Business and Financial Services and legal counsel, users are prohibited from establishing new business channels or communication channels using new Web technology.

Security

1. Credit card numbers, telephone calling card numbers, log-in passwords and other parameters used to access services within the University must not be sent over the Internet. If users are contacted via the Internet or other source asking for disclosure of service access passwords, the incident should be reported immediately to the Frontline at (901) 227-7777.
2. **At any time and without prior notice, the Administration of the University reserves the right to examine e-mail, personal file directories, and other information stored on University computers. This examination assures compliance with internal policies, supports the performance of internal investigations and assists with the management of the University.**
3. Lost, stolen or disclosed passwords must be reported to the Frontline at (901) 227-7777 immediately.
4. Users must not probe security systems at the University or other Internet sites.
5. Internet Telnet access, either outgoing or incoming, is not permitted for reasons of network security and safety from hackers.

Software Procurement

1. Exchanges of software and/or data with the University and any third party may not proceed unless a written agreement has first been signed and approved by the Vice President, Business and Financial Resources. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and/or protected.
2. The University strongly supports strict adherence to software vendors' license agreements. When at work, or when doing computing in conjunction with the University, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Sending or retrieving software to/from pirate software bulletin boards and similar activities is strictly prohibited.
3. All software and/or files downloaded from the Internet must be scanned for viruses before loading onto shared directories. No executable code should be imported to a University computer system without prior approval by Tech Support.

Public Representations

1. Reproduction of words posted or otherwise available over the Internet must be done only with permission of the owner.
2. Users may indicate their affiliation with the University in bulletin discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied. In any case, whenever workers provide an affiliation, they must also clearly indicate the opinions expressed are their own and not necessarily those of the University. Additionally, whenever any affiliation with the University is included with an Internet message or posting, "flaming" or similar written attacks are strictly forbidden. Users are prohibited from participating in discussions that are of a racially or sexually offensive nature.

Use of University Wireless Network

What is a "Peer-to-Peer" file-sharing program?

A Peer-to-Peer file-sharing program is any program that allows an unknown individual to search and download files from your computer. These programs allow an individual to share any type of file with a large number of people easily. Most often they are used to share copyrighted, illicit, or illegal material "anonymously." Commonly the files are used to share music and video files. Some examples of this type of program include but are not limited to:

BearShare	Gnotella	Gnucleus	GTK-Gnutella	LimeWire	Mactella
Morpheus	Phex	Qtella	Shareaza	SwapNut	XoLoX
WinMX	Kazaa	iMesh	eDonkey2000	Goto My PC	Direct Connect

USE OF ANY SUCH PROGRAMS ON BAPTIST UNUIVERSITY OF HEALTH SCIENCES NETWORK IS STRICTLY PROHIBITED. Additionally, peer-to-peer programs can cause many problems that you may not have considered. Below is a list of issues that arise with the use of these types of programs.

Legal and Moral Issues:

Baptist University of Health Sciences is a Christian University that endeavors to incorporate Christian values in all aspects of its environment. Since obtaining and redistributing copyrighted materials without compensation is stealing, Baptist University of Health Sciences will not tolerate any such programs on its network.

Furthermore, Peer-to-Peer network usage is actively being monitored by organizations that are dedicated to protecting Internet copyright laws. Should these organizations detect someone from Baptist University of Health Sciences' network to be illegally trading in copyrighted materials, Baptist University of Health Sciences and the Baptist Memorial Health Care Corporation could risk injunctions, damages, legal defense costs and possible criminal sanctions against Baptist University of Health Sciences, Baptist Memorial Health Care Corporation or its directors.

Malware (Viruses and other Harmful Code)

Symantec, creators of Norton Antivirus, has been tracking many devastating viruses and malware on Peer-to-Peer Networks that pose as popular files. These malware programs may cause physical damage to your computer and network computers, up to and including **deletion of data on network and local drives**.

Spyware

Peer-to-Peer software often includes "Spyware" that may report private information such as user web usage or critical internal network information to unauthorized third parties. Antivirus programs will not protect your computer.

Exposure of Student, Employee and Patient Data

Peer-to-Peer programs are often configured to allow anonymous users to browse the entire directory structure of participating hosts. This means that not only are music or other files available for download, but possibly every file on your local and network drives.

Loss of Internet Services to the Entire Baptist Memorial Health Care Corporation

Because the way these programs function and how we receive Internet services, use of file sharing programs can subject the entire corporation to a Denial of Service Attack, effectively blocking Internet access to and from the corporation.

Students should contact the frontline at 227-7777 if there is any possibility a program they wish to install on their personal computer is a peer-to peer program.

I, _____ have read the Peer to Peer file sharing information and understand or agree:

1. That I have a clear understanding of what constitutes Peer-to-Peer software and the dangers that are associated with such programs.

2. That Peer-to-Peer software in any form is strictly prohibited as long as my personal computer can be attached to the Baptist University of Health Sciences' network.

3. That installing any such software is strictly prohibited as long as my personal computer can be attached to the BCHS network.

4. That if Peer-to-Peer software is detected on my personal computer, network access will be disconnected until such time that the Dean of Student Services determines what disciplinary action is to be taken.

Additionally, I also agree not to use any type of Instant Messaging Program, (MSN, AOL, Yahoo, etc.) while on the University network.

University Internet Access Request

This is a request to add internet access to my University Computer User Account. I have read the Internet Access Policy. I understand and agree to the rules designated therein. I further understand that violation of this policy may result in disciplinary action up to and including termination of my employment at Baptist University of Health Sciences.

Student (please print or type)	Phone
Student Signature	Date
Director/Dean Approval	Date
University Administrator	Date