Technology Usage Policy

Policy Statement

This policy addresses the intended use of technology for the Baylor University community.

Reason for the Policy

This policy sets forth the appropriate and inappropriate uses of Baylor technical resources.

Individuals/Entities Affected by this Policy

Who is affected by this policy

This policy applies to all active members of the University community, including faculty, stQq0.BaTf1 0 0 1 7Pli(a)540.Ba(i)-6(n-7(t)]TJ)-346(f)(i)-6(n544(d)-6(--34(u)-6(s544(d)-6fl)7(ife)-6( )-(cy

Related Documents and Forms

University Policies and Documents

BU-PP 029 Handling of Confidential Information
BU-PP-023 Standards of Personal Conduct (political communication)
BU-PP 705 Faculty Dismissal Policy
BU-PP 807 Staff Discipline Policy
Incident Response Policy
Network Usage Policy
Student Disciplinary Procedure
Website and Email Privacy Statement
Information Use Policy
Payment Card Industry Policy

Other Documents

¶ Family Educational Rights and Privacy Act (FERPA) 20 USC §1232g and 34 CFR Part 99
¶ Health Insurance Portability and Accountability Act (HIPAA) 42 USC §300gg and 1320d; 29 USC §1181 and 45 CFR Parts 146160, 162 and 164
¶ Gramm-Leach-Bliley Act 15 USC §6801 et seq and 16 CFR Part 313 et seq
¶ Fair and Accurate Credit Transactions Act (Red Flags Rule) 15 USC §1601 et seq
¶ Protection of Human 45 CFR Part 46
¶ Texas Business and Commerce Code privacy laws Tex. Bus. & Comm. Code Chapters 501-503
¶ Privacy Act of 1974 5 USC §552a et seq
¶ Texas Public Information Act Texas Government Code Chapter 552
¶ 15 USC §6501 et seq and 16 CFR Part 312
¶ European Union General Data Protection Regulation (EU GDPR) EU 2016/679
¶ PCI DSS

Definitions

These definitions apply to terms as they are used in this policy.

Baylor University Technology Systems	Baylor-owned, licensed, or operated technology systems including, but not limited to, computers, computer accounts, internet, printers, networks, network devices, webpages, video systems, telephones, mobile devices, telephone long distance and voice mail accounts that are provided for the use of University community in support of the programs of the University
E-Discovery	Refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought is in electronic format
Incidental Personal Usage	Incidental personal use of University technology resources is permitted; as long as the personal use: ¶ Results in no additional cost to the University ¶ Is minimal in time and duration ¶ Does not interfere with job responsibilities ¶ Are not prohibited activites
ITS	Information Technology Services
Protected Materials	Software and other materials that are protected by copyright, patent, trade secret, or another form of legal protection
University Community	Faculty, staff, students, affiliates, authorized visitors, guests, and others for whom a University technology resource or access to the network has been provided

Contacts

Subject	Contact	Telephone

- ¶ When personal information is stored on University technology systems, such information is subject to University policy and practice, including important limitations in the privacy of such information

Individual Accountability

The U

¶ Fraudulent, harassing, offensive, or obscene messages or materials are not to be sent, printed, requested, displayed, or stored on Baylor-owned, licensed or operated technology systems.

¶ Information that invades or abuses an individual's privacy or is disparaging of an individual or business must not be published without the express consent of the person or business entity.

¶ No one may attempt to degrade the performance of a technology system or to deprive authorized personnel of reasonable access to University technology systems.

¶ The use of loopholes or specific tools to circumvent technology systems or network security, the use of special passwords, or the covert acquisition of passwords to damage technology systems, obtain extra resources, take resources from another must be stored on a Baylor-owned, licensed, or operated technology resource. Software is installed on University technology systems in order to support resource usage accounting, security, network management, hardware and software inventory, computer back-up systems, and software updating functions, and to provide better support to personnel. Authorized personnel may access others' files or systems when necessary for the maintenance of technology systems or when acting to protect performance, integrity, and security of technology resources or in compliance with court orders or other legal requirements. When possible, advanced notification of access will be given, except for cases covered by Exceptions/Approvals. When performing maintenance, reasonable effort will be made to safeguard the privacy of a user's files. However, if violations of University policy or applicable law are discovered, they will be reported to the appropriate vice president or the appropriate authorities.

¶ **Data Backup -** ITS provides centralized backups for faculty and staff primary computers. Due to the possibility of technical failure, e-discovery, or separation, faculty and staff are responsible for maintaining separate backups of personal files stored on Baylor University owned technology.

¶ **Access and Data Expiration -** Technology system accounts that expire, along with the files in the expired accounts, may be deleted. Accounts expire in accordance with the terms of the account. Email and voice mail messages that are older than the limit set by the system administrator will be deleted.

¶ **Content Restriction -** Baylor University contracts with a professional web-filtering service to block sites the vendor designates as adult content (e.g., obscenity, pornography). Additionally, the same service is used to block sites which pose an information security risk to the University (e.g., phishing and malware sites). The ITS Chief Information Security Officer oversees a process to address misclassifications of content. Reclassification and the decision to block or unblock

to the Vice President for Information Technology.

Exceptions/Approvals

Electronic mail, voice mail, and files on a Baylor-owned, Baylor-licensed, or Baylor-operated technology system are presumed to be private and confidential unless they have explicitly been made available to other authorized individuals or as required by law. Their contents may be accessed only by authorized personnel for compelling University business or security reasons. All requests for electronic records should be submitted to the Chief Information Security Officer or the Vice President for Information Technology. The request must be accompanied by the approval of the President or the appropriate divisional vice president:

¶ for faculty members, the Provost;

¶ for staff members, Vice President and Chief Human Resources Officer;

¶ for students, the Vice President for Student Life; or

¶ as required by law.

Sanctions

An individual's technology systems usage privileges may be suspended immediately upon the discovery of a possible violation of this or other University policy. ITS may also disable accounts to protect the integrity of the information technology infrastructure or data stored within. The chief information security officer or vice president for information technology may authorize the disabling of an account for up to one business day. Such suspensions will be confidentially reported to the appropriate department head/chair, dean, ITS staff, and divisional vice president. An account may be disabled for longer than one business day by following the same approval process outlined in Exceptions/Approvals.

The ITS administrative staff or supervising department head/chair may judge some violations of this policy as either major or minor. A first minor offense will normally be dealt with by the ITS administrative staff or supervising department head/chair. Appeals relating to minor offenses may be made to the appropriate vice president. Additional offenses will