Information Technology Services
Privacy Standard

Approved: February 11, 2020

Standard Statement

Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in university information resources. The university has the right to examine information on information resources that are under the control or custody of the university. The general right to privacy is extended to the electronic environment to the extent possible; however, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

Reason for Standard

This standard applies to electronic information created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the Tarleton State University.

The purpose of the implementation of this standard is to provide a set of measures that will mitigate information security risks associated with privacy issues. There may be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this standard based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated information security officer.

The audience is all users and administrators of university information resources.

Standards and Responsibilities

1. Privacy of information shall be provided to users of university information resources consistent with obligations of Texas and federal law and/or secure operation of university information resources.

2. In the normal course of their duties, system administrators may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

    2.1 In order to protect against hardware and software failures, backups of all data stored on

university information resources may be made. System administrators have the right to examine the contents of these backups to gather sufficient information to diagnose and correct problems with system software or hardware. It is the owner's responsibility to define the retention policies for any data of concern.

2.2 The organization unit head may designate certain individuals or functional areas that may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is occurring or has occurred. If files are examined, the file owner will be informed as soon as practical, subject to delay in the case of an ongoing investigation.

2.3 Files owned by individual users are to be considered as private, whether or not they are accessible by other users. The ability to read a file does not imply consent to read that file. Under no circumstances may a user alter a file that does not belong to him or her without prior consent of the file's owner. The ability to alter a file does not imply consent to alter that file.

2.4 Some individually owned files are by definition open access. Examples include Unix plan files, Web files made available through a system-wide facility and files made available on an anonymous ftp server. Any authorized user that can access these files may assume consent has been given.

3. If access to information is desired without the consent and/or knowledge of the file owner or if inappropriate use of Tarleton information resources is suspected, files may be reviewed without the consent and/or knowledge of the file owner if that review is part of the process of Standard Electronic Information Resource Complaints.

4. If criminal activity is suspected, the University Police Department or other appropriate law enforcement agency must be notified. All further access to information on university information resources must be in accordance with directives from law enforcement agencies

5. Information resource owners or custodians will provide access to information requested by auditors in the performance of their jobs. Notification to file owners will be as directed by the auditors.

6. Other than exceptions outlined in this standard, access to information by someone other than the file owner requires the owner's explicit, advance consent.

7. Unless otherwise provided for, individuals whose relationship with the university is terminated (e.g., student graduates; employee takes new job; visitors depart) are considered to cede

ownership to the information resource custodian. Custodians and/or owners should determine what information is to be retained and delete all others.

8. The university collects and processes many different types of information from third parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., Gramm-Leach-Bliley Act, Texas Administrative Code 202).

9. Individuals who have special access to information because of their position have the absolute responsibility not to take advantage of that access. If information is inadvertently gained (e.g., seeing a copy of a test or homework, access to employee records) that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

10. Users of Tarleton information resources shall call the Information Technology Services Executive Director/CIO, the Information Security Officer, or designee to report any compromise of security which could lead to divulging confidential information

---

Definitions

Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

Information Resources (IR): the standards, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

File Owner: Holder (assignee of the computer account which controls a file; not necessarily the owner in the sense of property.

Contact Office

Information Technology Services
CIO of Information Technology Services
254.968.9395