PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.10 Information Resources - Privacy
Approved May 26, 2009
Revised June 4, 2013
Revised December 7, 2018
Next Scheduled Review: December 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the responsibilities and limits for system administrators and users in providing privacy for Prairie View A&M University (PVAMU) information resources. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

Definitions

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Standard for additional information.

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

Information Security Officer (ISO) - person responsible to the executive management for administering the information security function within the University. The ISO is the University's internal and external point of contact for all information security matters.

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

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Official Procedures and Responsibilities

1. GENERAL

1.1 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, which 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. Contents of electronic files will be examined or disclosed only when authorized by their owners, approved by an appropriate University official, or required by law.

2. APPLICABILITY

2.1 This UAP applies to electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of Prairie View A&M University (PVAMU). The intended audience for this UAP includes, but is not limited to, all users and administrators of PVAMU information resources.

3. PROCEDURES AND RESPONSIBILITIES

3.1 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.

3.2 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.

3.3 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 user's responsibility to find out retention policies for any data of concern.

3.4 The department 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 may be informed as soon as practical, subject to delay in the case of an on-going investigation.

3.5 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.

3.6 Some individually owned files are by definition open access (e.g. Web files made available at PVAMU websites). Any authorized user that can access these files may assume consent has been given.

3.7 If access to information is desired without the consent and/or knowledge of the file owner or if inappropriate use of PVAMU information resources is suspected, files may be reviewed by the department head or designee without the consent

and/or knowledge of the file owner. In cases of inappropriate use, the ISO must be notified in writing.

3.8 If data or files are needed by a department to continue to conduct normal university business and the file owner is unable to provide access to the data/files, the data/files may be accessed by department personnel with the documented consent of the department head. The file owner may be notified of such access as soon as practical, subject to delay in the case of an on-going investigation.

3.9 If criminal activity (e.g. child pornography) is suspected, the University Police Department or other appropriate law enforcement agency must be notified as soon as practical. All further access to information on university information resources must be in accordance with directives from law enforcement agencies.

3.10 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.

3.11 Other than the exceptions stated in Sections 3.2 through 3.10, access to information by someone other than the file owner requires the owner's explicit, advance consent.

3.12 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 relinquish ownership to the information resource custodian. Custodians should determine what information should be retained or deleted.

3.13 The University collects and processes many different types of information from third parties. The majority of this information is confidential and shall be protected in accordance with all applicable laws and regulations.

3.14 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) that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

3.15 University web sites available to the general public shall contain a Privacy Statement such as that found at PVAMU Privacy Statement.

3.16 Users of PVAMU information resources shall call or contact the Information Security Officer to report any compromise of security which could lead to divulging confidential information including, but not limited to, posting social security numbers to the internet or sending student identification numbers via email.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Contact Office	
Office of Information Resources Management	936-261-9350