PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.20 Information Resources – Acceptable Use
Approved May 26, 2009
Revised May 3, 2013
Revised June 11, 2018
Next Scheduled Review: June 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish prudent and acceptable practices regarding the use of information resources, as well as, to educate individuals who may use Prairie View A&M University (PVAMU) information resources with respect to their role and responsibilities associated with such use. 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.

Mission Critical Information - information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the university or department.

Information Resources Manager (IRM) – person responsible to the State of Texas for management of the University's information resources. The designation of an IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the University's information activities, and ensure greater visibility of such activities within the University. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards, and guidelines to protect the information resources of the University. If an IRM is not designated, the title defaults to the University's executive director who then will be responsible for adhering to the duties and requirements of an IRM.

User - an individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

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.

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 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. PVAMU has developed University Rules and Administrative Procedures that address the acceptable use of information resources. The information resource owner or designee is responsible for ensuring that the risk mitigation measures described in this UAP are implemented.

1.2 There may be additional measures that department heads or deans will implement to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

2. APPLICABILITY

2.1 This UAP applies to all PVAMU information resources. The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

3. OWNERSHIP OF ELECTRONIC FILES

3.1 Electronic files created, sent, received, and/or stored on information resources owned, leased, administered, or otherwise under the custody and control of PVAMU are the property of the University.

4. PRIVACY

4.1 Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of PVAMU are not private and may be accessed by PVAMU Information Technology Services (ITS) employees at any time without prior consent or knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas

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

5. PROCEDURES

5.1 Users must report, in writing, any weaknesses in PVAMU's computer security and any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate department management and the ISO.

5.2 Users must not attempt to access any data or programs contained on PVAMU's systems for which they do not have authorization or explicit consent.

5.3 Users must not share their PVAMU account(s), password(s), personal identification numbers (PIN), security tokens (i.e. electronic key access), or similar information or devices used for identification and authorization purposes.

5.4 Users must not make unauthorized copies of copyrighted software.

5.5 Users must not install and/or use non-standard software without prior approval by the Office of Information Resources Management unless the software is adopted as a standard or is communicated by ITS as allowable.

5.6 Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of information resources; deprive an authorized PVAMU user access to a PVAMU resource; obtain extra resources beyond those allocated; circumvent PVAMU computer security measures.

5.7 Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, PVAMU users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on PVAMU information resources.

5.8 PVAMU information resources must not be used for personal benefit/gain.

5.9 Users must not intentionally access, create, store or transmit material which PVAMU may deem to be offensive, indecent or obscene.

5.10 Outside access to the network and the Internet from a PVAMU owned computer must adhere to all the same policies that apply to use from within PVAMU facilities. Employees must not allow any non-authorized family members or other non-employees to access PVAMU computer systems.

6. INCIDENTAL USE

6.1 PVAMU allows for incidental personal use of information resources. User abuse of this privilege may result in the removal of these rights or other disciplinary action. The following restrictions apply to incidental personal use of information resources:

6.1.1 Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to PVAMU approved users; it does not extend to family members or other acquaintances;

6.1.2 Incidental use must not result in direct costs to the University;

6.1.3 Incidental use must not interfere with the normal performance of an employee's work duties;

6.1.4 No files or documents may be sent or received that may cause legal action against, or embarrassment to the University;

6.1.5 Storage of personal email messages, voice messages, files and documents within the University's information resources must be nominal; and,

6.1.6 All messages, files and documents - including personal messages, files and documents - located on University information resources are owned by the University and may be subject to open records requests in accordance with this UAP.

7. DISCIPLINARY ACTIONS

7.1 Violation of this UAP may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students - suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to PVAMU information resources, civil, and/or criminal prosecution.

8. SUPPORTING INFORMATION

8.1 All University employees and other users of campus owned information resources are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. University employees are also responsible for reporting any suspected or confirmed violations of this UAP to the appropriate information resource owner, departmental supervisor and the ISO.

8.2 The use of information resources is intended for officially authorized business purposes. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers shall be responsible for proper authorization of information resource utilization, the establishment of effective use, and reporting of non-compliance to management.

8.3 Any data used in an information resource must be kept confidential and properly secured. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted, the data must still be protected as confidential and secured.

8.4 All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.

8.5 Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs form misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized, and controlled.

8.6 All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. University employees and other users of campus owned information resources must abide by all license agreements and must not illegally copy licenses software. The IRM reserves the right to remove any unlicensed software from any computer systems.

8.7 The IRM reserves the right to remove any non-business related or unauthorized software or files from any computer system or network service. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, IMAP email, music files, image files, freeware, shareware, or other software such as Software as a Service (SaaS) systems that reside in the cloud (such services may be blocked at the firewall to prevent data leakage).

Related Statutes, Policies, Regulations and Rules

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

Security Control Standards Catalog

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

System Policy 07.01 Ethics

System Regulation 10.02.01 Control of Fraud, Waste and Abuse

System Policy 33.04 Use of System Resources

System Regulation 29.01.02 Use of Licensed Commercial Software

---

Contact Office

Office of Information Resources Management 936-261-9350
