UAP Purpose

This University Administrative Procedure (UAP) provides procedures to ensure awareness and compliance with applicable statutes, regulations and mandates regarding the appropriate management and responsible use of the Internet/Intranet.

Definitions

Internet – the computer network linking smaller networks worldwide.

Intranet – the restricted access computer network within Prairie View A&M University (PVAMU) which uses software and protocols developed for the Internet.

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

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 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

PVAMU supports and encourages Internet and Intranet use for the benefits of a business function to all users of information resources. University information resources are strategic assets of the State of Texas and thus must be managed as valuable state resources.

This procedure is established to achieve the following:

1.1 To ensure compliance with applicable statutes, regulations, and mandates regarding the management of Internet/Intranet use;

1.2 To establish acceptable practices regarding the use of the Internet/Intranet; and,
1.3 To educate individuals who may use the Internet/Intranet with respect to their responsibilities associated with such use.

2. **APPLICABILITY**

2.1 This UAP applies to all PVAMU information resources. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this UAP are implemented. As stated in Texas Administrative Code 202.71, based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude control measures provided for in Texas Administrative Code Chapter 202. Any such exceptions shall be justified, documented in writing and approved by the Information Security Officer as part of the risk assessment process. The intended audience is all users of PVAMU information resources.

2.2 Exclusions are of two types:

2.2.1 A system specific exclusion may be granted to address the circumstances or business needs relating to an individual program or department. Requests for exclusions of this type are to be initiated by the information resource owner or designee.

2.2.2 An enterprise-wide exclusion may be issued to address circumstances that affect the University as a whole. Requests for exclusions of this type may be initiated by any person, office or department, or by the Chief Information Officer or designee.

3. **PROCEDURES**

3.1 Procedures regarding the protection of information resources against malicious codes; web site standards; purchases of information technology equipment or software; and, personal conduct can be found in the following policies and procedures:

UAP 25.07.03.P0.01 Acquisition of Goods and Services;

UAP 29.01.03.P0.20 Acceptable Use;

UAP 29.01.04.P0.01 Web Accessibility and Usability;

UAP 29.01.03.P0.18 Incident Management; and,

UAP 29.01.03.P0.05 Malicious Code.

3.2 No PVAMU confidential information shall be made available via University web sites without ensuring that the material is accessible to only authorized individuals or groups.

3.2.1 All confidential information transmitted over external networks must be encrypted.
3.2.2 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

3.3 Directors and department heads, or their equivalent, have the responsibility to ensure that appropriate security practices, System Regulations, University Rules and UAPs for PVAMU Internet/Intranet use are implemented and adhered to within their respective departments. Failure to comply with these requirements could result in disciplinary actions.

Related Statutes, Policies, Regulations and Rules

- System Regulation 29.01.03 Electronic Information Service Access and Security
- System Regulation 29.01.04 Accessibility of Electronic Information Resources
- UAP 25.07.03.P0.01 Acquisition of Goods and Services
- UAP 29.01.03.P0.20 Acceptable Use
- UAP 29.01.04.P0.01 Web Accessibility and Usability
- UAP 29.01.03.P0.18 Incident Management
- UAP 29.01.03.P0.05 Malicious Code

Contact Office

Office of Information Resources Management 936-261-9350