**UAP Purpose**

The purpose of this University Administrative Procedure (UAP) is to provide guidelines regarding the use of email through University owned information resources. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code 202.75 Information Resources Security Safeguards.

**Definitions**

**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.

**Sensitive Personal Information** - an individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- Social security number;
- Driver’s license number or government-issued identification number; and,
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

**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.

**Encryption (encrypts, encipher, or encode)** - the conversion of plain text information into a code or cipher-text using a variable, called a “key” and processing those items through a fixed algorithm to create the encrypted text that conceals the data’s original meaning.

**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. Since a large portion of University business is conducted using email, it is important that email services function in an efficient and reliable manner.

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 202.75 Information Resources Security Safeguards, 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 Prairie View A&M University (PVAMU) information resources. The intended audience for this UAP includes, but is not limited to, any University employee, student, guest, or visitor that may use any University information resource that has the capacity to send, receive or store email.

3. **PROCEDURES**

3.1 Whenever possible, the PVAMU email system(s) is/are the official communication system for University business.

3.2 Prohibited Uses:

3.2.1 The PVAMU email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any PVAMU employee should report the matter to their supervisor immediately.

3.2.2 Individuals must not send, forward or receive confidential or sensitive PVAMU information through non-PVAMU email accounts. Examples of non-PVAMU email accounts include, but are not limited to: Hotmail, Yahoo mail, Gmail, and email provided by other Internet Service Providers (ISP).

3.2.3 No sensitive and/or confidential PVAMU material should be transmitted via PVAMU email unless encrypted. See UAP 29.01.03.P0.22 Encryption of Confidential and Sensitive Information.
3.3 Personal Use:

3.3.1 Using a reasonable amount of PVAMU resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a PVAMU email account is prohibited. Virus or other malware warnings and mass mailings from PVAMU shall be approved by the Assistant Vice President for Information Resources Management before sending. These restrictions also apply to the forwarding of mail received by a PVAMU employee.

3.4 Monitoring:

3.4.1 PVAMU employees shall have no expectation of privacy in anything they store, send or receive on the University’s email system. PVAMU may monitor messages without prior notice. PVAMU is not obliged to monitor email messages.

3.5 Enforcement:

3.5.1 Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.6 Employees are prohibited from downloading and using personal IM software to transmit messages via the Internet. Any requests for exceptions must be routed to the ISO.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources
System Regulation 29.01.03 Electronic Information Services Access and Security
Texas Administrative Code 202.75 Information Security Standards
UAP 29.01.03.P0.22 Encryption of Confidential and Sensitive Information

Contact Office

Office of Information Resources Management 936-261-9350

Approved:

Michael L. McFrazier Date
Vice President for Administration