

**PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE**

29.01.03.P0.03 Information Resources – Email Usage

Approved May 26, 2009

Revised – May 4, 2011

Next Scheduled Review (May 2012)

1. PURPOSE

- 1.1 This UAP provides procedures regarding the use of email through University owned information resources.

The purpose of the implementation of this UAP is to provide a set of measures that will mitigate information security risks associated with email use. There may also 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 UAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and submitted to the Information Security Officer (ISO) for approval prior to implementation.

- 1.2 The intended audience of this UAP is any University employee, student, guest, or visitor that may use any University information resource that has the capacity to send, receive or store email.

2. DEFINITIONS

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

- 2.2 **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:

2.2.1 Social Security Number;

2.2.2 Driver's license number or government-issued identification number (including UIN or Student ID); and,

2.2.3 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.

- 2.3 **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.

2.4 **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.

3. PROCEDURES AND RESPONSIBILITIES

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 to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, 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 Prairie View A&M University information through non-Prairie View A&M University email accounts. Examples of non-Prairie View A&M University email accounts include, but are not limited to: Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

3.2.3 No sensitive and/or confidential Prairie View A&M University 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. 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 PVAMU VP Business Affairs before sending. These restrictions also apply to the forwarding of mail received by a PVAMU employee.

3.4 Monitoring. 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. 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 Information Security Officer.

Contact Office: Information Security Officer; 936-261-2126