

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

29.01.03.P0.21 Information Resources - Peer-to-Peer File Sharing

Approved (November 4, 2009)

Next Scheduled Review (November 2009)

I. PURPOSE

- 1.1 This University Administrative Procedure (UAP) provides procedures regarding the use of Peer-to-Peer (P2P) file sharing 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 P2P 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 reported to the designated Information Security Officer (ISO).

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 use P2P technology to download, copy, store or transfer copyrighted material.

2. DEFINITIONS

- 2.1 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.
- 2.2 Peer-to-Peer File (P2P) Sharing Software: computer software, other than computer and network operating systems, that has as its primary function the capability of allowing the computer on which the software is used to designate files available for transmission to another computer using the software, to transmit files directly to another computer using the software, and to request transmission of files from another computer using the software.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Users of state computers or networks shall not download/install any P2P software onto state computers, networks, or mobile computing device (PDA) without specific authorization in writing from the Information Security Officer (ISO)

- 3.2 Authorized network users may use P2P technologies for official business only if specifically authorized in writing by ISO.
- 3.3 If any copied or transferred data or information is licensed or copyrighted, the ISO and authorized network user will ensure that all notifications and costs are documented and approved.
- 3.4 Users of state institution computers and networks should keep in mind that all P2P may be recorded and stored along with the source and destination. Faculty, staff and students have no right to privacy with regard to P2P usage on PVAMU computers and networks. Management has the ability and right to view users' P2P on state institution systems.
P2P files recorded onto state institution computers or networks are the property of the institution. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.
- 3.5 Accessing; viewing downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (i.e., visual, textual, or auditory entity) on Prairie View A&M University computers or networks is strictly prohibited.

Contact Office: Information Security Officer 936-261-2126