PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.21 Information Resources – Use of Peer-to-Peer File Sharing Software
Approved November 4, 2009
Revised August 29, 2013
Revised December 7, 2018
Next Scheduled Review: December 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to provide specific guidance regarding the appropriate use of Peer-to-Peer (P2P) file sharing software through Prairie View A&M University (PVAMU) owned information resources. 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

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.

Peer-to-Peer (P2P) File 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.

University Network User - anyone owning and/or responsible for the operation of a computer attached to the PVAMU network.

Official Procedures and Responsibilities

1. GENERAL

1.1 This UAP describes requirements related to the appropriate use of peer-to-peer (P2P) file-sharing software. As an institution of higher education, PVAMU permits legal and authorized software of this type, as long as the software is appropriately licensed and its use does not violate any university rules or administrative

procedures, system policies or regulations, or any applicable state and federal laws. Generally, P2P software should be used only for legitimate university business. Use of P2P file sharing software may require special attention by individual users in order to prevent the unintended or inappropriate distribution of files.

1.2 PVAMU is committed to protecting copyrighted material. The unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing may subject you to civil and/or criminal penalties. You may be at risk of litigation if you share files illegally or even if you appear to do so. Violators of the Digital Millennium Copyright Act (DMCA) can be punished by substantial fines. Individuals also may be held civilly liable for actual damages or lost profits, or for statutory damages. Attempting to profit from file sharing can even result in a prison sentence. For more information on copyright laws and how they may affect you, please visit http://www.copyright.gov/.

1.3 In accordance with provisions of the Higher Education Opportunity Act (HEOA), Information Technology Services (ITS) has developed and implemented plans to effectively combat the unauthorized distribution of copyrighted material by users of the PVAMU network. (See P2P Security Program.) Every effort has been made not to interfere or impede network traffic for University business, educational, and research activities that support the mission of the University.

1.4 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 any device attached to the PVAMU network. The intended audience for this UAP includes, but is not limited to, any university employee, student, or visitor that may use any university information resource that has the capacity to use P2P technology to download, copy, store or transfer copyrighted material.

3. PROCEDURES

3.1 Users of state computers or networks shall not download/install any P2P software onto state computers, networks, or mobile computing devices 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 the ISO.

3.3 Any PVAMU network user who utilizes P2P file sharing software should be thoroughly familiar with the proper use, options, and default settings of the particular P2P

program. The user must ensure that the P2P program configuration does not allow automatic/unintended file sharing.

3.4 Insecurely configured file sharing programs may be cause for removal of network access from the hosting computer.

3.5 For instances in which the department is the owner-custodian or custodian of a system using P2P software, the department is responsible for ensuring compliance with this procedure. Each department will be asked to identify uses of P2P file sharing software and report/document the installations/uses as part of the annual Information Security Risk Assessment.

3.6 Users of PVAMU computers and networks should keep in mind that all P2P activity may be recorded and stored along with the source and destination identifiers. 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 PVAMU computers or networks are the property of the University. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

3.7 Personal use of P2P should not impede the conduct of PVAMU business. 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 PVAMU computers or networks is strictly prohibited. (Refer to UAP 29.01.03.P0.20 Acceptable Use.) Employees should not use P2P on state computers or networks for any personal monetary interests or gain.

3.8 Any violation or inappropriate use of P2P file sharing software shall be reported immediately to the ISO and appropriate actions will be taken by the Office of Student Conduct for students and the Office of University Compliance for employees, to possibly include disciplinary action up to and including termination.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

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

---

Contact Office

Office of Information Resources Management 936-261-9350
