The Division of Information Technology
University Information Security Standards

Information Security Standard – Peer-to-Peer (P2P)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. GENERAL

This information security standard describes requirements related to the appropriate use of peer-to-peer (P2P) file-sharing software. As an institution of higher education, West Texas A&M University 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 procedures, Texas A&M University System policies, regulations, or any applicable state and federal laws. The Governor of the State of Texas issued Executive Order RP58 relating to P2P file sharing in partnership with the Texas Department of Information Resources. The official order is available at: http://governor.state.tx.us/news/executive-order/3630.

West Texas A&M University 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 can be punished by substantial fines. Individuals also may be held civilly liable for actual damages or lost profits, or for statutory damages up to $150,000 per infringed copyright. 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 for detailed information related to the Digital Millennium Copyright Act (DMCA).

In accordance with provisions of the Higher Education Opportunity Act (HEOA), the Division of Information Technology has developed and implemented plans to effectively combat the unauthorized distribution of copyrighted material by users of the West Texas A&M University network. 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.

In compliance with DMCA requirements, West Texas A&M University must respond expeditiously to notices of alleged copyright infringement. An individual usually finds out about a notice when they receive an email from Network Services, the Information Technology Service Center or the Information Security Officer.

This email informs the individual that a copyright holder has sent the University a notice of alleged infringement, which identifies the offender's IP address. The individual is requested to confirm receipt of the notice, implement all actions specified, and take all appropriate actions. If the individual ignores the request, then other actions may ensue including disabling the network connection or disciplinary action up to and including termination. In the case of students, the process may involve convening a required hearing before Student Judicial Affairs. Student Judicial Affairs may impose sanctions on the student that may range from a letter of reprimand to expulsion from the university.

2. APPLICABILITY

This information security standard applies to all individually or University owned computing systems attached to the West Texas A&M University network. The intended audience includes all University network users.

3. DEFINITIONS

3.1 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.

3.2 University Network User: anyone owning and/or responsible for the operation of a computer attached to the West Texas A&M University network.

4. PROCEDURES

4.1 Any University network user using legal, authorized 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 or disrupt network traffic. P2P software is subject to audit review by information technology personnel at all times.

4.2 Insecurely configured file sharing programs may be cause for removal of all network access from the hosting computer and/or user. This includes, but is not limited to, Windows file sharing with no password and other systems with unauthenticated and/or unrestricted uploading and/or downloading capabilities.

4.3 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.

4.4 Any violation or inappropriate use of P2P file sharing software shall be reported immediately to the information security officer (ISO) and appropriate actions will be taken, including disciplinary action up to and including termination.

5. PRIVACY

Users of university computers and networks should keep in mind that all P2P activity may be recorded and stored along with the source and destination identifiers. Employees have no right to privacy with regard to P2P usage on university computers and networks. Management has the ability and the right to view user's P2P on state institution systems. P2P files recorded onto university 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.

6. RESTRICTIONS

Personal use of P2P should not impede the conduct of university 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 university computers or networks is strictly prohibited. Employees should not use P2P on state computers or networks for any personal monetary interests or gain.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer