STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.25 Information Resources – Use of Peer-to-Peer File Sharing Software

Approved October 24, 2006
Revised April 27, 2010
Revised February 10, 2012
Revised August 14, 2013
Next Scheduled Review: August 13, 2018

Standard Administrative Procedure Statement

This procedure describes requirements related to the appropriate use of peer-to-peer (P2P) file sharing software. Being an institution of higher education, use of any software is allowed as long as the software is appropriately licensed, and its use does not violate any Federal or State laws, System policies or regulations, or University rules or procedures. Generally, P2P software should be used only for legitimate University business. However, as with other software, brief and occasional personal use of P2P software is allowable if such use is in accordance with the rule for incidental use (University Rule 29.01.03.M3). Use of P2P file-sharing software may require special attention by individual users in order to prevent the unintended or inappropriate distribution of files.

Definitions

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 Texas A&M University network.

Official Procedure/ Responsibilities/ Process

---

1. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all individually or University owned computing systems attached to the Texas A&M University network. The intended audience includes all University network users.

The information resource owner or designee (e.g., custodian or owner), is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management consideration and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 29.01.03.M1.27 *Exclusions from Required Risk Mitigation Measures*.

2. PROCEDURES

2.1 Any University 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.

2.2 Insecurely configured file sharing programs may be cause for removal of network access from the hosting computer. This includes, but is not limited to, Windows file sharing without password protection and other systems with unauthenticated and/or unrestricted uploading and/or downloading capabilities.

2.3 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. 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 Assessment, Awareness, and Compliance (ISAAC) process (University SAP 29.01.03.M0.01 *Security of Electronic Information Resources*).

2.4 Any violation or inappropriate use of P2P file sharing software shall be reported in accordance with University Rule 32.01.99.M1 *Complaint Procedures for Electronic Information* by sending an email message to complaint@tamu.edu. A problem ticket will be opened and routed to the appropriate personnel assigned by the Office of the Associate Vice President for Information Technology & Chief Information Officer to handle the problem.

Related Statutes, Policies, or Requirements

University SAP 29.01.03.M0.01 *Security of Electronic Information Resources*

University Rule 29.01.03.M3 *Incidental Computer Use*

University Rule 32.01.99.M1 *Complaint Procedures for Electronic Information*

Contact Office

CONTACT: Information Technology Networking and Information Security (NIS)

OFFICE OF RESPONSIBILITY: Associate Vice President for Information & Chief Information Officer Technology