Peer-to-Peer (P2P) File Sharing Policy **August 1, 2013**

Purpose

While Peer-to-Peer (P2P) technologies have many important and legitimate uses, P2P file sharing applications are often used to obtain copyrighted materials (e.g. music, movies, videos, text, etc.) without the permission of the owner or distributor while utilizing a disproportionate amount of network bandwidth and leaving the user's computer vulnerable to computer viruses. Running P2P file sharing applications on ACOM computers also introduces the risk of inadvertently sharing files containing sensitive ACOM Data. The purpose of this policy is to articulate ACOM's position on the use of Peer-to-Peer file sharing applications and the unauthorized acquisition or distribution of copyrighted or licensed material.

Scope

This policy applies to all students, faculty and staff, and other individuals using ACOM information technology resources or data.

Effective Date

This policy became effective on August 1, 2013.

Authority

This policy responds to requirements in the Higher Education Opportunity Act of 2008 that colleges develop plans to effectively combat the unauthorized distribution of copyrighted materials.

Policy

1. Use of Peer-to-Peer file sharing applications for the unauthorized acquisition or distribution of copyrighted or licensed material is prohibited on any ACOM computer or ACOM network. Furthermore, P2P file sharing applications commonly used for these illicit purposes may not be installed on any ACOM computer, and technological deterrents will be used to block their use on the ACOM network.

2. Any violation of this policy may result in the suspension of access to network resources or other appropriate college discipline, up to and including termination of employment and/or expulsion. In addition, the unauthorized acquisition or distribution of copyrighted or licensed material, including unauthorized peer-to-peer file sharing, may subject individuals to civil and criminal liabilities.

3. ACOM will annually inform students of this policy and associated procedures, consistent with the requirements of the Higher Education Opportunity Act of 2008.

Definitions

1. Digital Millennium Copyright Act (DMCA) - A federal law passed in 1998 that revised copyright law for the digital environment to, among other things, define how alleged copyright infringements are to be handled and establish liability limitations for "online service providers."

2. Peer-to-Peer (P2P) - A network environment where participants share their resources (such as files, disk storage, or processing power) directly with their peers without having to go through an intermediary network host or server.

3. Peer-to-Peer file sharing applications - Programs or services that use P2P technology to share music, movies, software, or other digitally stored files.

4. ACOM computer - Any computer considered to be the property of ACOM.

5. ACOM network - Any part of ACOM's data network physically located on the Dothan, Alabama campus. This includes devices on the network assigned any routable and non-routable IP addresses, typically 10.X.X.X, respectively, and applies to ACOM's wireless network and the network serving ACOM's student residence hall at Summer Hill Apartments.

Roles and Responsibilities

1. Director of Information Systems - ACOM - the DIS-ACOM will determine the set of prohibited P2P file sharing applications, with input from ACOM's Security Incident Response Team. The DIS-ACOM is also responsible for technology-based deterrents used to enforce this policy.

2. Dean of Student Services - is responsible for notifying students about this policy at the beginning of every fall semester.

Implementing Procedures

1. The Director of Information Systems - ACOM will maintain and publish a list of P2P file sharing applications that are commonly used for unauthorized acquisition or distribution of copyrighted or licensed material. Examples include but are not limited to Ares, Bit Torrent, eDonkey (aka eMule), and Gnutella (aka LimeWire). These applications cannot be installed on ACOM computers and will be blocked on the network using appropriate technology-based deterrents.

2. Notices of alleged copyright infringement per the Digital Millennium Copyright Act (DMCA) will be handled according to the following procedure.

Related Laws, Regulations, or Policies

1. ACOM copyright and intellectual property information

2. ACOM Information Technology Usage Policy

3. ACOM Security for Information, Computing and Network Resources policy

4. ACOM procedures for removing compromised computers from the network

5. ACOM Student Conduct Code

6. Higher Education Opportunity Act of 2008 (H.R. 4137) - http://www.ed.gov/policy/highered/leg/hea08/index.html

7. Criminal penalties and civil remedies for violation of Federal copyright laws are summarized in the Congressional Research Services report titled, "Intellectual Property Rights Violations: Federal Civil Remedies and Criminal Penalties Related to Copyrights, Trademarks, and Patents "http://assets.opencrs.com/rpts/RL34109_20081031.pdf.

8. U.S. Copyright Office information on designating an agent for notification of claims of infringement: http://www.copyright.gov/onlinesp/

9. Summary of the DMCA: www.copyright.gov/legislation/dmca.pdf
http://www.copyright.gov/legislation/dmca.pdf

10. Full text of the DMCA: www.copyright.gov/legislation/pl105-304.pdf
http://www.copyright.gov/legislation/pl105-304.pdf

Questions/Waivers

The Director of Information Systems - ACOM is responsible for this policy. The DIS-ACOM or designee must approve any exception to this policy. Questions relating to this policy should be directed to ACOM designated copyright agent. Questions about the list of prohibited P2P file sharing applications should be directed to the Director of Information Systems - ACOM.