Auburn University at Montgomery
Policies and Procedures

Title: Policy on Peer-to-Peer (P2P) File Sharing

Responsible Office: Information Technology Services

I. PURPOSE

The purpose of this policy is to safeguard Auburn University at Montgomery's (AUM) bandwidth and technology resources by prohibiting unauthorized peer-to-peer (P2P) file sharing.

II. POLICY

The use of P2P file sharing applications on the AUM network without the prior authorization of the CIO is strictly prohibited. In addition to consuming bandwidth and technological resources, P2P file-sharing also exposes the University network to viruses, spyware and other attacks. P2P is also frequently used to illegally distribute copyrighted works.

III. EFFECTIVE DATE

July 1, 2010

IV. APPLICABILITY

All students, faculty, staff, and contractors who have access to the AUM network are subject to this policy.

V. RESPONSIBILITY

The provisions of this policy will be implemented and enforced by the Chief Information Officer.

VI. DEFINITIONS

Peer-to-peer (P2P) File Sharing: The sharing of files between computers via the internet using P2P software. P2P software allows users to both share content from their computers and to connect to other, similarly configured computers without going through a server, for the purpose of downloading or transferring electronic content.

VII. GENERAL PROCEDURES

A. File Sharing Risks:

Copyright
There are legal and legitimate academic, research, and personal uses of P2P applications. However, many people use P2P file sharing to distribute copyrighted files without the permission of the copyright owner. Such use is illegal and subjects the user to **personal liability** in copyright infringement claims. Copyrighted works in such files should not be stored, transmitted, or used on University owned computers or servers without explicit permission of the copyright holder.

Bandwidth and Network Resources
AUM provides shared computing and electronic communication resources for faculty, staff, and students. The use of P2P applications often uses a great percentage of those shared resources. The result is that other network activities, such as academic research and file transfers, may operate at reduced efficiency.

Security
P2P applications can copy files from unknown resources to the user's computer, making the user's computer vulnerable to hacking and computer viruses, and putting the user's personal and private data at risk. These viruses could then be transferred to other systems on the network, putting other users' computers and files at risk.

B. Regulation

Any use of P2P applications that is in violation of law, University policy, or in ways that interfere with the University's network integrity or security is prohibited.

C. Procedure

The AUM Information Technology Services (ITS) department will monitor the AUM network for P2P file sharing activity.

VIII. ENFORCEMENT/SANCTIONS

A. Upon discovery than an individual has committed an apparent violation of this policy, ITS will immediately terminate that individual's access to the AUM network. ITS will then notify the user and require that the user immediately cease the prohibited activity and delete any files that violate copyright law. ITS may inspect the user's system for illegal files or applications before restoring network access.

B. The user will be required to submit a signed certification page that states that the user understands the ramification of the offense. (See attached)
C. Network access will be restored no sooner than two business days after receipt of the certification page.
D. Furthermore, violation of this policy can result in disciplinary action, including termination of a user's University computer account.
E. The existence and imposition of University sanctions **do not** protect members of the campus community from any legal action by external entities or the University itself. For example, individuals found guilty of online infringement of copyrighted music can receive punishment of up to five years in prison and/or $250,000.00 in fines. Individuals may be held liable for damages and lost profits up to $150,000.00 per infringed copyright. The minimum penalty is $750.00.

IX. EXCLUSIONS

No employee, student, or contractor is excluded from this policy without prior approval of the CIO. A request to use P2P software for a legitimate academic need must be submitted to the CIO for review prior to the use of the software on University equipment.

X. LEGAL ALTERNATIVES TO FILE SHARING

Music and movies may be legally obtained through online subscription services or from sites officially permitted by the copyright holder to offer certain downloads. Some of these "free" or "pay-for-play" services are listed below. AUM does not recommend or endorse any one of these services.

Music	**Movies**
www.amazon.com/mp3	www.atomfilms.com
www.ruckus.com	www.cinemanow.com
www.napster.com	www.itunes.com
www.iTunes.com	www.movieflix.com

XI. INTERPRETATION

The Chief Information Officer is responsible for any interpretation of this policy.

APPROVAL TO PROCEED: _____ **DATE:**_____

Auburn University at Montgomery

P2P File Sharing Violation
Certification Page

I understand that I have been found in violation of Auburn University at Montgomery's P2P File Sharing policy and that a subsequent violation will result in immediate suspension of my network access and referral to the AUM Committee on Discipline (for students) or to my appointing/sponsoring authority (for all others). I understand that, for a subsequent violation, my network access will not be restored until the case is adjudicated by the AUM Committee on Discipline (for students) or reviewed and decided by my supervisor (for all others). I understand that a subsequent violation may result in permanent loss of network access and/or referral of my name to appropriate authorities for civil or criminal prosecution.

Signature	Date
Printed Name	Employee or Student ID Number

Please print and sign an additional copy of this page for your records. An original copy must be delivered to the Chief Information Officer.

Your network access may be restored no earlier than two business days after receipt this page.