October 2022

Document title: **[Peer-To-Peer File Sharing Policy – October 2022]**

Approval date: **[January 2016]**

Purpose of document: **[** The purpose of this policy is to outline the acceptable use of AUC IT resources with regard to peer to peer applications. These rules are in place to protect the Staff, Faculty, Students, and AUC community.**]**

Office/department responsible: **[Office of Information Security]**
Approved by: **[Wessam Maher, Principal Campus Information Security Officer]**

Document classification level: **[PUBLIC]**

Document accessible: **[http://www.aucegypt.edu/about/policies/Pages/default.aspx]**

Document includes: **[Policy]**

Related documents/see also: **[AUC Data Governance Policy, Information Security Policy, Electronic Mail Email Policy, Acceptable Use Policy, Peer to Peer Sharing Policy]**

AUC Policy Banning Peer-To-Peer File Sharing In Accordance With The Higher Education Opportunity Act Of 2008

Policy Statement

In compliance with the Higher Education Opportunity Act of 2008 (HEOA), the American University in Cairo adopts the following plan in order to deter the unauthorized distribution of copyrighted material by users of the university's network while at the same time not unduly interfering with educational and research-related use of the network.

Reason for Policy/Purpose

The purpose of this policy is to outline the acceptable use of AUC IT resources at AUC. These rules are in place to protect the Staff, Faculty, Students, and AUC community. Inappropriate use exposes AUC to risks, including information disclosure, virus attacks, compromise of network systems and services, and legal issues.

Who Approved This Policy

Wessam Maher, Principal Campus Information Security Officer

Who Needs to Know This Policy

Entire AUC Community

Web Address for this Policy

http://www.aucegypt.edu/about/policies/Pages/default.aspx

Contacts

Responsible University Official: Wessam Maher, Chief Information Security and Risk Officer.
Responsible University Office: Office of Information Security.

If you have any questions on the policy or procedure, you may send an e-mail to infosec@aucegypt.edu

Definitions

Term (alphabetical order)	**Definition as it relates to this policy**
P2P	Peer to Peer

Policy/Procedures

The use of peer-to-peer computer file-sharing programs (e.g., BitTorrent, KaZaA, Morpheus, Limewire, iMesh, Gnutella, Grokster, and all similar programs and their successors) that are primarily employed to share copyrighted works is prohibited on the campus network. Where possible, peer-to-peer communication will be intercepted and blocked by network control systems. The use of methods designed to evade that blocking is prohibited. Specific exceptions to this policy may be approved by the Chief Technology Officer in instances where such programs will be used exclusively for educational/research purposes and in a manner that complies with the Egyptian and US copyright laws.

Technology-Based Deterrents

AUC employs a multi-layer of technologies to combat illegal file sharing, using Intrusion Prevention and application control features to block delectable P2P traffic across the university. Also, bandwidth management and throttling are employed to limit bandwidth consumption and the number of connections that can be utilized by P2P to hinder P2P activity.

Educating the Community

The university uses numerous mechanisms to educate and inform the community by using several channels to communicate with its community, such as AUC news website, Email Announcements targeted to Students, Faculty, and Staff. In addition, the students who run publications will be invited to cover this topic. The University is planning to include this policy in the student, faculty, and staff handbooks in the future.

Procedures for Handling Unauthorized Distribution of Copyrighted Material

The Information security office traces the source of the distribution of illegal content. Upon successful identification of the device used and or the user, the Information security office reports the incident to the appropriate disciplinary entity based on the user role at AUC; Accordingly, Students, Faculty, and Staff cases are forwarded to VP of Student Affairs, Provost, Human Resources Executive Director respectively.

Legal Alternatives to Downloading

AUC has not made any special arrangements of this type.

Procedures for Periodic Review of This Plan

On a Semi-annual basis, the Information Security office conducts tests to ensure the effectiveness of the solution in place and accordingly decides if further enhancements should be implemented or not.

Enforcement:

Any user found to have violated this policy (or part thereof) may be subject to disciplinary action, up to and including termination of employment or dismissal from the University.

Forms/Instructions

Kindly contact the IT Help Desk for more info, at support@aucegypt.edu

History/Revision Dates

Origination Date:	June 2010
Last Amended Date:	January 2016
Last Review Date:	October 2022
Next Review Date:	October 2025