PEER-TO-PEER POLICY

Policy Statement

The abuse of network resources to illegally obtain and distribute media or software, through peer-to-peer (P2P) networks, Usenet, or direct download, is a problem for many institutions of higher education. While The University of Southern Mississippi (USM) recognizes that there are legitimate uses for the previously mentioned applications, the University also understands that significant risks are implicit in the use of such applications. The Higher Education Opportunities Act of 2008 (HEOA) [34 CFR Section 668], specifically requires universities to take steps to mitigate illegal downloads and Peer-to-Peer (P2P) abuse. The University does not seek to ban any method for distributing or acquiring digital media, and will continue to support academic freedom and any technologies that can be used to foster collaboration. However, USM must also protect its assets and reputation, as well as comply with federal regulations.

Reason for Policy/Purpose

This policy is required for the effective communication of University policies regarding P2P usage. It has been revised in order to limit the exposure of the University to security risks and liabilities associated with the irresponsible use of University resources for illegal file sharing activities.

Who Needs to Know This Policy

This policy applies to all individuals, regardless of affiliation or status with the University, at such time they are using any of the following resources: computer workstations, laptops, servers, networked appliances, and any other device if such device is owned by USM; or any device utilizing University network resources, even if that device is privately owned by an individual or third party.
Definitions

**Device:** An instrument used to process or store digital records and data; including, but not limited to, personal computers, workstations, laptops, tablets, externally connected hard drives, flash drives, removable media, and any other equipment or media capable of electronically storing data.

**Digital Millennium Copyright Act (DMCA):** United States copyright law that complies with World Intellectual Property Organization treaties, specifically addresses digital access control and digital rights management, and enhances penalties for copyright infringement over the Internet.

**Downloading:** Network trafficking of data files originating from an external network and destined for the USM network.

**Family Educational Rights and Privacy Act (FERPA):** Federal law that protects the privacy of, and access to, student education records.

**Illegal Download:** Any downloaded file that was obtained in violation of law, or is itself against the law to possess, distribute, duplicate, or create.

**Log:** Collection of information, typically used to document activity and events.

**Peer-to-Peer (P2P):** Direct data communication between two or more network capable devices over the Internet or other network, usually for the purpose of sharing any data file (including, but not limited to, music, pictures, video, software, and documents).

**P2P application:** Any application that allows a network-capable device to participate in one or more P2P networks.

**P2P network:** A collection of distributed network-capable devices participating in P2P activity.

**Personally Identifiable Information (PII):** Information, when used by itself or with other information, can be used to uniquely identify an individual.

**Protected Health Information (PHI):** Individually identifiable information concerning a person’s health, maintained by a covered entity or business associate, including demographic information.

**Sharing:** The action and activity of making any data file available to one or more P2P networks.

**Uploading:** Network trafficking of data files originating from the USM network and destined for an external network.

Policy/Procedures

1. **Prohibited Activity**
   1.1. This policy strictly prohibits, by any method, the distribution, downloading, uploading, or sharing of any material, software, data, document, sound, picture, or any other file that is:
      1.1.1. Specified as illegal by any federal or state law, statute, proclamation, order, or decree.
1.1.2. Copyrighted and not authorized for distribution by the copyright owner.
1.1.3. Considered to be proprietary, privileged, private, or otherwise vital to the operation of the University; including, but not limited to, personnel, student, financial, or strategic records and documents, or any material governed by federal and state regulations.
1.1.4. Malicious software for the purpose of deployment or implementation with ill-intent.

1.2. Any P2P activity is strictly forbidden for the following instances:
   1.2.1. On devices used to process, store, collect, or transmit:
      1.2.1.1. Sensitive Personally Identifiable Information (PII)
      1.2.1.2. Protected Health Information (PHI)
      1.2.1.3. Information protected by the Family Educational Records and Privacy Act (FERPA)
      1.2.1.4. Any other information affected by regulations and standards compliance.
   1.2.2. On any device hosting or providing network accessible services to the public or the University community, including but not limited to: websites, forums, educational and research software, and learning management systems.
   1.2.3. On computer workstations and other network devices readily accessible to multiple users, and in computer labs.
   1.2.4. Laptops, computer workstations, and any other device provided by Information Technology Services (iTech) through the Equipment Services department.

1.3. Users of USM resources may not attempt to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the University for the purpose of P2P mitigation.

2. Permitted Activity
2.1. Any P2P activity or network traffic that is not explicitly prohibited by this policy, another University policy, state law, federal law, or any other regulation, is generally permissible. Additional information may be found in Appendix A.

3. Rights and Responsibilities
3.1. All individual persons or groups utilizing USM networks, including but not limited to, USM employees, students, guests, external business entities, and non-profit entities shall bear legal and financial responsibility for events or consequences resulting from their own use of network resources.
3.2. Individual departments, colleges, administrative areas, and other entities must respond in a timely and efficient manner to all inquiries and complaints that arise in regard to this policy.
3.3. iTech and USM are required by federal law to report certain illegal activities to specified law enforcement agencies without notice to the user or the appropriate department.

4. Technology Mitigation
4.1. The University shall deploy a technical control at the perimeter of the USM network that must be configured to employ a method of detecting known P2P protocols and application traffic.
4.2. The technical control must be configured to drop network connections identified as P2P traffic and log the event.

5. Enforcement and Penalties
5.1. University Community:
   5.1.1. Any faculty, staff, or student found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion, and/or termination of employment in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.

5.2. Individuals not affiliated with USM:
   5.2.1. Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

5.3. Internet Access:
   5.3.1. Any individual, regardless of their affiliation or status with the University, can have their Internet access permanently suspended for egregious or multiple violations of this policy.
   5.3.2. A notice of alleged copyright violation that adheres to requirements for claiming infringement specified by the Digital Millennium Copyright Act (DMCA), will be referred to as a "DMCA notice." DMCA notices received by USM citing an IP address originating from the USM network will be researched, and if possible matched with the individual responsible for the abuse.

   5.3.2.1. Students:
      5.3.2.1.1. For the first and second occurrence of one or more DMCA notices received during a 24-hour period, the notice(s) will be forwarded directly to the student’s email address along with a reminder of the P2P and Acceptable Use policies.
      5.3.2.1.2. For the third occurrence of a DMCA notice, or multiple DMCA notices received during a 24-hour period, any associated wired network connection will be disabled and the student's wireless Internet access will be temporarily suspended until that student receives counseling by the Dean of Students.
      5.3.2.1.3. The fourth occurrence of a DMCA notice will result in any associated wired network connection disconnection and the student's wireless account being permanently suspended.

   5.3.2.2. Faculty, Staff and other University employees:
      5.3.2.2.1. For the first occurrence of a single DMCA notice, or multiple DMCA notices received during a 24-hour period, the notice(s) will be forwarded directly to the employee along with a reminder of the P2P and Acceptable Use policies.
      5.3.2.2.2. For the second occurrence of a DMCA notice, or multiple DMCA notices received during a 24-hour period, the notice(s) will be forwarded directly to the employee and the employee's supervisor or department head, along with a reminder of the P2P and Acceptable Use policies.
5.3.2.2.3. For the third occurrence of a DMCA notice, or multiple DMCA notices received during a 24-hour period, any associated wired network connection will be disabled and the employee's wireless account will be temporarily suspended pending discussion between the employee's supervisor or department head and the Technology Security Officer (TSO).

5.3.2.2.4. The fourth occurrence of a DMCA notice will result in the employee's wireless account being permanently suspended.

5.3.2.3. For all users of the “USM Public” wireless network:

5.3.2.3.1. The individual will have their access to the network permanently banned if USM receives just one DMCA notice linked to the guest's account, or on any other offense of this policy.

5.3.2.4. For all non-University business entities:

5.3.2.4.1. Violations of this policy will be addressed as described in any contract with that entity, as allowed in this policy, or per resolution agreed, through arbitration, between the Office of the CIO and the external entity.

5.3.3. Appeals

5.3.3.1. Faculty, staff and students may appeal a decision to suspend individual network access by submitting a written request to infosec@usm.edu.

5.3.3.2. The appeal should include all pertinent facts and information related to the incident or event that led to the suspension of service.

5.3.3.3. iTech will, examine all available information regarding the suspension of service and decide to either reinstate network access or continue the suspension.

5.3.3.4. The suspension of Internet access account can only be appealed once.

5.3.3.5. “USM Public” wireless network users may not appeal to reverse the decision to suspend network access.

5.3.3.6. In regards to penalties, other than the suspension of network access, faculty, staff, and students may appeal disciplinary decisions per the University handbook appropriate for that individual.

5.4. Legal and Civil penalties

5.4.1. 17 U.S.C. § 504 specifies that a person infringing on copyright may be obligated to repay up to $30,000 per work in a civil action, or up to $150,000 per work if it is proven that the copyright infringement was willful.

5.4.2. 18 U.S.C. § 2319 makes it a federal crime to infringe copyright when it can be proven that the violation was committed willingly with attempt to profit. An individual convicted of infringing copyright can face up to 10 years of imprisonment, depending on the specifics of the case.

6. Sources for Permissible Digital Music and Video Entertainment

6.1. Sources for digital music and video entertainment can be found in Appendix A.

---

Review

The Chief Information Officer (CIO) is responsible for the review of this policy every four years (or whenever circumstances require immediate review).
Appendix A

ABOUT EXTERNAL LINKS

The University of Southern Mississippi (USM) is not responsible for the content of any off-site pages that are referenced by or that reference the USM web site.

USM is not responsible for any defamatory, offensive, misleading or illegal conduct of other users, links or third parties, and the risk of injury from the foregoing rests entirely with the user.

Links from the USM web site to other sites, or from other sites to the USM web site, do not constitute an endorsement by USM.

It is the responsibility of the user to evaluate the content and usefulness of information obtained from other sites. All information provided by the USM web site is made available to provide immediate access for the convenience of faculty, staff, and students of USM. While USM believes the information is reliable, human or mechanical error remains a possibility. Therefore, USM does not guarantee the accuracy, completeness, timeliness, or correct sequencing of information. USM shall not be responsible for errors or omissions, or for the use of, or results obtained from the use of, the information.

Reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring by USM or its affiliates.

MUSIC SERVICES

Apple iTunes: https://www.apple.com/itunes/
Google Play: https://play.google.com
Spotify: https://www.spotify.com

VIDEO SERVICES

Apple iTunes: https://www.apple.com/itunes/
Google Play: https://play.google.com
Netflix: https://www.netflix.com
HBO: https://www.hbonow.com/
History
Amendments: Month, Day, Year – summary of changes

1. 11/16/06: Added link to Password policy.
2. 04/23/08: Modified policies menu.
3. 07/13/10: Multiple major revisions reflecting compliance with IHL mandate.
4. 07/16/10: Moved list of recommended links from Permitted Activity to its own section.
5. 07/16/10: "DMCA Notice" definition added to Individual Wireless Internet Access Accounts section.
6. 06/29/15:
   a. Alphabetized definitions and made changes regarding network controls.
   b. Removed reference to HEOA under “Reason for Policy/Purpose”
7. 10/23/15:
   a. Added definitions for “Device”, “DMCA”, “FERPA”, “PII”, and “PHI”
   b. Created Appendix A for “Sources for Digital Music and Video Entertainment” section and moved external link disclaimer from “Related Information” to the appendix.
   c. Revised 1.2 about instanced that p2p is strictly forbidden.
   d. Removed examples of Allowed and Prohibited activity.
   e. Revised enforcement to include sanctions against users of hardwired connections
8. 06/07/16: Minor edits for formatting.
Authorization

Title: Peer-to-Peer Policy
Policy number: ACAF-IT-011

RECOMMENDED BY:

[Signature]
Responsible University Administrator

[Signature]
Responsible University Officer

REVIEWED BY:

[Signature]
Director of Compliance and Ethics

[Signature]
Office of General Counsel

APPROVED:

[Signature]
President

7-27-16
Date

7/26/16
Date

7/29/16
Date

29 JUL 2016
Date

8-6-16
Date