Peer to Peer File Sharing and Copyright Infringement Policy

Overview

The abuse of network resources to illegally obtain and distribute media or software, through peer to peer (P2P) networks, or direct download, is a problem for many institutions of higher education. While Regent University 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 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, Regent University must also protect its assets and reputation, as well as comply with federal regulations.

Purpose

This policy is designed to limit the exposure of the University to security risks and liabilities associated with the irresponsible use of university network resources for illegal file sharing activities and bring Regent University into compliance with the HEOA.

Scope

This policy shall apply to all computer workstations, laptops, servers, networked appliances, and any other device utilizing University network resources, even if that device is privately owned by an individual or third party.

This policy applies to all individuals, regardless of affiliation or status with the University, at such time they are using any Regent University network resource.

Policy

Prohibited Activity

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:

- Specified as illegal by any federal or state law, statute, proclamation, order, or decree.
- Copyrighted and not authorized for distribution by the copyright owner.
- 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.

- Any virus or malicious software for the purpose of deployment or implementation with ill-intent.
- Any P2P activity is strictly forbidden in the cases of:
    - Computer labs.
    - Computer workstations and other network devices readily accessible to multiple users
    - Computer workstations and other network devices used in daily operation by areas and departments heavily affected by federally mandated regulatory compliance.
    - Laptops, computer workstations, and any other network capable device provided by Information technology

Users of Regent University's 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.

Examples of Prohibited activity:

- Use of a BitTorrent client to download a popular movie currently running in theaters.
- Downloading a 'cracked' copy of a commercial software title, so that it may be used without the purchase of a valid licenses
- Using any BitTorrent client, Ares Galaxy, or Limewire on a lab workstation.

Permitted Activity

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.

Examples of permitted activity:

- The downloading of music files from a musician's website, where the artist has explicitly given permission to download those files.
- Use of a BitTorrent client, on a personal laptop, to download a freely available operating system.

Rights and Responsibilities

All individual persons or groups utilizing Regent University networks, including but not limited to Regent University 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.

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.

The Information Technology Department and Regent University are required by federal law to report certain illegal activities to specified law enforcement agencies without notice to the user or the appropriate department.

Technology Mitigation

The Information Technology department has implemented network devices to monitor and protect our network if required. These devices attempt to:

- Allow legal P2P traffic.
- Limit all P2P bandwidth to preserve network usage for business and educational use.
- Allow for manual blocking as needed

Suggested links to legal sources for digital media

Regent University encourages users to fully participate in the Internet experience and in the free exercise of individual rights and academic freedoms while at the same time complying with all laws and University policies governing the downloading and sharing of copyrighted material. As alternatives to illegal downloading, there are several legitimate download services available for use. The list of legitimate media services includes the following:

- Amazon
- Apple iTunes
- Hulu
- Pandora
- Netflix

Privacy

Information Collection

- Logs detailing P2P traffic and usage on the Regent University networks will be collected.
- Logs will contain IP addresses involved in data transfer, direction of transfer (if retrievable), metadata (if retrievable), time, protocol used, and amount of data transferred.
- Logged information will be kept on our security devices up to 30 days.
- Information generated from logged activity will be archived indefinitely.

Information Use

- Logs will be subject to periodic review for enforcement of this policy.
- Information collected may be used in aggregate format for reporting purposes.
- Individual usage will not be actively or routinely monitored.
- Logs maybe used to investigate complaints or suspicious traffic patterns.

Information technology will not release any information collected by our devices to any entity external to Regent University unless compelled or obligated by law or court order, subpoena, warrant, or writ.

Enforcement and Penalties

University Community

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 Regent University administrative policies stated in the handbook governing that individual.

Individuals not affiliated with Regent University

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.

Individual Wireless Internet Access Accounts

Any individual, regardless of their affiliation or status with the University, can have their wireless Internet access permanently suspended for egregious or multiple violations of this policy.

A notice of alleged copyright violation that complies with the Digital Millennium Copyright Act, will be referred to as a "DMCA notice". DMCA notices received by Regent University as a result of abuse while utilizing an individual wireless internet access account will be researched, and if possible matched with the individual responsible for the abuse.

Students:

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 along with a reminder of the P2P and Acceptable Use policies.

For the third occurrence of a DMCA notice, or multiple DMCA notices received during a 24 hour period, the student's wireless account will be temporarily suspended and Student Services will be notified.

The fourth occurrence of a DMCA notice will result in the student's wireless account being permanently suspended for the remainder of the semester.

Faculty, Staff and other University employees:

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.

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, along with a reminder of the P2P and Acceptable Use policies.

For the third occurrence of a DMCA notice, or multiple DMCA notices received during a 24 hour period, the employee's account will be temporarily suspended pending discussion between the employee's supervisor and the Information Technology Department

For all Guest, Temporary, and Contractor access:

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

Appeals

Faculty, Staff, and Students may appeal a decision to suspend individual wireless Internet access by submitting a written request to infosec@regent.edu. The appeal should include all pertinent facts and information related to the incident or event that lead to the suspension of service. The IT department will, re-examine all available information regarding the decision to suspend service and come to a decision.

Guest and Temporary users may not appeal to reverse the decision to suspend wireless Internet access.

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

Legal and Civil penalties

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

18 U.S.C. Sec 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.

Definitions

- P2P (peer-to-peer), in the context of this policy, is defined as 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 network, in the context of this policy, is defined as a collection of distributed network-capable devices participating in P2P activity.

- Peer-to-Peer (P2P) application is defined as any application that allows a network-capable device to participate in one or more P2P networks.

- Sharing, in the context of this policy, describes the action and activity of making any data file available to one or more P2P networks.

- Illegal Downloads are defined as any downloaded file that was obtained in violation of law, or is itself against the law to possess, distribute, duplicate, or create.

- Logs are defined as collections of information, typically used to document activity and events.

- Uploading describes network trafficking of data files originating from the Regent University network and destined for an external network.

- Downloading describes network trafficking of data files originating from an external network and destined for one of Regent University's network.