UNAUTHORIZED DISTRIBUTION OF COPYRIGHTED MATERIALS

James Madison University Information Technology – September 2011

INTRODUCTION

The Higher Education Opportunity Act (HEOA) of 2008 placed new requirements on James Madison University and other institutions of higher education to address unauthorized distribution of copyrighted material on their networks. While these provisions do not change existing copyright law, they add new responsibilities not applicable to other network providers/commercial ISPs. This document describes JMU's plan to deal with the following new HEOA copyright compliance concerns:

- Annual disclosure to students describing copyright law and the university's policies and sanctions for dealing with violations;
- A written and implemented plan to effectively combat on-campus copyright abuse; and an
- Offer of Alternatives to Illegal Downloading.

ANNUAL DISCLOSURE

Each fall the Assistant Vice President of Information Technology and the Dean of Libraries and Educational Technologies distribute a joint communication to all students and employees emphasizing that unauthorized distribution of copyrighted material is illegal and exposes violators to civil, criminal penalties (see example in Appendix 1). The communiqué references university policies and penalties for unauthorized distribution of copyrighted material using the institution's IT systems. The university's Appropriate Use of Technology Resources policy (http://www.jmu.edu/JMUpolicy/1207.shtml) and the JMU student handbook (http://www.jmu.edu/judicial/handbook/) both speak directly to computer misuse and infringement of copyright. A resource page containing the annual disclosure notice and other information related to illegal file sharing is available at http://www.jmu.edu/computing/fileshare.shtml.

EFFECTIVELY COMBAT ON-CAMPUS COPYRIGHT ABUSE

JMU has also implemented the following technology-based deterrents to address infringing activity:

1. Bandwidth shaping;
2. Traffic monitoring to identify largest bandwidth users; and,
3. Procedures to accept and respond to DMCA infringement notices and
4. Educational programs to raise student, faculty and staff awareness for copyright responsibilities.

The university's plan for combating illegal file sharing is reviewed and updated annually. Specific procedures used in implementing the plan are available in Appendix 2.

BANDWIDTH SHAPING

Information Technology has enacted bandwidth limitations on certain protocols to ensure that adequate bandwidth will remain available for the business of JMU and its community. We strictly limit the amount of outgoing peer to peer traffic and cap the amount of incoming peer-to-peer traffic as well.

TRAFFIC MONITORING

JMU operates its networks under the assumption that individuals behave responsibly and in accord with the university's Appropriate Use Policy. See the Appropriate Use Policy (AUP) at http://www.jmu.edu/JMUpolicy/1207.shtml. Given this assumption, IT's monitoring program focuses on maintaining the utility of the network, the protection of JMU resources. Individual identities are considered only when they become relevant in dealing with network anomalies and/or inappropriate use.

DEALING WITH INFRINGEMENTS

JMU responds to complaints from industry representatives by notifying the student that a complaint has been received, requesting that immediate action be taken to remove any copyrighted materials illegally possessed or shared, and further reminding the student that continued violation of copyright may lead to serious legal consequences. Egregious or repeat cases are referred to Judicial Affairs for action. And, if law enforcement becomes involved, JMU responds to properly presented requests for information (subpoenas, etc.).

OFFER ALTERNATIVES TO ILLEGAL DOWNLOADING

A resource website is (http://www.jmu.edu/computing/fileshare.shtml) available to provide additional detail and includes reference to a list of legal alternatives to illegal downloading (maintained by Educause in behalf of higher education. See http://www.educause.edu/legalcontent).

OTHER MEANS OF INFORMING THE COMMUNITY

Information Technology discourages illegal use of copyrighted materials through an on-going program of awareness. Information about illegal downloading and the potential dangers of peer-to-peer file sharing is available through:

- News articles such as the one at http://www.jmu.edu/computing/af/
- Technical information included in our RUNSAFE security awareness program http://www.jmu.edu/computing/runsafe/nullify.shtml#music
- Reminder bookmarks distributed through technology and library outlets around campus

The library maintains the following sites, to provide general guidance on use of copyrighted materials:

http://www.jmu.edu/copyright/.

APPENDIX 1 – EXAMPLE OF ANNUAL DISCLOSURE NOTICE

Internet File Sharing and Copyrighted Materials

All students, faculty and staff,

Easy access allows each of us to explore the vastness of the Internet in different ways. On our quest for adventure, individuality, community and information, we find new experiences and ways to entertain and express ourselves. While most of this activity is healthy and encouraged, some behaviors cause problems that can harm us individually and threaten our community.

One example is the widespread use of Internet file sharing. Through peer-to-peer applications such as Gnutella, BitTorrent and eDonkey individuals have previously caused severe congestion of the JMU network, denying effective Internet access for others and causing teaching, learning, research and service functions to all suffer.

Besides adversely affecting network traffic flow, inappropriate use of file sharing programs to exchange copyrighted songs, movies, software and games has resulted in legal risk to individuals in our community and forced the university's increased involvement with handling recording and movie industry complaints served on such persons. Aggressive steps—such as invasive content scans, suspension of Internet access and cooperation with industry representatives in their pursuit of legal remedies—loom as potentially necessary actions. Such measures have already been undertaken at other universities.

In a manner consistent with our tradition of promoting individual responsibility within the university community, JMU has to this point relied most heavily on the individual commitment of students, faculty and staff to behave responsibly. We have expected each member of the JMU community to honor university policies and applicable laws. Yet each year there are some among us who abuse this trust by using the university's information technology resources inappropriately.

Individuals who abuse this trust must realize that when possible violations of copyright law are brought to our attention, JMU administrators have no choice but to make contact and ask for remedy of the problem. Failure to respond to such a request will be handled in a manner consistent with existing JMU policies. Consequences can be serious including suspension or termination from the university. And those who violate copyright law are also subject to civil and criminal penalties which can be quite severe.

Please avoid such a situation by informing yourself about JMU policies, educating others and demonstrating responsible behavior that respects the rights of fellow students, faculty and employees as well as the rights of copyright owners.

For additional security details and applicable policies see: www.jmu.edu/computing/fileshare.shtml.

Thank you for your cooperation.

Ralph Alberico
Dean of Libraries & Educational Technologies

Dale Hulvey
Assistant Vice President for Information Technology

APPENDIX 2 – PROCESSES FOR HANDLING INCIDENTS

The following documents outline the processes used for handling copyright and standard notifications used for responding to situations where copyright infringement, excessive bandwidth utilization or illegal file sharing become apparent. These processes vary slightly according for various members of the university community (students, faculty and staff).

- Incident Handling Procedure for Students
- Incident Handling Procedure for Faculty
- Incident Handling Procedure for Staff
- Standard Notification Messages (not available in on-line version)

Process for Handling Copyright Infringement, Excessive Bandwidth, and Illegal File Sharing Incidents Involving Students

Introduction:

JMU is experiencing a significant increase in the use of its network bandwidth and other resources for the collection, storage and sharing of illegally obtained copyrighted works (music, videos, etc.) JMU's IT department has taken steps to curb this activity, but the situation continues to prompt complaints to the university from media industry organizations (e.g. RIAA, MPAA, etc.). These complaints request that the university intervene to stop the illegal file sharing activity of its students/employees. As public opinion and financial impacts continue to draw more industry attention to this behavior, the complaints are becoming more aggressive. Some universities (most recently Boston College and MIT) have received subpoenas to turn over names/contact information for the students/employees associated with the offending file sharing sites. This circumstance places universities in a precarious legal/policy dilemma. A thorough and consistent approach to managing its response to these incidents, is considered a necessary part of demonstrating due diligence.

General Approach:

- If the university is served with a subpoena to turn over names and other information related to such issues, existing procedure will be used to evaluate and respond.
- IT has collected information from other universities in Virginia on their current status/procedures related to these issues. The process outlined below is based on this information and is considered comparable to actions being taken at other institutions.
- IT created a relationship with Student Affairs that allows for handling of students' technology abuse behavior similarly to other abuses that don't involve technology. IT will act as a point of contact, technical resource and/or complainant.
- The generalized process will apply to the majority of situations, but is not intended to address those where the abuse is being conducted for profit (i.e. black market resale of music, videos, etc.) or is otherwise particularly heinous. JMU reserves the right to alter its processes in keeping with the specific circumstances of the situation.

Incident Response Process:

Reports of copyright Infringement, excessive bandwidth utilization and/or illegal file sharing by students shall be handled as follows:

1) **Initial incident notifications** (received from media industry complainants or generated by IT based on its analysis of traffic flows) are funneled to a single point (A member of Technical Services, Systems staff).

2) **Initial Response by IT --** Based on the incident notification, IT will make an entry into a tracking spreadsheet and attempt to match the offending IP address to an owner based

on information in the IP tables maintained by IT. Those inquiries which generate an immediate, legitimate match, will result in an email to the IP owner requesting that within 5 calendar days[i] they: a) remove any illegal files and respond to the notice indicating that they have done so; or, b) to explain why they believe such a response is inappropriate. The notice will also recommend that any server software used for illegal file sharing also be removed from the computer. Any questions regarding this request will be directed back to IT and if assistance is required for the clean-up, a CampusNet RNA will be dispatched to assist. Address inquiries that cannot be validated will be so noted in the spreadsheet and directed to second-level technical staff for follow-up

3) **Initial Reply by Student:**
   a. If the student replies within the 5-day period that s/he has taken the file down, the complaint is closed. Students will be reminded that any further complaints will be turned over to Judicial Affairs.
   b. If the student replies that it is 'Not Me', the information surrounding the compliant will be noted, but no further action will be taken with the student other than to acknowledge that the response was received and considered a 'free pass' but that any future complaint may be referred to Judicial Affairs for follow-up.
   c. If the student fails to reply within the 5-day period, IT will turn off the student's Internet access.. IT will also notify the student that the access has been turned off because of their failure to reply. Status updates/copies of the email exchanges will be maintained by IT using the tracking spreadsheet and a departmental email account.

The actions taken by IT in Steps 1-3 remain largely the same for successive incidents involving the same individual. Exceptions/additional actions are noted below.

4) **2nd Incident:** If in performing the IP look-up IT finds that this is the second time the individual has been associated with such an incident, in addition to emailing the student, IT will refer the complaint along with associated backup information to Judicial Affairs. Upon receipt Judicial Affairs generates a letter to the student stating that a second complaint has been received and that it is being considered as a judicial offense. The letter will also include the contact for follow-up. At this point, further communications are between the individual and Judicial Affairs (JA). IT takes on the role of information provider to Judicial Affairs as they determine an appropriate resolution to the incident.

   If Judicial Affairs determines that the complaints against the student are legitimate, they will determine and apply sanctions as appropriate. Judicial Affairs will supply the student with written notification of the sanction.

   Sanction: The suggested sanction is required attendance at an Ethics class that includes this topic.

5) **3rd Incident and Successive Incidents:** If a student is involved in three or more incidents, IT and Judicial Affairs responses are the same except that more severe sanctions are applied. IT will assist Judicial Affairs as an advisor/information provider and by implementing technical controls necessary to implement sanctions once they are determined.

Sanction:

An appropriate sanction is determined by Judicial Affairs commensurate with the behavior. The suggested minimum includes loss of internet connectivity in their residence for a period of at least 30 semester days[ii]. Additional penalties, including fines, or loss of other computing privileges, may also be assessed

[i] Breaks and holidays recognized as part of the official university calendar will be taken into account in calculating the "five calendar day" time period for reply. The clock for the five-day period begins with the date and time stamped on the original e-mail notification and can include weekends.

[ii] Semester days are any class days and weekends within the course of a regular Fall or Spring term.

Process for Handling Copyright Infringement, Excessive Bandwidth Utilization and Illegal File Sharing Incidents Involving Faculty

Introduction:

JMU is experiencing a significant increase in the use of its network bandwidth and other resources for the collection, storage and sharing of illegally obtained copyrighted works (music, videos, etc.) JMU's IT department has taken steps to curb this activity, but the situation continues to prompt complaints to the university from media industry organizations (e.g. RIAA, MPAA, etc.). These complaints request that the university intervene to stop the illegal file sharing activity of its students/employees. As public opinion and financial impacts continue to draw more industry attention to this behavior, the complaints are becoming more aggressive. Some universities (most recently Boston College and MIT) have received subpoenas to turn over names/contact information for the students/employees associated with the offending file sharing sites. This circumstance places universities in a precarious legal/policy dilemma. A thorough and consistent approach to managing its response to these incidents, is considered a necessary part of demonstrating due diligence.

General Approach:

- If the university is served with a subpoena to turn over names and other information related to such issues, existing procedure will be used to evaluate and respond.
- IT has collected information from other universities in Virginia on their current status/procedures related to these issues. The process outlined below is based on this information and is considered comparable to actions being taken at other institutions.
- IT created a relationship with Student Affairs that allows for handling of student technology abuse behavior similarly to other abuses that don't involve technology. The process below was developed through a similar relationship with Human Resources and Academic Affairs for incidents involving faculty. IT will act as a point of contact, technical resource and/or complainant.
- The generalized process will apply to the majority of situations, but is not intended to address those where the abuse is being conducted for profit (i.e. black market resale of music, videos, etc.) or is otherwise particularly heinous. JMU reserves the right to alter its processes in keeping with the specific circumstances of the situation.

Incident Response Process:

Situations involving copyright infringement, excessive bandwidth utilization and illegal file sharing Incidents Involving Faculty

1) **Initial incident notifications** (received from media industry complainants or generated by IT based on its analysis of traffic flows) are funneled to a single point (Technical Services, Systems staff).

2) **Initial Response by IT --** Based on the incident notification, IT will make an entry into a tracking spreadsheet and attempt to match the offending IP address to an owner based on information in the IP tables maintained by IT. Those inquiries which generate an immediate, legitimate match, will result in an email to the IP owner requesting that within 5 calendar days[iii] they: a) remove any illegal files and respond to the notice indicating that they have done so; or, b) to explain why they believe such a response is inappropriate. The notice will also recommend that any server software used for illegal file sharing be removed from the computer. A copy of the request is also sent to the appropriate director/ department head for informational purposes. Any questions regarding this request will be directed to IT and if assistance is required for the clean-up, a Computing Support staff member will be dispatched through the HelpDesk to assist. Address inquiries that cannot be validated will be so noted in the spreadsheet and directed to second-level technical staff for follow-up.

3) **Initial Reply by faculty member:**
   a. <u>If the faculty replies within the 5-day period that s/he has taken the file down</u>, the complaint is closed. The faculty member will be reminded that any further complaints will be referred for further review by his/her director/department head and Human Resources.
   b. <u>If the faculty replies that it is 'Not Me',</u> the information surrounding the compliant will be noted, but no further action will be taken with the faculty member other than to acknowledge that the response was received and considered a 'free pass' but that any future complaint may be referred for review to his/her director/department head and Human Resources for follow-up.
   c. <u>If the faculty fails to reply within the 5-day period</u>, IT will turn off the Internet access to the faculty's machine. IT will also notify the faculty member and his/her director/department head that the access has been turned off <u>because of the failure to reply</u>. Status updates/copies of the email exchanges will be maintained by IT using the tracking spreadsheet and a departmental email account.

The actions taken by IT in Steps 1-3 remain largely the same for successive incidents involving the same individual. Exceptions/additional actions are noted below.

4) **2nd incident:** If in performing the IP look-up IT finds that this is the second time the individual has been associated with such an incident, IT refers the complaint along with associated backup information to the appropriate director/department head and Human Resources. At this point, further communications are between the individual, his director/department head and Human Resources (HR). Upon receipt of such a referral the director/department head will review the complaints in detail.

If the complaints against the individual warrant action, the director/department head will work with Human Resources to determine and apply appropriate sanctions.

5) **Any Successive Incident:** Following the same process, any additional incidents associated with an individual will be further evaluated and resolved on a case-by-case basis. Human Resources will work with the director/department head to determine and levy appropriate sanctions beyond those already used. IT will assist their efforts by advising/providing information and by establishing technical controls necessary to implement sanctions once they are determined.

[iii] Breaks and holidays recognized as part of the official university calendar will be taken into account in calculating the "five calendar day" time period for reply. The clock for the five-day period begins with the date and time stamped on the original e-mail notification and can include weekends.

Process for Handling Copyright Infringement, Excessive Bandwidth Utilization and Illegal File Sharing Incidents Involving Classified Employees

Introduction:

JMU is experiencing a significant increase in the use of its network bandwidth and other resources for the collection, storage and sharing of illegally obtained copyrighted works (music, videos, etc.) JMU's IT department has taken steps to curb this activity, but the situation continues to prompt complaints to the university from media industry organizations (e.g. RIAA, MPAA, etc.). These complaints request that the university intervene to stop such illegal filesharing activity of its students/employees. As public opinion and financial impacts continue to draw more industry attention to this behavior, the complaints are becoming more aggressive. Some universities (most recently Boston College and MIT) have received subpoenas to turn over names/contact information for the students/employees associated with the offending filesharing sites. This circumstance places universities in a precarious legal/policy dilemma. A thorough and consistent approach to managing its response to these incidents, is considered a necessary part of demonstrating due diligence.

General Approach:

- If the university is served with a subpoena to turn over names and other information related to such issues, existing procedure will be used to evaluate and respond.
- IT has collected information from other universities in Virginia on their current status/procedures related to these issues. The process outlined below is based on this information and is considered comparable to actions being taken at other institutions.
- IT created a relationship with Student Affairs that allows for handling of students' technology abuse behavior similarly to other abuses that don't involve technology. The process below was developed through a similar relationship with Human Resources for incidents involving employees. IT will act as a point of contact, technical resource and/or complainant.
- The generalized process being developed will apply to the majority of situations, but is not intended to address those where the abuse is being conducted for profit (i.e. black market resale of music, videos, etc.) or is otherwise particularly heinous. JMU reserves the right to alter its processes in keeping with the specific circumstances of the situation.

Incident Response Process:

Reports of copyright infringement, excessive bandwidth utilization and illegal file sharing by classified employees will be handled as follows:

1) **Initial incident notifications** (received from media industry complainants or generated by IT based on its analysis of traffic flows) are funneled to a single point (Technical Services, Systems staff).

2) **Initial Response by IT --** Based on the incident notification, IT will make an entry into a tracking spreadsheet and attempt to match the offending IP address to an owner based on information in the IP tables maintained by IT. Those inquiries which generate an immediate, legitimate match, will result in an email to the IP owner requesting that within 5 calendar days[iv] they: a) remove any illegal files and respond to the notice indicating that they have done so; or, b) to explain why they believe such a response is inappropriate. The notice will also recommend that any server software used for illegal filesharing also be removed from the computer. A copy of the request is also sent to the employee's supervisor for informational purposes. Any questions regarding this request will be directed to IT and if assistance is required for the clean-up, a Computing Support staff member will be dispatched through the HelpDesk to assist. Address inquiries that cannot be validated will be so noted in the spreadsheet and directed to second-level technical staff for follow-up.

3) **Initial Reply by Classified Employee:**
   a. <u>If the employee replies within the 5-day period that s/he has taken the file down</u>, the complaint is closed. Employees will be reminded that any further complaints will be referred to Human Resources.
   b. <u>If the employee replies that it is 'Not Me',</u> the information surrounding the compliant will be noted, but no further action will be taken with the employee other than to acknowledge that the response was received and considered a 'free pass' but that any future complaint may be referred to Human Resources for follow-up.
   c. <u>If the employee fails to reply within the 5-day period</u>, IT will turn off the Internet access to the employee's machine.. IT will also notify the employee and his supervisor that the access has been turned off <u>because of the failure to reply</u>. Status updates/copies of the email exchanges will be maintained by IT using the tracking spreadsheet and a departmental email account.
   d.

The actions taken by IT in Steps 1-3 remain largely the same for successive incidents involving the same individual. Exceptions/additional actions are noted below.

4) **2nd Incident:** If in performing the IP look-up IT finds that this is the second time the individual has been associated with such an incident, IT refers the complaint along with associated backup information to Human Resources. Upon receipt Human Resources generates a letter to the employee and his supervisor stating that a second complaint has been received and that it has been referred for potential action by Human Resources. The letter will also include the contact for follow-up. At this point, further communications are between the individual, his supervisor and Human Resources (HR).

If the complaints against the employee warrant action, Human Resources will work with the supervisor to determine and apply appropriate sanctions.

5) **Any Successive Incident:** Following the same process, any additional incidents associated with an individual will be further evaluated and resolved on a case-by-case basis. Human Resources will work with the supervisor to determine and levy appropriate sanctions beyond those already used. IT will assist Human Resources as an advisor/information provider and by establishing technical controls necessary to implement sanctions once they are determined.

[iv] Breaks and holidays recognized as part of the official university calendar will be taken into account in calculating the "five calendar day" time period for reply. The clock for the five-day period begins with the date and time stamped on the original e-mail notification and can include weekends.