Higher Education Opportunity Act (HEOA) Compliance Program

Unauthorized Distribution of Copyrighted Materials

James Madison University Information Technology – September 2021

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 added new responsibilities not applicable to other network providers/ commercial ISPs. This document describes JMU's plan to address HEOA copyright compliance concerns:

- Annual disclosure to students describing copyright law and the university's policies and sanctions for dealing with violations;
- Implementation of a written 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 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 (https://www.jmu.edu/osarp/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 bandwidth limitations on certain protocols to ensure adequate bandwidth availability for the business of JMU and its community. We strictly limit the amount of outgoing peer-to-peer traffic and also cap the amount of incoming peer-to-peer traffic.

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, Information Technology'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 Office of Student Accountability and Restorative Practices 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 on behalf of higher education. See http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/educause-policy/issues-and-positions/intellectual-property/legal-sources-onli).

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, information and alerts on the IT website http://www.jmu.edu/computing/
- RunSafe resource page outlining secure computing practices available at http://www.jmu.edu/computing/runsafe/nullify.shtml#music

JMU Libraries also maintains a site at http://www.jmu.edu/copyright/offering general guidance on use of copyrighted materials.

Processes for Handling Incidents

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

Appendix 1: Annual Disclosure Notice

Appendix 2: Incident Handling Procedure for Students

Appendix 3: Incident Handling Procedure for Faculty

Appendix 4: Incident Handling Procedure for Staff

Appendix 1:

Annual Disclosure Notice (example 09/2021)

Internet File Sharing and Copyright

Dear students, faculty, staff, and JMU affiliates,

Movies, music, games, software and other copyrighted materials are all just a click away on the Internet. Most of us at JMU engage with such content in productive and ethical ways.

This is an annual reminder that—without explicit permission of the owner—your possession or distribution of copyrighted material may be a violation of federal copyright law. Violations commonly occur through naïve or ill-advised use of Internet file sharing. Use of peer-to-peer (P2P) applications such as BitTorrent, Kazaa, Gnutella, etc. can easily lead to illegal file sharing situations and have previously caused unwarranted congestion of the JMU network, denied access for others, and impacted the educational, research, and service efforts of the university.

Inappropriate use of file sharing programs to exchange copyrighted songs, movies, software and games presents legal risk to you as an individual and forces the university toward increased involvement in handling complaints served by media organizations and the artists they represent. Use of aggressive steps, such as invasive content scans, suspension of Internet access, and cooperation with industry representatives as they pursue legal remedies are not the preferred JMU Way, but federal requirements on us as an institution could make them necessary as a response to illegal file sharing.

Advocating instead for individual responsibility within our university community, JMU relies heavily on the ethical commitment of our students, faculty and staff. Each member of the JMU community is advised of their obligation to behave responsibly and honor university policies and applicable laws. When possible violations of copyright law are brought to our attention, JMU Information Technology and its network delivery partners have no choice but to make contact and seek remedy of the situation. Failure to respond will be handled in a manner consistent with existing JMU policies. Consequences can be serious, including suspension or termination from the university. Additionally, those who violate copyright law may be subject to severe civil and/or criminal penalties.

To avoid such a situation, please respect the rights of copyright owners and other members of the JMU community by informing yourself about JMU policies, educating others, and demonstrating responsible behavior. To help you learn more about copyright and Fair Use, the JMU Libraries have provided an extensive Guide: guides.lib.jmu.edu/copyright. Please also see the JMU Libraries Guide to Free Media for Creative Use: guides.lib.jmu.edu/freemedia. Finally, review www.jmu.edu/computing/fileshare.shtml for additional security and copyright information and further details on JMU processes for dealing with violators.

Thank you for your cooperation.

Robin Bryan, AVP, Information Technology

Dr. Bethany Nowviskie, Dean of Libraries

Appendix 2:

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

Introduction:

JMU continues to experience increased use of network bandwidth and other resources for the collection, storage and sharing of illegally obtained copyrighted works (music, videos, etc.) JMU's IT department and Apogee (JMU's student connectivity partner) have 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. Many universities 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 or its partner are 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 and elsewhere regarding best practices regarding 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 Apogee and JMU Student Affairs' Office of Student Accountability and Restorative Practices (OSARP) 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.

General Incident Response Process:

Reports of copyright Infringement, excessive bandwidth utilization and/or illegal file sharing by students in non-residential portions of the JMU network 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 (Information Technology Security).
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[1] 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

[1] 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.

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. Address inquiries that cannot be validated will be so noted in the spreadsheet and directed to second-level technical staff for follow-up as necessary.

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 the Office of Student Accountability and Restorative Practices (OSARP).

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 OSARP 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 OSARP. Upon receipt OSARP generates a letter to the student stating that a second complaint has been received and that it is being considered as a student conduct offense. The letter will also include the contact for follow-up. At this point, further communications are between the individual and OSARP. IT takes on the role of information provider to OSARP as they determine an appropriate resolution to the incident.

   If OSARP determines that the complaints against the student are legitimate, they will determine and apply sanctions as appropriate. OSARP 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 OSARP responses are the same except that more severe sanctions are applied. IT will assist OSARP 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 OSARP commensurate with the behavior. The suggested minimum includes loss of internet connectivity in their residence for a period of at least 30 semester days[2]. Additional penalties, including fines, or loss of other computing privileges, may also be assessed.

The process above describes the process used to handle incidents on the JMU network. However, since JMU partners with Apogee (http://apogee.us) to provide network and streaming services to residence halls. Below is the process Apogee uses to handle incidents on the residential network.

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

Incident Response for Residential Network

JMU provides residential network service through partnership with Apogee. Similar reports of copyright Infringement, excessive bandwidth utilization and/or illegal file sharing by JMU students where the related network services are provided/ managed through Apogee, the following procedure will apply:

1) ISP of Record

As the ISP of record for JMU's residential network, Apogee receives email notifications of alleged copyright infringement cases from various companies such as RIAA, MediaSentry, HBO, Paramount, Universal Studios, etc. It is our responsibility to pass these notices along to the end users.

2) Notification Matching

- End users are matched against the IP address, date and timestamp provided in the notification. An email is then sent to the email address(es) provided on the end user's account; this email includes the actual notification as well.
- The first offense is a warning, the second is a warning and the 3rd is a 7-day suspension from the network.
- If end users have an additional violation after 3rd notice, the suspension time defaults to the highest offense, which is a 7 day suspension from the ResNet network.

Process:

The process outlined below is Apogee's method for handling compliance in processing DMCA notifications. This compliance process will apply to end users using JMU's residential network and is incorporated in whole as part of JMU's HEOA Compliance plan.

- 1st Offense
  - Forward DMCA notice to the end user and request that, if he/she is sharing copyrighted information, to cease and remove the specified files
  - Warning only
  - Account remains active
- 2nd Offense
  - Forward DMCA notice on to the end user and request that, if he/she is sharing copyrighted information, to cease and remove the specified files
  - Second warning
  - Account remains active
- 3rd Offense
  - Forward DMCA notice on to the end user and request that, if he/she is sharing copyrighted information, to cease and remove the specified files
  - Account shut off for seven (7) days
  - Office of Student Accountability and Restorative Practices will be copied and will contact the student regarding potential charges related to student conduct/appropriate use violation.

On the following pages are samples of the notification emails you can expect to receive from Apogee.

1st Offense

Dear (name of student):

Apogee has recently received a complaint from a copyright holder (included below), alleging that you are distributing protected works. We are required by the Digital Millennium Copyright Act to take these complaints very seriously. If, in fact, you are engaging in the downloading, uploading, or other unauthorized distribution of copyrighted materials you may also be at risk for being sued by the copyright holder or a representative of the copyright holder, pursuant to the DMCA. In addition, downloading or sharing of copyrighted materials without authorization is a violation of University Policy J5-100 Computer Misuse and can result in a referral to the Office of Student Accountability and Restorative Practices and possible university sanctions.

Since this is your first notice of an offense, Apogee is required to notify you of this alleged violation and request that you remove the materials from your computer, and cease and desist trading or sharing of their material. You may notify Apogee by replying to this email stating what actions have been taken or if you dispute this allegation. Apogee will then anonymously forward your response to the copyright holder.

If you do not submit a response and/or another alleged violation occurs involving the same account, you may be subject to more serious penalties, including the long-term termination of your ResNet/Internet account with no refund.

Please use your online services responsibly. Remember, copyright infringement is illegal and can have very significant legal ramifications. A copy of this email may also be sent to Office of Student Accountability and Restorative Practices.

Thank you for your attention to the urgent matter. For questions, please call 855-410-7377.

Respectfully,

Apogee Customer Service

Received 1st DMCA Notice - [1st notice count] Forwarded email to customer. No consequences - this notice is just a warning. Copyright holder referenced date/time as DateTime:

CC: abuse@jmu.edu

Suspended: No, Warning only

2nd Offense

Dear (name of student):

Apogee has recently received a complaint from a copyright holder (included below), alleging that you are distributing protected works. We are required by the Digital Millennium Copyright Act to take these complaints very seriously. If, in fact, you are engaging in the downloading, uploading, or other unauthorized distribution of copyrighted materials you may also be at risk for being sued by the copyright holder or a representative of the copyright holder, pursuant to the DMCA. In addition, downloading of copyrighted materials without authorization is a violation of University Policy J5-100 Computer Misuse and can result in a referral to the Office of Student Accountability and Restorative Practices and possible university sanctions.

This is your second notice of an offense, Apogee is required to notify you of this alleged violation and request that you remove the materials from your computer, and cease and desist trading or sharing of their material. You may notify Apogee by replying to this email stating what actions have been taken or if you dispute this allegation. Apogee will then anonymously forward your response to the copyright holder.

If you do not submit a response and/or another alleged violation occurs involving the same account, you may be subject to more serious penalties, including the long-term termination of your ResNet/Internet account with no refund.

Please use your online services responsibly. Remember, copyright infringement is illegal and can have very significant legal ramifications. A copy of this email may also be sent to Office of Student Accountability and Restorative Practices.

Thank you for your attention to the urgent matter. For questions, please call 855-410-7377.

Respectfully,

Apogee Customer Service

CC: abuse@jmu.edu

Received 2nd DMCA Notice - [2nd notice count] Forwarded email to customer. This notice is just a warning; next offense will have Internet suspension for 7 days. Copyright holder referenced date/time as DateTime:

Suspended: No, Second Warning

3rd Offense

Dear (name of student):

Apogee has recently received a complaint from a copyright holder (included below), alleging that you are distributing protected works. We are required by the Digital Millennium Copyright Act to take these complaints very seriously. If, in fact, you are engaging in the downloading, uploading, or other unauthorized distribution of copyrighted materials you may also be at risk for being sued by the copyright holder or a representative of the copyright holder, pursuant to the DMCA. In addition, downloading of copyrighted materials without authorization is a violation of University Policy J5-100 Computer Misuse and can result in a referral to the Office of Student Accountability and Restorative Practices and possible university sanctions.

As this is your third [or higher] notice of an offense, your ResNet/Internet services will be shut off for seven (7) days and a copy of this letter has been sent to the Office of Student Accountability and Restorative Practices which may be contacting you regarding potential charge(s) of a university policy violation. Please monitor your JMU email account for a charge notification. If another alleged violation occurs involving the same account, you may be subject to more serious penalties, including the long-term termination of your ResNet/Internet account with no refund.

If you do not submit a response and/or another alleged violation occurs involving the same account, you may be subject to more serious penalties, including the long-term termination of your ResNet/Internet account with no refund.

Please use your online services responsibly. Remember, copyright infringement is illegal and can have very significant legal ramifications.

Thank you for your attention to the urgent matter. For questions, please call 855-410-7377.

Respectfully,

Apogee Customer Service

CC: abuse@jmu.edu

Received 3rd DMCA Notice - [3rd notice count] Forwarded email to customer. INTERNET WILL BE SUSPENDED FOR 7 DAYS. The student will be charged and contacted by the Office of Student Accountability and Restorative Practices. Customer will need to wait until suspension is over to access Internet. Account may be reactivated 7 days AFTER the date of suspension (see logs above for date that account was place on hold). Copyright holder referenced date/time as DateTime:

Suspended: Yes- 7 Days

Appendix 3:

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 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 and elsewhere regarding best practices 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:

Reports of copyright infringement, excessive bandwidth utilization and illegal file sharing by faculty 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 (Information Technology Security).
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[3] they: a) remove any illegal files and respond

[3] 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.

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 IT Help Desk 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. If the faculty replies within the 5-day period that s/he has taken the file down, 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. If the faculty replies that it is 'Not Me', 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. If the faculty fails to reply within the 5-day period, 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 because of the 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, 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.

Appendix 4:

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 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 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 and elsewhere regarding best practices 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 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 (Information Technology Security).
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[4] 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. 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 IT Help Desk 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. If the employee replies within the 5-day period that s/he has taken the file down, the complaint is closed. Employees will be reminded that any further complaints will be referred to Human Resources.

   b. If the employee replies that it is 'Not Me', 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. If the employee fails to reply within the 5-day period, 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 because of the 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, 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.

1) **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.

[4] 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.