Approved: 7/22/05

Procedures For Responding To Notifications of Copyright Violation or Requests For The Content Of Electronic Communication, Any Information About Users Of the University of Massachusetts Systems/Networks, or Traffic On The University of Massachusetts Network

Introduction

Several laws allow for the disclosure of electronic information (e.g., USA Patriot Act, Electronic Communications Privacy Act – ECPA, Digital Millennium Copyright Act - DMCA) while others restrict the disclosure of certain types of information (e.g., FERPA non-directory student records). The disclosure of electronic information is based on a certain set of legal procedures, documents and protocols. In order for the University to fulfill both its legal responsibilities under the law and its obligations to protect the privacy of its students and employees, consistent procedures must be followed when responding to requests for electronic information.

General Procedures

University/Campus Chief Information Officers shall assign Designated University Officials on each campus to process/respond to requests concerning electronic communications or databases.

Employees will not discuss requests for information regardless of type (e.g., warrant, subpoena, take down request, etc.) with anyone except as instructed in the following procedures.

Employees contacted by law enforcement to answer general questions about University systems or the types of services provided to users to enable them to write a meaningful subpoena, warrant, etc. should refer such questions to University legal council.

Employees contacted by or working with law enforcement should try to make a copy of any search warrant served, and should retain copies of all confidential logging/audit trails and other information shared with law enforcement. Employees should also document all activities (e.g., what is requested, how the University responded, the person the information was given to and when, etc.) related to the served search warrant.

Campus Designated University Officials may institute other sanctions or judicial processes available within the University system in addition to any legally required procedures/processes.

Responding to Legal Papers – Procedures

- **Disclosures with Authorization from Law Enforcement**

Any University employee asked by individuals representing themselves as law enforcement agents to provide the content of electronic communication or any information about users of or traffic on the University of Massachusetts network **with or without any form of written authorization** (Legitimate requests for information take a variety of forms, including subpoenas, warrants, administrative orders, and court orders) should **not** disclose any information. Additionally, the existence of the request should **not** be disclosed to anyone other than those names below, including the student, alumnus or employee who is the subject of the request.

All requests for such information, regardless of whether the individual about whom the request is being made is a student, an alumnus, or an employee, should be forwarded to University legal counsel and the Designated University Official at the applicable campus.

Presentation of a Search Warrant

If the law enforcement official presents a search warrant the agent or officer may begin a search as soon as the order is served. The University staff or faculty ember on whom the order is served should ask if they can contact the appropriate administrator before the search begins. The University staff or faculty member should immediately contact University legal counsel and the Designated University Official at the applicable campus to inform them that a court ordered search has been requested or initiated. University faculty and staff should cooperate with, not hamper, the search when a search order is served.

If neither University legal counsel or the Designated University Official can be reached and an employee is confronted with an immediate demand to search, the employee should check the identification/credentials of the person(s) demanding data, review the served documentation to see whether anything appears suspicious or obviously invalid, make a copy of the search warrant if possible, preserve copies of data and system integrity as much as possible, comply with the demand **as written** and immediately document what happened. The employee should continue to attempt to contact University legal counsel and the Designated University Official while the search is taking place. Once contacted, the employee should give University legal counsel or the Designated University Official copies of the documentation noted above.

Presentation of a Subpoena Unlike search warrants, subpoenas do not require an immediate response. If the law enforcement official presents a subpoena, contacted University staff or faculty member should immediately contact University legal counsel and the Designated University Official at the applicable campus. If law enforcement requests the contacted employee to so they should preserve the applicable data pending the University response to the subpoena. If imminent loss of data is possible or a threat, the employee should take steps to freeze or copy the data until a decision can be made to review or disclose the applicable data. University legal counsel and the Designated University Official

will determine and review the information that should be produced in response to the subpoena. Only requested information will be released.

Below is a summary of the types of legal documents needed to compel the disclosure of electronic information to law enforcement:

Electronic Information Type/Issue	**Required Legal Document**
Content-Unread E-Mail (Less Than Or Equal To 180 Days)	Search Warrant (May Be Nation-Wide Under USA Patriot Act)
Stored Content/Files And Read E-Mail	Subpoena (ECPA Does Not Apply)
Transactional Records (I.E., Sites Visited, Etc.)	Court Order
Information Including "Subscriber/Customer" (May Refer To Students, Staff, Faculty, Alumni) Name, Address, Length And Types Of Service, IP Address, Remote IP Address From Which They Connects, Records Of Session Times And Durations, Any Temporarily Assigned Network Address, Local And Long-Distance Telephone Connection Records, Telephone Or Instrument Number Or Other "Subscriber/Customer" Number Or Identity	Subpoena
Disclosure Of Any Tangible Things ("Any Tangible Things" Include Books, Record, Papers, Documents, And Other Items) For An Authorized Investigation To Protect Against Terrorism Or Clandestine Intelligence Activities.	Court Order
Disclosure, **Without Student Consent**, Of Education Records Law Enforcement Officials Consider Relevant To A Terrorism Investigation	Court Order

Disclosure For Foreign Student Name And Address; Visa Classification And Issuance Or Extension Date; Full-Time Enrollment Status; And Disciplinary Action Resulting From Criminal Conviction	Under U.S. Citizenship and Immigration Services (i.e., USCIS), foreign students "consent" to release of all this info when they come here. The University also has to report this information regularly under SEVIS. The University is also required to provide this info to a USCIS officer if one shows up and no legal paperwork is needed.
Disclosure Of Voice Mail	Warrant
Required Disclosure Of Communications Or Records	Warrants, Subpoenas, And Court Orders
Business Records	Subpoenas
Wiretap Of Computer Or Telephone / Use Pen Registers And Trap-And-Trace Devices To Obtain Dialing, Routing, Addressing, Or Communication Information If Such Information Does Not Include Communication Content	Wiretap Order (Can Be Nation-Wide Under USA Patriot Act)
Order To Take Down Or Block Access To The Material On Network.	Notification From Copyright Representative That Complies With DMCA Requirements

• Emergency Disclosures

Should any University employee, in the course of business, reasonably believe that they have accessed information about an emergency involving immediate danger of death or serious physical injury, they should contact Public Safety/University Police immediately. After contacting Public Safety/University Police, they should report that contact and underlying information immediately to the Designated University Official at the applicable campus. Public Safety/University Police shall respond to the immediate emergency situation and then subsequently follow up with the appropriate Designated University Official.

• Authorization for Law Enforcement Investigation of Computer Trespass

Any member of the University community who reasonably believes that their

department's computer system has been compromised by a computer trespasser and who would like law enforcement to investigate the matter shall first report the matter to the Designated University Official at their campus and the Campus Public Safety/Police. Public Safety/Police, in conjunction with information technology, shall investigate the matter and consult with appropriate University management and the legal counsel prior to contacting law enforcement.

- **Notification of Copyright Violations Under The Digital Millennium Copyright Act (DMCA)**

  Any University employee asked to respond to bona fide notice of copyright violation by copyright holders shall forward the notice to the appropriate campus Digital Millennium Copyright Agent (e.g., Agent). A bona fide notice of copyright violation is one that follows DMCA requires and should include:

  - A physical or digital signature of the owner of an exclusive copyright right (i.e., the copyright owner himself or the owner's exclusive licensee of the right(s) to reproduce, distribute, display, perform or create derivatives) or the owner's authorized agent;
  - Specific identification of work that is allegedly being infringed,
  - A statement that the notifier believes in good faith that the use of the material is not authorized by the owner, the owner's agent or the law;
  - A statement that the information in the notice is accurate and, under penalty of perjury, that the notifier is authorized to act on behalf of the owner of one or more exclusive copyright rights;
  - The IP address, IP port, network and protocol used in the alleged violation;
  - The date(s) and times(s), including time zone, of the alleged copyright violations;
  - The alleged account or username offering this infringing material;
  - The name and size of the file being offered; and
  - The number of repeat violations recorded at this specific location.

  If the notice of copyright does not comply with DMCA requirements, the Agent should contact University counsel who will determine if the notice of copyright

should be sent back to the notifier informing them of the noncompliant nature of their notices.

If the notice of copyright complies with DMCA requirements, the Agent, in conjunction with University legal counsel, will determine if the University will use the Digital Millennium Copyright Act (DMCA) process for handling the specific allegations of copyright violations within the University's domain. This will be decided by determining if the University is acting as a content-neutral Internet service provider (ISP) and not as a content provider.

Even if the University is eligible to use the DMCA-defined processes**,** which are entirely voluntary for both copyright owners and ISPs, there may be times when it will not use them*,* especially when alternatives will more quickly resolve the matter to the satisfaction of all parties. If the University chooses the DMCA-defined processes, the Agent will request that the appropriate network administrator block the Internet Protocol (IP) address alleged by the notice to be in violation of federal law and provide the agent with the identity of the user or party responsible for the computer (responsible party). The Agent will then notify the user or responsible party of the notice and request a cease and desist statement by return e-mail. Upon receipt of that statement, the Agent will then request that the appropriate network administrator unblock the IP address.

In the case where the copyright notice is the result of a computer compromise (electronic activities that cause damage to a computer), or a "hacking," and not the intentional activity of file sharing on the part of the computer's user, the Agent shall instruct the user to fix the computer or to make an appointment with the appropriate Campus help desk to have it fixed. The Agent will request the block be lifted upon receipt of information that the machine has been repaired.

Counter Notice of Copyright Violations Under DMCA

After the page owner voluntarily takes down the page or the Agent arranges to disable access to it, the Agent may receive a substantially conforming counter-notification from the page owner.

Counter-notices can only claim two things: (i) that the copyright owner is mistaken and that the work is lawfully posted or (ii) that the work has been misidentified. A page owner may assert that a use of another's work qualifies as a fair use and so the copyright owner is "mistaken" in characterizing it as infringing.

DMCA requires that counter-notices from page owners contain the following:

- A physical or digital signature of the page owner;
- A description of the material removed and its location before it was removed;

- A statement that the page owner believes in good faith that the material was removed by mistake or because it was misidentified**;**

- The page owner's name, address and phone number and their consent to jurisdiction of the Federal District Court for that address or any Federal District Court if the address is foreign; and

- A statement that the page owner will accept service of process from the notifier.

Under the DMCA, the University will not be liable to the owner of the page for any harm he or she might suffer because of its actions in disabling access to a page so long as it:

- Takes reasonable steps to notify the page owner about the allegations in a notice that it has received;

- Promptly sends a copy of any substantially conforming counter-notice to the notifier indicating that it will restore access in 10 business days; and

- Restores access to the allegedly infringing work within 10 to 14 business days after the day it receives the counter-notice, ***unless*** it first receives a notice from the complainer that he or she has filed an action seeking a court order to restrain the page owner. If the University receives notice that the notifier has filed an action seeking a court order to restrain the page owner, the University will not repost the allegedly infringing work. It will forward the notice to the page owner and to University legal counsel for response as appropriate.

• Providing personally identifiable information to business partners, vendors, outside agencies and individuals.

The University has business relationships with various outside companies and business partners. These relationships may require that these outside entities obtain information about University community members or that the university provides data files containing that information. Information may not be provided to outside entities or individuals unless a verified business relationship exists. In most cases, University ID numbers (e.g., student or employee id) or social security numbers (e.g., SSN) should not be provided to external entities. If data files must be interfaced, consult with information technology staff about alternative record identifiers. Only provide the vendor with the information they

require for the business relationship or transaction. Work with University information technology staff to develop any data extracts or reports to ensure that they comply with specifications. University employees should review any information or report before submission to any external agency to ensure that only necessary information is included and that there are no SSNs or credit card numbers included in the file or report.