Approved: May 26, 2007

University of Massachusetts
Procedures for the Preservation of and Response to Demands for Electronically Stored Information

General

In order to comply with legal obligation the University must be able to identify the location and format of ESI, and have clear records retention and disposition standards (i.e., University Records Management, Retention and Disposition Standards) that are consistently followed and executed. If a legal claim has been filed or is reasonably anticipated, the University may be required to preserve past and future information in its original electronic form that might become relevant to the claim.

When dealing with the preservation of electronic information, the form of the data and the type of electronic device on which the data is stored must be considered.

Data can exist in several forms:

- **Active Data -** e-mail and electronic files that a person or business can access at present. It includes, but is not limited to, data on laptops, personal computers, networks, e-mail or web servers, personal digital assistants (i.e., PDA's), USB drives and smart phones.
- **Metadata -** metadata are the hidden attributes and characteristics for each file (e.g., name of the file; dates of creation, alteration, deletion; who accessed the data; from where data was accessed; e-mail header; BCC recipients, etc.). There can be hundreds of different metadata for each file.
- **Replicant Data -** computer systems automatically make these files, often without the user's knowledge and direction. Replicant data includes auto-backup files generated by operating systems, word processing applications, as well as system/audit logs, Internet visit data (such as cookies), and recovered fragments from system crashes.
- **Backup Data -** information the institution regularly backs up. These backups contain an enterprise-level view or snapshot in time of the institution's data.
- **Residual Data -** deleted files, unallocated data and data fragments.

Electronic data may be stored on different electronic devices (e.g., internal and external drives, PDAs, smart phones, servers, laptops, backup tapes, etc.) and may also reside at different locations (e.g., on the home or work systems, University or personal systems, in departmental files, in "employee" files, etc.). The same rules apply to **any** computer that stores information potentially relevant to a lawsuit.

All University employees are under a legal duty to preserve all evidence, whether ESI or hardcopy, when notified to do so by the General Counsel's office. Failure to do so may result in fines and may jeopardize the University's position in a claim or lawsuit.

The University will take steps to protect employee and student privacy and to ensure that protected/privileged information is not disclosed, however this privacy can not be guaranteed because the court ultimately determines whether confidential information must be disclosed.

Preservation/Litigation Hold Procedure
The preservation of electronic data is considered a data incident requiring compliance with the University of Massachusetts Data Security Incident Handling Process and Plan.

The following steps shall be followed regarding preservation of ESI:

1. University legal counsel will determine whether, what, and when ESI will be preserved or put "on hold" (i.e., preservation or litigation hold). This will usually occur if a legal claim has been made, if the University has been put on notice that litigation is imminent or if the University has reason to believe that litigation is reasonably anticipated. Upon determination that electronic information needs to be preserved, University legal counsel will inform the appropriate Chief Information Officer (i.e., CIO) and Records Administrator via a written request that a litigation hold should be put in place. This notice shall identify the:

    - Names of the plaintiff(s), defendant(s) and any other known parties or witnesses that may control or possess potentially relevant data.
    - Departments involved.
    - What information needs to be preserved if known (e.g., emails, word processing documents, etc.). This will greatly minimize the amount of unnecessary data collection and resource use.
    - The period of data preservation.

    Preservation notices are confidential and should be shared on a "need to know" basis only.

2. The CIO will identify the Incident Investigating Team Lead (i.e., Lead) and any administrative representatives within the impacted department and authorize ESI preservation activities. The CIO, or their designee, will ensure that:

    - The Incident Investigating Team(s) take steps to preserve ESI. Note that this ESI must be preserved **and** accessible. This means that copies of all application programs and utilities which may be used to process the ESI must also be preserved.
    - Routine record retention/disposition standards and procedures, recycling of backup tapes, disk defragmentation or compression, and manual deletion of electronic data by employees for ESI is put on hold/suspended. Any activity that may result in the loss of the ESI in whole or in part must be discontinued.
    - Any electronic data storage devices or media that may contain ESI is not disposed of. Such devices or media should be stored with the Incident Coordinator or Legal Counsel.
    - Mechanisms or processes have been instituted to preserve any new ESI generated after the preservation notice is given (e.g., future documents created that may be relevant to the case be stored in a specific directory, future mail correspondence be stored in a specific mail folder or a copy sent to a specific mail folder, all systems used for future creation of ESI be backed up on a regular schedule and retained, etc.)

3. The Incident Investigating Team, under the supervision of the Lead, will take immediate steps to preserve all relevant EIS. Preserved EIS will be stored with the Incident Coordinator or Legal Counsel.

4. University Records Management, Retention and Disposition Standards require that Official Records Custodians obtain approval for the transfer/destruction of records for which they are responsible from the appropriate Records Administrator and Archivist. The Records Administrator shall review these records to ensure no litigation hold exists prior to giving approval for the record transfer/destruction. If such records have a litigation hold the Records Administrator will ensure that the records are properly transferred to the Incident Coordinator.

5. University legal counsel, in coordination with appropriate CIO and Lead, will identify the set of data that must be preserved (e.g., emails related to employee x), discuss how the ESI was collected and discuss any other processes or circumstances particular to the specific lawsuit.

6. Upon determination that the electronic information preservation can be removed, University legal counsel will inform the appropriate CIO and Records Administrator via a written request that the preservation notice can be removed. Removal of a preservation notice generally occurs when the statute of limitations related to the claim has expired or when the lawsuit and all appeals have ended.

7. Upon receipt of the removal of preservation notice from University legal counsel, the CIO will notify the Lead and appropriate administrative representatives of the impacted department that normal record retention/ disposition, recycling of backup tapes disk, defragmentation or compression, and manual deletion of electronic data by employees for the previously preserved electronic information can resume. The previously preserved data will be properly disposed of by the Incident Coordinator.

Preservation Methods

Depending on the application, location and format of the electronic information the specific method used to preserve the electronic information will be different. Regardless of the method used, it is critical that the integrity of all evidence is maintained, and chain of custody (i.e., legal term that describes the collection, transportation, and storage of evidence to prevent alteration, loss, physical damage, or destruction) is established (see the University Data Security Incident Handling Plan and Process for more information regarding chain of custody requirements). The first step in authenticating evidence is that the original evidence needs to be preserved by removing it from normal use and sealing it from possible tampering. Once you preserve the evidence, it needs to be forensically copied in a way that does not alter the original. Electronic data should be captured as soon as possible and the process of making copies of evidence should be witnessed and signed off by an independent party.

Electronic information preservation methods may include, but are not limited to:

- **Desk Top And Laptop Hard Drives; Blackberries; and PDA's**- Imaging. Suggested protocols for hard drive imaging can be found within guidelines standardized by institutions and organizations like the Department of Justice (DOJ) and the National Institute of Standards and Technology (NIST). Cell Phone standards can be found in NIST Draft 800-101, "Guidelines on Cell Phone Forensics". PDA standards can be found in NIST Special Publication SP800-72. Once imaging is completed, a digital fingerprint of the acquired media (i.e., MD5 hash) should be created.
- **Instant Messaging –** Collect Backup Tapes including logging.

- **Mail Server** – Collect Backup Tapes of Email Content and Server Logs. Reroute Copy Of New Emails To Duplicate User Mailbox.
- **Smart Phones** – Physical (a bit by bit copy of an entire RAM chip) and logical (bit by bit copy of directories and files) data acquisition. Guidelines found in NIST document NISTIR-7250.
- **Web Server** (external and internal, SharePoint, IntraLearn, etc.) – Collect Backup Tapes

NIST has also developed the document SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response" which may be helpful when preserving ESI.

Discovery
The following steps shall be followed upon receipt of a discovery request for ESI:

1. Upon receipt of a request for ESI, University legal counsel will inform the appropriate CIO via email that the discovery process has begun.

2. The CIO will assign information technology (i.e., IT) staff to assist University legal counsel with compiling specific information requirements.

3. Assigned IT staff will meet with University legal counsel to determine:

    - Specific requirements (e.g., search terms, data types, timeframes, etc.).
    - Cost of compliance with the discovery request.
    - Any extraordinary circumstances that may impact compliance with the discovery request.

4. Assigned IT staff will generate a set of preserved ESI based on agreed upon requirements.

5. University legal counsel will determine whether the set of preserved data is sufficient to meet the requirements of the discovery request.

6. If requested to do so by University legal counsel, assigned IT staff will work to retrieve additional ESI whether from central or local data repositories.

7. University legal counsel will review the retrieved ESI to determine legal relevance, privilege or other protected status and will handle the discovery response.

Compliance
Failure to comply may result in disciplinary action, and/or restrictions on University computer use/access.