University of California, Merced

Measures Regarding Litigation Holds and Preservation of Electronically Stored Information (ESI)

Responsible Officials:	Executive Vice Chancellor and Provost Vice Chancellor for Business and Administrative Services
Responsible Office:	Campus Counsel
Issuance Date:	04/22/2014
Effective Date:	04/22/2014
Summary:	Guidance for Ensuring Legal Compliance in Preserving and Handling Electronically Stored Information Requested in Discovery
Scope:	This procedure applies to all University administrative, academic, and research units.

Contact:	Carol Castillo, Risk Manager
Email:	ccastillo22@ucmerced.edu
Phone:	(209) 228-4763

I. REFERENCES AND RESOURCES

Federal Laws and Regulations
- Federal Rules of Civil Procedures

State Laws and Regulations
- California Electronic Discovery Act

UC Policies
- Business and Finance Bulletin RMP-1: University Records Management Program
- Business and Finance Bulletin RMP-8: Legal Requirements on Privacy of and Access to Information

II. POLICY SUMMARY

When a legal claim has been filed or is reasonably anticipated, the University may be required to initiate a litigation hold to preserve past and future information in both written and electronic form. This includes electronically stored information (ESI) in its original electronic form that may be relevant to the claim.

Generally, identifying, segregating, and preserving written information, such as written files and records, are straightforward. But in order to comply with its legal obligation with respect to the preservation of ESI, the University must be able to identify the location and format of ESI, determine how to preserve the information identified, and have clear records retention and disposition standards that are consistently followed and executed by all campus personnel.

The ESI preservation procedures set forth below describe the ESI preservation measures that will be taken when the potential need for a litigation hold is identified. Depending on the type of claim identified or nature of potential ESI identified, additional case-by-case measures may need to be developed by the E-Discovery Team.

III. DEFINITIONS

Preserve: Preserve means to preserve evidence in original form in which it was created until litigation or potential litigation is resolved. This includes new information generated after the hold is implemented. Preserving information does not necessarily mean "producing" that information. A decision about what to produce will be made by campus counsel after litigation is filed.

Electronically Stored Information (ESI): Electronically stored information (ESI) and data are subject to possession, control, or custody of an institution regardless of its format and the media on which it is stored. ESI includes, but is not limited to: electronic files; communications, including email and instant messages sent or received, and voicemail; data produced by calendaring software; and information management software. In addition to specific data that are electronically stored and readily retrievable, ESI includes data that may not be visible that is generated by computer hard-drive, email and instant messaging, information management software, handheld computer devices (ex: Android), telecommunications devices, and back-up storage devices. ESI may be stored on different electronic devices and removable devices (ex: internal and external drives, PDAs, smart phones, servers, laptops, backup tapes, thumb drives, CDs, DVDs) and may also reside at different locations (e.g., on the home or work systems, institutionally-owned or personal systems, in departmental files, etc.). See Attachment 1 for examples of ESI subject to preservation and production.

IV. PROCEDURE

A. WHEN DOES THE DUTY TO PRESERVE ARISE?

The duty to preserve may arise when:

- A demand to preserve evidence is received
- Litigation or court complaint is filed or served
- A court issues a preservation order
- Litigation is reasonably anticipated

Factors to weigh in determining when litigation is reasonably anticipated:

- Threat to sue with some degree of specificity
- Individual's litigation history
- Media or industry interest
- Specific and repeated inquiries/complaints
- Complaint with EEOC, DFEH, OCR
- Major accident or injury occurs
- Contractual performance issues
- Criminal liability issues

In addition, an employee termination will routinely trigger a remote preservation of email accounts for all individuals that may have potentially relevant ESI.

All employees have an affirmative duty to notify the campus Risk Manager whenever they are on reasonable notice that the University may become involved in litigation that could trigger a duty to preserve.

B. ASSESSING THE NEED FOR AND INITIATING A LITIGATION HOLD

1. When circumstances are identified that may require a litigation hold, the Campus Counsel and Risk Manager will evaluate whether those circumstances indicate a need to preserve documents and decide whether to issue a litigation hold notice.

2. The Campus Counsel and Risk Manager will identify a liaison in the department(s) who is likely to have potentially relevant knowledge and/or evidence of the claim/dispute. The liaison identified should not include individuals directly involved in the claim/dispute.

3. The Campus Counsel, Risk Manager, Information Security Officer, and the department liaison identified for a given claim/dispute comprise the core E-Discovery Team.

C. DETERMINING THE SCOPE OF THE LITIGATION HOLD AND RELEVANT ESI

The E-Discovery Team will take the following steps:

1. Determine the scope of information that should be preserved.

2. Identify and locate potential sources and locations of ESI (See Attachment 1).

3. Identify key individuals who may have potentially relevant ESI.

4. Determine retention practices for active data and archives, and back up data accessibility and retention practices.

5. Determine cost of compliance and how costs will be allocated.

D. IMPLEMENTING THE LITIGATION HOLD

Campus Counsel in consultation with Risk Manager will:

1. Authorize and implement a remote preservation of email accounts for all individuals that may have potentially relevant ESI.

2. Send the official litigation hold notice to all identified key individuals advising them of their legal obligation to preserve and not delete, destroy, alter, or modify pertinent ESI. This notice shall identify:

    a. Names of the plaintiff(s), defendant(s), and any other known parties or witnesses that may control or possess potentially relevant data;

b. Departments involved;

c. What information needs to be preserved;

d. The period of data preservation.

3. Ensure that recipients immediately return written confirmation of receipt of notice, which includes a statement that they will abide by the notice within a specified deadline.

4. Send reminder notices quarterly in cases of lengthy disputes.

5. Send written notice when litigation hold is released. Removal of a hold generally occurs when the statute of limitations related to the claim has expired or when the lawsuit and all appeals have ended.

E. COLLECTION AND RETENTION OF ESI

1. Key individuals in possession of potentially relevant information are under a legal duty to immediately preserve the documents wherever located and in whatever form when notified to do so.

2. Under the guidance of the Information Security Officer, key individuals will:

   a. Put on hold or suspend routine record retention/disposition standards and procedures, recycling of backup tapes, disk defragmentation or compression, and manual deletion of electronic data. **Any activity that may result in the loss of the ESI in whole or in part must be discontinued.**

   b. Preserve and maintain ESI created after receipt of the litigation hold if relevant to the case.

   c. Preserve all potentially relevant ESI on active systems and hard copy files and segregate active data into identified folders

      - General communications
      - Privileged communications

   d. Move any newly created data related to the potential claim into these identified folders periodically.

   e. In addition to the segregation and preservation of ESI by key individuals, at the direction of Campus Counsel, the Information Security Officer will place an automatic litigation hold on specified affected Outlook accounts in order to preserve any emails deleted from the account during the period of the litigation hold.

3. The Information Security Officer will notify Risk Manager when the ESI collection process is complete.

4. If back-up data storage must be preserved, the Information Security Officer will remove the relevant data storage from rotation and preserve.

5. The Information Security Office will assess back-up data storage on a case-by-case basis:

    - Duplicative of active data:

      If active data is already being preserved, then recycling of backup data storage can continue.

    - Sole source of potentially relevant data:

      If ESI on back up data storage is not available from readily accessible sources, then data storage may need to be preserved.

    - Used as archive:

      If data on backup data storage is made available upon request, it is similar to active data.

6. Before litigation is reasonably anticipated, routine, good-faith document retention operations that destroy ESI are protected under the law. This includes recycling of back up data storage and deleting accounts.

7. When an employee under duty to preserve is separated, transferred or reassigned, the department must ensure that the ESI continues to be preserved.

8. The department will follow University records retention policy upon removal of the hold. The previously preserved data will be properly disposed of by the Information Security Officer.

F. MAINTAIN WRITTEN RECORD

1. The Risk Manager will maintain written records of:

    a. The initial decision making process

    b. Retained reasonably accessible ESI

    c. Retained ESI not reasonably accessible

    d. ESI not retained and reasons for decision

    e. Notices and receipts of preservation requests

    f. Confirmations of preservation

    g. Quarterly reminders of litigation hold

    h. Notices of release from preservation duty

G. FUNDING OF LITIGATION HOLDS AND ESI PRESERVATION

Funding for the hard costs (such as equipment and storage capacity) associated with a litigation hold and ESI preservation is the responsibility of the department(s) in which the claims/disputes arose. The Information Security Officer will maintain the necessary equipment to implement litigation holds and ESI preservation in a timely manner. The department will be recharged by IT for the hard costs associated with the litigation hold and preservation of ESI.

H. COMPLIANCE

Failure to respond or to respond in a timely manner to an e-discovery request can result in fines and/or penalties and may jeopardize the University's position in a claim or lawsuit. **Disciplinary consequences may follow if the litigation hold is not complied with.**

ATTACHMENT 1

ESI CHECKLIST

Data Files:

☐Active
☐Archived
☐Backups
☐Legacy
☐Internet (Web)

System Files:

☐Audit trails
☐Access control lists
☐Metadata
☐Logs
☐Internet "Footprints"
☐Cookies
☐Internet History
☐Browser Activity

Electronic Communications

☐Email
☐Instant messages

Hardware Devices

☐Servers
☐Desktops
☐Laptops
☐Personal Digital Assistants (PDA)
☐Mobile Phone
☐USB Drives
☐Network appliances
☐Storage area Networks (SANS)
☐Backup Media (e.g., CD, tape)
☐Internal and external disk drives
☐MP3 / IPOD players
☐Other _____

Software Applications

☐ERP systems
☐CRM Systems
☐Financial / Accounting Systems
☐Student Information Systems
☐e-Learning Management Systems
☐Software application code
☐Email systems / service
☐Voicemail systems
☐Instant messaging system / service
☐Calendaring systems
☐Network activity monitoring systems
☐Third-party systems? (e.g., ISP, outsourcer, etc)
☐Archiving / Records Management systems (e.g., Filenet)
☐Collaboration systems
☐Database various
☐Spreadsheets
☐Other _____

Locations:

☐Work devices, applications and departments
☐Home devices and applications
☐Third-party devices and applications