Preservation of Electronic Records for Litigation
University Operations - Administrative

EWU Policy 201-02
Effective: December 2, 2008

Authority: Board of Trustees
Proponent: University President

Summary: This policy describes standards and procedures for preservation and retrieval of records and information-Electronically Stored Information (ESI) at Eastern Washington University as required for pending or reasonably anticipated litigation.

History: This policy revises and supersedes the previous version dated publication is new. It was adopted during open session of the EWU Board of Trustees on December 2, 2008 and is effective as of that date.

Applicability: This policy applies to all Eastern Washington University employees and Eastern Washington University records.

Delegation: The Board of Trustees delegates authority for modification of appendices to this policy to the University President.

Review: This policy will be reviewed every three years.

Supplementation: Supplementation of this policy is not authorized.

Suggested improvements: Users are invited to send comments and suggested improvements to:
Office of the President
ATTN: Policy Administrator
Eastern Washington University
214 Showalter Hall
Cheney, WA 99004

Contents
Chapter 1
Introduction
- Purpose • Paragraph 1-1
- Background • 1-2
- Actual or Anticipated Litigation • 1-3
- References • 1-4

Chapter 2
Responsibilities
- University President • 2-1
- Lead Unit • 2-2
- Information Preservation Team • 2-3
- University Records Officer • 2-4

Chapter 3
Electronically Stored Information (ESI)
- ESI Types / Formats • 3-1
- ESI Locations • 3-2

Chapter 4
Preservation of Records
- General • 4-1
- Information Preservation Plan • 4-2
- Litigation Hold • 4-3
- Litigation Hold Responsibilities • 4-4

Chapter 5
Retrieval of Records
- General • 5-1
- Records Retrieval Options • 5-2
- Considerations in Records Retrieval • 5-3
- Post-Retrieval Review • 5-4
- Post-Production Duties • 5-5

Appendices
A. Process Flowcharts
B. Frequently Asked Questions
C. Information Preservation Plan — Sample
D. Litigation Hold — Sample
E. ESI Sources / Locations
F. Computer System Checklist — Individual
G. Statement of Compliance — Sample

Ending Preservation Requirements • 4-5
1. INTRODUCTION

1-1. Purpose

This document establishes Eastern Washington University policy and procedures for the retrieval and preservation of electronic information and material in response to pending or anticipated legal actions.

1-12. Background

EWU is required by federal and state law. Court decisions and rules place obligations on public and private organizations to preserve records and information. Electronic materials that could be relevant to pending or reasonably anticipated lawsuits or external investigations and to retrieve and produce such materials in the course of such litigation. Failure to meet these obligations may subject the university and the individuals involved to sanctions and liability.

Although these legal duties require that information be preserved, the preserved information need not be disclosed to legal opponents without first being appropriately reviewed to ensure legally privileged information is removed. The university, in collaboration with the Assistant Attorney General, and its attorneys will take steps to see that legally protected information is not disclosed to the opposing party.

1-23. Actual or Reasonably Anticipated Litigation

The obligation to preserve potential evidence arises most commonly when there is actual or reasonably anticipated litigation. A lawsuit has already been filed. However, the obligation can also arise when one knows or should know that future litigation is “reasonably likely.” Any university employee who receives notice of a potential lawsuit against the university must contact either the university’s risk manager or the university’s Assistant Attorney General.

The risk manager and Assistant Attorney General will determine whether, based on the information provided, litigation is reasonably anticipated. Determining when facts or circumstances are reasonably likely to lead to litigation requires a case-by-case consideration of the facts based on experience and professional judgment. Factors which can indicate whether litigation is “reasonably foreseeable” or “reasonably likely” include:

a. Historical Experience – similar situations in the past that led to litigation
b. Filed Complaints – complaints filed with the university or an enforcement agency
c. Significant Incidents – events resulting in known and significant injury
d. Attorney Statements – statements by an attorney regarding a dispute with the university

e. Employee, or Student or third party Statements – statements by employees or, students or officials or third parties regarding potential litigation
f. Initiation of Dispute Resolution Procedures – initiation of a dispute resolution clause in a contract
g. Public Records Disclosure Requests – public records disclosure requests which suggest likely future litigation
h. Event Reported In the Press – events reported in the press, where history suggests litigation

1-4. References

a. RCW 40.14, Preservation and destruction of public records

2. RESPONSIBILITIES

2-1. University Risk Manager/University President

The University President, when deemed necessary, will appoint a staff member to head the lead unit for the legal matter at issue.

2-2. Lead Unit

The University Risk Manager/Lead Unit is responsible for a group organized for the purpose of coordinating and overseeing all university activities in response to a current or reasonably anticipated litigation legal matter. Typically, the Lead Unit will be headed by a duly appointed staff member and will include representatives of the Attorney General’s Office and the division of Human Resources, Rights and Risk. The University Risk Manager shall coordinate information gathering and preservation consistent with applicable laws and university policies.

2-2. Assistant Attorney General

The Assistant Attorney General (AAG) initiates and facilitates preservation efforts for the university.

2-3. University Employees Information Preservation Team

All university employees have an obligation to immediately notify the university’s AAG when they are aware of somebody filing or threatening to file a lawsuit or a complaint with an external agency. To help meet its obligations, the university uses an Information
Preservation Team: The purpose of the team is to help gather and preserve relevant information consistent with applicable laws and university policies. The Information Preservation Team is made up of representatives from:
The Attorney General’s Office
Human Resources, Rights, and Risk
Information Technology
University Records Office

2-4. University Records Officer
As required by RCW 40.14.040, the University Records Officer manages and oversees university compliance with state and federal laws and regulations relating to the preservation and destruction of electronic and paper information.

3. ELECTRONICALLY STORED INFORMATION (ESI)

3-1. ESI Types / Formats
This policy specifically pertains to the preservation, retrieval, and disclosure of Electronically Stored Information (ESI). ESI includes all forms of electronic communications and records. Examples of ESI include, but are not limited to:

- Email messages
- Text (SMS) messages
- Word-processing documents
- Documents shared on drives, such as Sharepoint, Dropbox, Google Drive
- Spreadsheets
- Databases
- Digital images
- Video files
- Audio files (including voicemails)
- Web pages
- Instant messages
- Blogs
- Calendars
- Internet cookies
- Internet bookmark / favorite addresses

3-2. ESI Locations
The requirements for preservation and retrieval of ESI apply without regard to where the ESI is stored – at a university work station, on a laptop or mobile device, PDA, and even at an employee’s home.

While many records are stored on network servers, many other ESI records are stored on individual desktop computers, or portable devices, or on shared drives. Email messages, for instance, may be maintained on the university servers or copied in “local folders” on an individual desktop, laptop, mobile device, PDA, etc.

ESI may also be available on backup storage media. The university maintains a backup process that periodically copies system data to backup media in order to enable system restoration in the event of an emergency. The backup system recycles storage media on a regular basis. For normal preservation purposes, emergency recovery copies of data are not practically accessible and interrupting their recycling would be impractical and expensive. As a result, such disaster recovery systems will usually be considered outside the scope of a Notice of Records Preservation, unless otherwise directed.

A checklist for identifying potential locations for ESI is at Appendix E.

CHAPTER 4
PRESERVATION PROCESS OF RECORDS

4-1. General
When a lawsuit is filed – or reasonably anticipated – the university must take special precautions to prevent the loss or destruction of potentially-relevant electronic data/information. Unless circumstances require a different approach, the procedures described in this section serve as a guide for responding to potential litigation in this chapter will be followed.

4-2. Information Preservation Plan
When a lawsuit is commenced against the university – or information is received such that a lawsuit is reasonably anticipated – the Risk Manager, in consultation with the AAG, Lead Unit, in consultation with the Information Preservation Team, shall assess the issue and its risks and determine the university’s immediate preservation response. A Preservation Plan outlining the immediate steps that need to be taken. An example preservation plan is shown in Appendix C.

The university’s response efforts will typically include:

1. Identifying the departments, operating units, and individuals who might possess potentially relevant electronic data/information and notifying them of their responsibilities to preserve potentially relevant information;
2. Assessing what electronic records might need preserving and developing a plan for gathering and preserving such records. Send a Litigation Hold to the individuals identified; and

3. Designating a specific person to coordinate and serve as a contact, and:
   
   d. Where the matter is complex or unusual, the following steps may also be considered:
      
      (5) Gather a summary of the hardware and software involved. (Sample Computer System Checklists are included at Appendices E and F).
      
      (6) Determine whether more aggressive steps (such as "imaging" or sequestering computers, stopping rotation of disaster recovery tapes, or taking snapshots of network folders) are warranted.

4. Establishing a method for following up, which may include sending out reminders, conducting preservation compliance checks, and addressing new questions or issues from agency employees with potential evidence;

7-5. Under certain circumstances, the university will consider additional preservation efforts such as imaging or sequestering of computers, imaging certain types of ESI, or other technological solutions to supplement the regular preservation efforts.

---

4-3. Litigation Hold

In most cases, key players who may have records relevant to pending or reasonably anticipated litigation will receive a Litigation Hold Notice. A Litigation Hold Notice will typically include:

a. A definition of what constitutes a “record” of potentially relevant information.

b. Direction to protect potentially-relevant records from destruction or modification. (see Appendix C).

c. General information on how to protect records (which might include checklists from Appendices E and F). This may include directing the administrator(s) of relevant system(s) to avoid any centralized or automatic destruction or alteration of such records.

d. Identification of the categories of information to be preserved.

e. Contact information for the Lead Unit and the Information Preservation Team AAG and/or the University Risk Manager.

The AAG will usually send out the Litigation Hold Notice; however, the University Risk Manager or other university official may also issue a litigation hold.

---

4-4. Litigation Hold Responsibilities

Receipt of a Litigation Hold does not necessarily mean the recipient is directly involved in the matter. Rather, it means the potential evidence which the university must preserve may be in the person’s possession or scope of responsibility and that the person, as an employee of the university, must immediately take reasonable steps to preserve such information. In particular, the person must:

a. Acknowledge receipt of the Litigation Hold by signing and returning the Litigation Hold Notice Acknowledgment if one was included in the Litigation Hold Notice.

b. Suspend any university or departmental policies or procedures that might call for the routine destruction of electronic records under the recipient's control.

c. Discontinue personal practices regarding the deletion of electronic records. For example, the deletion of possibly-relevant emails, voice mails, drafts of documents, and the like must also be suspended.

d. Disable any “janitorial” functions, such as the automatic deletion of emails or other electronic records. The designated computer support person should be immediately contacted if assistance is required to disable such functions.

e. Protect and preserve all potentially relevant electronic records in their original electronic form, so that all information within it, whether visible or not is available for inspection. In other words, electronic records must be preserved, regardless of whether they have also been reduced to a hard-copy or whether a hard-copy already exists.

f. Protect and preserve any new documents that are generated or received that may be relevant to the litigation after receipt of a Litigation Hold.

g. Advise the Information Preservation AAG and/or Risk Manager of any personal information that may potentially be affected by the Litigation Hold.

h. Follow all other specific instructions in the Litigation Hold.
i. Consult with the Information Preservation Team AAG and/or Risk Manager regarding any questions involving electronic records.

4-5. Follow-Up
The AAG and Risk Manager shall, as needed, follow up on active litigation holds. They shall also coordinate with the Associate Vice President for Human Resources and other university personnel on preservation of records for outgoing personnel.

4-66. Ending Preservation Requirements
When the litigation or threat of litigation that prompted the Litigation Hold has ended or litigation is no longer reasonably anticipated, the AAG or Risk Manager or their designee Lead Unit will inform those who received the notice that they are no longer under any special obligations to preserve the identified categories of materials. At that point, only the university’s normal retention schedules will apply to the documents. The Division of Human Resources, Rights, and Risk and the university’s attorneys will be responsible for applying their own special retention schedules for “litigation” records.

CHAPTER 5
RETRIEVAL OF RECORDS

5-1. General
In most cases, the need to actually produce preserved electronic records will come weeks or months after the preservation has occurred. When the university receives a request from an opposing party for production (“discovery”) of electronic records, the university’s Lead Unit will determine the best approach to take in order to efficiently produce a complete and accurate response. The response may consist of any or all of the following:

a. supplying the requested information;
b. attempting to obtain a modification of the request (e.g., by narrowing the request’s scope or obtaining agreement as to specific search terms);
c. declining to provide some or all of the requested data based upon expense of production or other basis.

5-2. Options for Records Retrieval
Where some or all of the requested records must be retrieved, reviewed, and potentially disclosed, the following options should be considered in selecting the best approach to the specific request:

a. Relying on the Computer User. In many instances, it is reasonable and sufficient to simply ask the computer user to identify, copy, and provide potentially responsive electronic records and to certify that these steps have been taken. In these instances, the production of electronic data resembles the typical production of physical documents.

b. Enlisting University Technical Support. Sometimes the system administrator or other university technical support personnel will directly retrieve the responsive records due to particular concerns about an individual user’s time, skill, or dependability in identifying the universe of responsive records. Such personnel are often able to bring to bear sophisticated tools for searching and extracting large volumes of responsive records.

c. Using Outside Consultants. Where identification or recovery of records requires technical expertise beyond that readily available from internal resources, an outside firm may be called upon for some or all of the work.

5-3. Factors to Consider in Records Retrieval
a. Thoroughness. The approach in a specific case needs to be reasonably calculated to gather all potentially relevant records.

b. Operational Efficiencies. The activities required should be operationally efficient to ensure timely preservation and processing of the data.

c. Individual Privacy. The processes implemented to respond to electronic discovery must take into account personal privacy concerns.

d. Risk of Data Loss. Reasonable steps will be needed to protect data from loss through inadvertent or intentional deletion of files or loss of data storage media.

e. Individual Disruption. Procedures should take into account potentially significant impacts in terms of time and effort for individuals named in the lawsuit.

f. Procedural Consistency. The University will require that procedures developed to meet these new rules are consistently followed and executed.

5-4. Post-Retrieval Review
As potentially responsive electronic records are gathered, they will be provided to the Lead Unit for further processing.

5-5. Post-Production Duties
Preservation and production of information related to a lawsuit does not end with an initial production of records. Potentially relevant records generated after
the Litigation Hold must be preserved for possible future retrieval.
**Record Preservation**

- **Lawsuit / Threat**
  - Lead Unit
    - Identify units / people with data
    - Consider other extraordinary steps
    - Work with Information Preservation Team
  - Litigation Hold
    - Data Holders
      - Comply with Litigation Hold
    - System Administrators
      - Comply with Litigation Hold

**Discovery / Production**

- **Discovery Request**
  - Lead Unit
    - Identify response measures
    - Select best method for record search
    - Work with Information Preservation Team
  - Retrieval Instructions
    - Data Gatherers
      - Retrieve & Forward Records
    - Lead Unit
      - Review & Forward Records
APPENDIX B
FREQUENTLY ASKED QUESTIONS
REVISED: Dec 2, 2008

1. What do "electronic discovery" and "data preservation" mean? 
"Discovery" is the process by which potentially relevant documents are captured and produced by the parties in a lawsuit. One of the ways a party can obtain "discovery" of potentially relevant documents is by asking other individuals or entities to produce documents. Federal and state courts recognize that the term "documents" includes electronic data and that electronic data is subject to the same discovery rules as other documents potentially relevant to a lawsuit. The issue has received substantial national attention recently, however, because of a series of court rulings resulting in the imposition of huge sanctions on parties for their failure to preserve electronic data and because of amendments to the Federal Rules of Civil Procedure that took effect on December 1, 2006. Upon notice that a lawsuit has been commenced against the university (or a charge filed with an administrative agency), or if it is reasonably anticipated that a lawsuit may be brought (or a charge filed), the university and all of its faculty and staff members are under a legal duty to preserve all documents, whether hard copy or electronic, that might be relevant to the lawsuit.

2. What data needs to be preserved? 
The new federal rules require a party to suspend routine or intentional purging, overwriting, re-using, deleting, or any other destruction of electronic information potentially relevant to a lawsuit, wherever it is stored – at a university work station, on a laptop, or cellular phone, or at an employee’s home. It includes all forms of electronic communications, e.g., e-mail, word processing documents, calendars, voice messages, instant messages, spreadsheets, SharePoint files, wiki materials, videos or photographs. This electronic information must be preserved so that it can be retrieved – if necessary – at a later time. The information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection – i.e., it is not always sufficient to make a hard copy of electronic communication. However, back-up tapes may not have to be preserved, and the university should consult with their attorneys on a given case regarding the disaster recovery system procedures.

3. What will I have to do? 
You will be notified of the responsibility to preserve electronically stored information (ESI) through a notice called a “litigation hold” or “preservation hold.” You will then be asked to cooperate with the Attorney General’s Office, the Division of Human Resources, Rights, and Risk, and/or university IT personnel in order to identify and preserve reasonably identifiable potential sources of ESI in your possession or under your control. You may be asked to complete and return a questionnaire identifying all potential sources of ESI. If so, it is critical that you complete and return the questionnaire without delay. You may also be asked to complete a signed statement confirming that you have completed the required search and retention as requested. Until IT personnel have taken steps to preserve your ESI, you should be particularly careful not to delete, destroy, purge, overwrite, or otherwise modify existing ESI.

4. How long will this go on? 
The university’s counsel and/or primary university contact (Risk Management, Human Resources or other unit) will advise you when you and the university are no longer obligated to retain the preserved data. Generally, this will be when the statute of limitations has expired with respect to the claim or – if litigation has been commenced – when the lawsuit and all appeals have concluded. When preservation effort ends, the preserved data will be returned to you or destroyed, at your option and in accordance with records management schedules. If at any time you question whether to continue retaining the records, you should contact the appropriate contact person listed in the Litigation Hold communication before destroying any documents.

5. Do I need to also preserve data on my home computer? 
The same rules apply to any computer that stores information potentially relevant to a lawsuit involving the university. Thus, if you use your home computer for university-related business (including e-mail on your university e-mail account or on a personal account such as AOL, Gmail, etc.), you must preserve the data on that computer.
6. Can I take personal or sensitive material that isn’t relevant to the case off my computer?  
You may be questioned under oath at a later date by an attorney representing the opposing party about what data you took off your computer. Thus, if you believe there is something personal on your computer, you should consult...before removing it. The material may also be a public record, and public records are subject to the university’s retention policies.

7. I previously deleted something that might be relevant — should I be concerned about that?  
Preservation of information arises when there is a lawsuit, reasonable anticipation of litigation, or if there has been a public records request. Electronically stored information deleted before a lawsuit, reasonable anticipation of a lawsuit or a records request that was properly deleted pursuant to retention policies, should not create a problem.

8. What if I am involved in an ongoing matter relating to the person who is suing the university?  
You must also preserve any newly created documents generated after receipt of a litigation hold that may be relevant to the dispute (such as an employment claim by a current employee where relevant new documents may be created during the ongoing employment relationship).

9. Who is going to be paying for the cost of preserving electronic records?  
Most external costs (such as IT consultants) associated with complying with the electronic discovery requirements will be handled in the same manner as other litigation expenses are presently handled. Internal costs (time spent by university staff members, applicable storage costs and the like) will be absorbed by the department.

10. Who will be looking at university data from my computer?  
This depends on the reason for the Litigation Hold. If the matter involves a complaint or claim that requires investigation, appropriate university department personnel from departments such as the President’s Office, the Division of Human Resources, Rights, and Risk, the Attorney General’s Office, and perhaps others may be reviewing records in your computer files in the course of the investigation. In other cases, it may be that no one will initially review your records until and if there is a lawsuit filed with discovery requests made.

11. Who decides what data will be turned over to the opposing party?  
The university, as owner of the data, will make these decisions based on advice from its attorneys. Before any data is turned over to the opposing party, the university’s attorneys will review it for relevance and confirm it is not otherwise protected or privileged.

12. Since when did we have to go to all this trouble?  
Because of the egregious misconduct by several organizations and because of the ever-widening use of computers, over the last several years the courts have developed rules specific to the preservation of electronic data. The new amendments to the Federal Rules of Civil Procedure addressing electronic discovery took effect December 1, 2006.

13. What should I do with my electronic data if I leave the university?  
If you plan to leave your employment with the university during the pendency of a lawsuit for which you have received a preservation hold, you should confer with your supervisor, university IT staff and the Attorney General’s Office or other contacts listed in the Litigation Hold notice.

14. What if I have additional questions?  
Get in touch with the university’s counsel and/or primary university contact (Risk Management, Human Resources or other unit) contacts listed in the Litigation Hold notice.
MEMORANDUM

To: [Individual with ESI], [Department]

From: [Head of Lead Unit or Information Preservation Team], [Title], [Mailstop]

Date: Sep 12, 2008

Re: [Description or reference to description of Matter]

{Greeting},

To prepare for the defense of the actual or potential litigation described, the university will need access to a complete copy of all documents that could reasonably relate to this matter. These documents may reside in your office, your home, may be held in the university records center and/or university archives, or may exist in other places.

“DOCUMENT” INCLUDES A WIDE VARIETY OF RECORDS AND MATERIALS.

Be aware that “document” typically is broadly defined by courts to include, among other things:

• writings
• e-mails
• drawings
• graphics
• charts
• photographs
• phone records
• images
• all electronically-stored information, and
• any other data compilations from which information can be obtained.

DO NOT DESTROY, DELETE OR DAMAGE ANY DOCUMENTS THAT MAY RELATE IN ANY WAY TO THIS MATTER.
It is important that potentially relevant documents that can be reasonably identified be retained, preserving as well the original format, if feasible. In addition, if you are aware of other documents that may be relevant but which you do not currently have access to, please so inform ____________. In addition, please suspend any scheduled destruction, archiving, or deletion of documents related to this matter until you specifically have been advised that you are authorized to do so. Failure to comply with any of the above could result in penalties imposed upon the university and/or you by a court.

INCLUDE EVERYTHING REASONABLY RELATING TO THIS MATTER.

Since it is early in this matter, it is difficult to determine what information may or may not be relevant. However, at a minimum, you should retain the originals and copies of documents that can be reasonably identified as being potentially relevant (including emails and electronically stored documents) that you may have in your possession that: (1) were sent to or from ____________, (2) refer to __________ by name, title, or implication, (3) relate to any employees in __________’s work group and managers and/or discuss their duties and performance, (4) relate in any manner to __________’s performance or (termination), including to any event in which __________ was investigated, disciplined or counseled, (add other matters pertinent to case).

If you have any doubt as to whether a document might be relevant, retain it. Do not delete or dispose of it. You should retain the documents in a place where they can be easily located upon request. Please do not hesitate to communicate with ________ if you have any questions.

Since “documents” include existing documents, as well as documents that may be created in the future, you also should provide this office with documents created since your receipt of this letter.

IF YOU HAVE QUESTIONS ABOUT THESE INSTRUCTIONS, CONTACT ONE OF THE FOLLOWING INDIVIDUALS

_________________________

_________________________

_________________________
This list can help identify potential locations of ESI that may be relevant to a litigation issue. Additionally, individuals who receive a Litigation Hold may use this list to help record the different locations where they believe relevant ESI is located.

### Servers
Describe each server or server cluster: what kind, their purpose, and how many.

### Mainframes
Describe what kind, their purpose, how many

### Digital printers, copiers, scanners
List any devices in which ESI gets stored in scanning directories and is not saved to the main server directory.

### SharePoint, wiki, or Blog Sites
List employee chat rooms or collaborative space where work is conducted or conversations occur.

### Password Protected Internet Sites
List all sites used by employees who work with outside consultants through a password protected internet site.

### Backup Tapes

### Text or Instant Messaging
List any applications that enable employees to send “text or instant messages”

### Databases
List any databases and indicate what, when, where and how many

### Email lists
Specify any email lists (what, when and who is on it)

### Metadata Scrubbing Software
Indicate if you use this type of software on any of your storage

### Portable Storage Media (Media Card, CD/DVD, Flash Drives, etc.)

### Computers (Desktop, Laptop, Ultra-Mobile PCs, etc.)

### Portable Electronic Devices (Cellphone, PDA, IPod, etc.)
The checklist below may be used by individuals as they determine potential locations of electronically stored information (ESI) that might assist the university in responding to a potential or existing lawsuit.

Name ___________________________ Date ____________
Campus address ____________________________
Campus phone ____________________________
Email address ____________________________

1. Computers
Please identify other computer systems (including home computers, laptops, blackberry, and personal digital assistants) you use to conduct university business.

For each computer system that you use, please answer the following. For “Name” please enter a unique designation which will allow you to distinguish this system from the others that you use. If you are sure that a system has no information related to your position at the university, you do not need to list it.

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Type</th>
<th>Ownership</th>
<th>Location of Use</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>university or personal?</td>
<td>Home, office, travel, all?</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Data storage
Besides the internal hard disc(s) in the above system(s), please list the other places where you store electronic data related to your position at the university. Note that back-ups are treated separately in the next section. If a data store is associated with one of the computers listed above, please enter that system’s number as listed in the first column above.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Purchase $</th>
<th>Location of Use</th>
<th>Computer No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>university $ or personal $?</td>
<td>Home, office, travel, all?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Backups
Please state how the backups are completed for each system listed above.

<table>
<thead>
<tr>
<th>Computer No.</th>
<th>Type and Location</th>
<th>Schedule for Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Departmental Network Backup, Local Tape, Local DVD, etc.?</td>
<td>Daily, weekly, irregularly?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. Mail service
List the email service(s) on which you send or receive university-related messages. If you store messages on a local computer, give the associated system number(s).

<table>
<thead>
<tr>
<th>Service</th>
<th>Use</th>
<th>Messages Stored Locally?</th>
</tr>
</thead>
<tbody>
<tr>
<td>university email Service, Department mail Service, MSN, AOL, Yahoo, etc.</td>
<td>Work, personal, or both?</td>
<td>on Computer No.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Collaborative work
List any Web pages, email lists, blogs, wikis, or other collaborative environments you participate in for university work.

<table>
<thead>
<tr>
<th>Collaborative system</th>
<th>Location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiki, SharePoint, Web server,</td>
<td>URL, archives, etc.</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Your primary computer support person/group
Complete the contact information for the individual or group that provides your computing and networking support.

Name _____________________________
Email address ____________________________
Phone number ___________________________
Employee Signature ___________________________
APPENDIX G
STATEMENT OF COMPLIANCE
REVISED: Dec 2, 2008

THIS DOCUMENT IS PROVIDED UNDER THE ATTORNEY-CLIENT PRIVILEGE AND SHOULD BE CONSIDERED CONFIDENTIAL

I was assigned responsibility by the Eastern Washington University to search for specified documents on behalf of the agency pertinent to [INSERT CASE NAME].

In accordance with instructions, procedures, and directions received from the representative of the university's legal team, I conducted a reasonable, diligent and good faith search of the files and records in my possession or control.

To the best of my knowledge, information and belief, I have identified the potentially relevant documents maintained in the ordinary course of business that may be responsive to the requests for production have been provided to the representative of the university's legal team. I am aware of no documents in university files that are responsive that have not been thus provided, and I have no reason to believe that any such documents exist.

DATED this _________ day of __________________, [year].

Signature

Others Who Assisted:

Print Name

Telephone; Address

Files For Which I Was Assigned Search Responsibility