POLICY TITLE	Retention of Electronic Files	**Policy Number**	451
Section	Facilities, Operations, and Information Technology	**Approval Date**	October 9, 2008
Subsection	Information Technology	**Effective Date**	October 9, 2008
Responsible Office	Office of the Vice President of Finance and Administration		

1.0 PURPOSE

1.1 The purpose of this policy is to establish rules and procedures for the retention of electronic documents, messages, and files in accordance with state and federal law and the established practices of the University.

2.0 REFERENCES

2.1 *Computer Matching and Privacy Protection Act of 1988,* P.L. 100–503

2.2 *The Privacy Act of 1974,* 5 U.S.C. § 552a (2000)

2.3 *The Freedom of Information Act,* 5 U.S.C. § 552, As Amended By, Public Law No. 104–231, 110 Stat. 3048

2.4 Utah State Code, Title 63G, Chapter 2, *Government Records Access and Management Act (GRAMA)*

2.5 Utah State Board of Regents' Policy R132 *GRAMA Guidelines*

2.6 UVU Policy 133 *Compliance with Government Records Access and Management Act (GRAMA)*

2.7 UVU Policy 443 *Ethics in Computer Usage*

2.8 UVU Policy 449 *Private Sensitive Information*

3.0 DEFINITIONS

3.1 "Shredding" of electronic documents/data: A process or device that physically demolishes the platters of a hard disk to ensure that the contents can never be recovered. Hard drive shredding services may be offered by service companies that shred paper and microfilm. These

procedures require that the data are "shredded" (meaning over-written with meaningless data) or the device/IT resource storing the data is physically destroyed.

4.0 POLICY

4.1 The individual creator, sender, and/or receiver of electronic messages, documents, and files must determine which information should be retained or archived. Records should be retained in accordance with the University's financial and administrative policies on records retention and disposition (UVU Policy 133 *Compliance with Government Records Access and Management Act*), Utah State code, and federal law.

4.1.1 Records that are retained by an individual, even if they are retained on an electronic medium, are subject to the *Freedom of Information Act* and the *Privacy Act*.

4.1.2 Current electronic technology available to individuals is not considered acceptable for archival storage, except for specifically approved systems.

4.1.3 Documents judged to be archival should be stored on an appropriate medium.

4.1.4 All electronic data stored on university-leased or -owned equipment is subject to this policy.

4.2 Electronic mail and voice communications are vehicles for delivery of information and not mechanisms for the retention or archiving of such information.

4.3 When equipment is retired from service or is transferred to another individual, disposal or "shredding" of electronic documents or data on that equipment is required.

5.0 PROCEDURES

5.1 List of Approved Electronic Systems for Archival Storage

5.1.1 Only approved systems shall be used for archival storage. Approved systems include the Banner Administrative Systems and the BMI Imaging System. To qualify, systems must have an archival backup system and schedule and must be approved by the Enterprise Application Committee (EAC). A complete list of approved systems shall be maintained by Information Technology.

5.2 Retention Practices of E-mail

5.2.1 Electronic mail ("e-mail") is a method of communicating information and does not necessarily constitute a public record in and of it. However, the information transmitted through the use of e-mail may become a public record if it meets the definition of a "record" pursuant to

Utah Code 63-2-103. If information transmitted by e-mail meets the definition of a "record," then it may not be deleted or otherwise disposed of except in accordance with a records retention schedule approved by the State Division of Archives or allowed by UVU's record retention guidelines. The content of the e-mail message determines the retention requirement.

5.2.2 The legal "custodian" of an e-mail message is normally the originator of the message, if that person is a university employee; otherwise, it shall be the individual to whom the message is addressed once the message is received. The legal custodian is the person responsible for ensuring compliance with Utah's *Government Records Access and Management Act (GRAMA)*. See Utah Code 63-2-101, et seq. Although most state entities also periodically backup information residing on system hard drives, this is not done for archival purposes or in order to meet the requirements of *GRAMA*, but as a safety measure in case of system failure or unlawful tampering ("hacking"). The system administrator is not the legal custodian of messages which may be included in such backup files. UVU e-mail servers are provided only to facilitate the delivery of e-mail. UVU e-mail servers are NOT provided for archival purposes; therefore, Information Technology cannot guarantee that e-mail delivered to recipients actually originated from the person or persons indicated on the e-mail message.

5.2.3 While all e-mail messages need to be assessed in accordance with *GRAMA*, e-mail messages generally fall into two categories:

1) First, some e-mail is of limited or transitory value. For example, a message seeking dates for a proposed meeting has little or no value after the meeting date has been set. Retention of such messages in the computer system serves no purpose and takes up space. Such messages may be deleted as soon as they no longer serve an administrative purpose.

2) Second, e-mail is sometimes used to transmit records having lasting value. For example, e-mail about interpretations of a university's policies or regulations may be the only record of that subject matter. Such records shall not be maintained in e-mail format, but shall be transferred to another medium and appropriately filed, thus permitting e-mail records to be purged at regular intervals.

5.2.4 While the methods for reviewing, storing, or deleting e-mail vary, compliance with the retention requirements of *GRAMA* may be accomplished by doing one of the following:

1) Print the e-mail and store the hard copy in the relevant subject matter file as would be done with any other hard copy communication. Printing the e-mail permits maintenance of all the information on a particular subject matter in one central location, enhancing its historical and archival value.

2) Electronically store the e-mail in a file, a disk, or approved UVU server, so that it may be maintained and stored according to its content definition under the pertinent records retention policy.

5.2.5 In the event of any litigation, all pertinent e-mail is subject to discovery and a hold shall be placed on all such email, so that no pertinent e-mail shall be deleted or destroyed.

5.3 Retention Practices of Voice Mail

5.3.1 Phone voice mail communications may be deleted by individuals or by automated rules established by the telephone switch administrator based on the following practices:

1) Individuals may delete at any time voice mail from their voice mailbox.

2) Voice mail may be saved by individual users in their voice mailbox for 30 days. Messages may be saved by individuals for additional 30-day periods of time.

5.4 Retention Practices of Electronic Files on Local Computer Hard Drives and Mediums

5.4.1 Retention of electronic files on local computer hard drives and mediums is the responsibility of individual users and shall be done within the rules of state and federal law and university policies and procedures, including the policy on private sensitive information (see UVU Policy 449 *Private Sensitive Information*). Caution shall be taken by the individuals to secure these devices and backup critical information. Disposal or transfer of devices must be done in accordance with the disposal procedures below. All such information on university-owned computer storage devices is considered university data and may be discoverable within the guidelines of state and federal law and university policy. University data stored on devices not owned by the University is still university-owned data and must be removed from the device upon the request of the University or upon termination of employment with the University. Private sensitive information must be completely destroyed by shredding (see UVU Policy 449 *Private Sensitive Information*).

5.5 Retention Practices of Network Storage

5.5.1 Information that is stored on network storage (U: and S: drives) is backed up and retained according to the following practices:

1) Incremental backups are made on a daily basis at night.

2) Full backups are done weekly.

3) Weekly tapes are kept for three months before they are overwritten.

5.5.2 Department-owned servers and storage may or may not be backed up according to the above schedule.

5.5.3 Departments shall have their own retention procedures and publish them to their affected constituents.

5.6 Retention Practices of Administrative Systems Data

5.6.1 Information that is stored within the Banner Administrative System is backed up and retained according to the following practices:

1) Incremental backups are made on a daily basis each night.

2) Full backups are done every other day.

3) A weekly full backup done on the weekend is duplicated and one copy stored at the University in a tape vault and one copy is sent to an off-site storage facility.

4) Weekly tapes are kept for three months before they are overwritten.

5.7 Disposal Practices

5.7.1 If a piece of computer equipment or electronic storage device is retired or surplused, the following procedures shall be followed:

1) Any identified records that shall be retained by the University shall be removed and stored appropriately.

2) The device shall be electronically shredded so that no information can be retrieved. If electronic shredding is not possible, the device must be physically destroyed.

5.7.2 If a piece of computer equipment or an electronic storage device is transferred to another university employee that requires access to the information on the device (has the same job function and security level), the information may be retained on the device when granted permission by the supervisor.

5.7.3 If a piece of computer equipment or electronic storage device is transferred to anyone else, the following procedures shall be followed:

1) Any identified records that must be retained by the University shall be removed and stored appropriately.

2) The device shall be electronically shredded so that no information can be retrieved.

3) If electronic shredding is not possible, the device must be physically destroyed.

5.8 Procedures for Computer Equipment Repairs by Third Party

5.8.1 When computer equipment containing university data is sent off campus for repair, university data shall be backed up and removed from the equipment if possible and practical. If removal is not possible or is impractical, the data shall be secured as well as possible and the third party shall agree to and sign a confidentiality/nondisclosure document.

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity