POLICY TITLE	Private Sensitive Information	**Policy Number**	449
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 Information Technology		

1.0 PURPOSE

1.1 University information technology resources are at risk from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action. The purpose of this policy is to secure the private sensitive information of faculty, staff, students, and others affiliated with the University, and to prevent the loss of critical operational information.

2.0 REFERENCES

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

2.2 Utah State Code, Title 63D, Chapter 2, *Governmental Internet Information Privacy Act*

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

2.4 Utah State Board of Regents' Policy R341 *Computing Systems Program*

2.5 Utah State Board of Regents' Policy R343 *Information Management*

2.6 Utah State Board of Regents' Policy R345 *Information Technology Resource Security*

2.7 UVU Policy 133 *Compliance with Government Records Access and Management Act*

2.8 UVU Policy 445 *Institutional Data Management and Access*

3.0 DEFINITIONS

3.1 Data custodian: An individual directly responsible for creating, maintaining, and using data to support the University's operation and its information needs.

3.2 Data steward: A senior university official who has planning and policy-level responsibility for data within his or her functional areas.

3.3 Encryption: The process of encoding a message so it can be read only by the sender and the intended recipient (*American Heritage New Dictionary of Cultural Literacy*, 3rd Edition, 2005, Houghton Mifflin Company).

3.4 Enterprise Application Committee (EAC): The management group for enterprise data and data systems which includes all of the data stewards or their designee.

3.5 Incident: A confirmed or suspected security breach.

3.6 Incident Response Team: Directed by the Information Security Officer (ISO) and made up of campus personnel, the Incident Response Team is responsible for immediate response to any breach of security. The Incident Response Team is also responsible for determining and disseminating remedies and preventative measures that develop as a result of responding to and resolving security breaches.

3.7 Information Security Officer: A senior university official, assigned by the President, to oversee the security of the University's electronic data.

3.8 Private Sensitive Information (PSI): Social security numbers, credit card information, health, and medical records, financial records, that give specific information about an individual that is considered private or sensitive and can lead to adverse consequences if disclosed, such as identity theft, financial loss, or invasion of privacy. Access to such data is governed by state and federal laws, both in terms of protection of the data, and requirements for disclosing the data to the individual to whom it pertains. It does not include "public information" as defined by GRAMA or directory information as defined by FERPA.

4.0 POLICY

4.1 University employees, or anyone else given access to university data, must not knowingly retain on personal computers, servers, portable or other computing or storage devices, nor should they transmit by electronic means, any private sensitive information as defined above, unless specifically approved by the Enterprise Applications Committee (EAC) and registered with Information Technology according to the procedures below.

4.2 Employees with PSI access must take reasonable precautions to safeguard the information including, but not limited to, encryption, strong password protection, screen and computer locks, and making screen displays or physical storage devices unavailable to unauthorized personnel.

5.0 PROCEDURES

5.1 Identifying PSI

5.1.1 PSI, secured data, and any other information that must be safeguarded against unauthorized access should be identified and protected. Anyone with access to data resources who is uncertain whether or not an IT resource contains PSI or data that should be secured must seek direction from the Enterprise Application Committee (EAC), the appropriate data steward or data custodian, the campus HIPAA Privacy Officer, or the University's Information Security Officer (ISO).

5.2 Approval, Registration, and Securing of PSI Storage or Transmission

5.2.1 If any individuals need to store, have access to, or transmit PSI for the performance of their duties to conduct the business of the University, they must obtain permission to do so from the appropriate data steward and the EAC, upon the recommendation of their supervisor or department chair, as appropriate; their director or dean, as appropriate; and the respective vice president. The ISO must be notified that permission has been granted. The ISO shall work with the individual, where appropriate, to implement reasonable precautions and provide training to secure the PSI.

5.2.2 Permission is not required to retain student grades, letters of recommendation, and patentable research findings that are used regularly in the performance of faculty and staff duties. However, if a computer containing such data is readily accessible to unauthorized individuals, the responsible resource owner must take reasonable precautions to secure the data.

5.2.3 Security procedures must be designed for IT resources that do not necessarily store, process, or transmit PSI, if access to such IT resources provides the possibility of a breach of security.

5.3 Physical Security of PSI

5.3.1 Individuals are responsible for ensuring that all electronic information, hard copy information, and hardware devices in their possession are physically protected in accordance with the record classification level as either private or protected data (refer to UVU Policy 133 *Compliance with Government Records Access and Management Act).*

5.3.2 Adherence to security controls for each work area, including access restrictions, sensitive data handling procedures, and security plans must be ensured.

5.4 Destruction or "Shredding" of Electronic Media

5.4.1 Departments and individuals shall destroy PSI, as well as other personal or financial information, as appropriate. PSI shall be destroyed on a campus IT resource or on personal computers, servers, or other campus computing devices, using established university procedures, when such information is no longer needed for the conduct of business or for legal purposes.

5.4.2 Data must be “shredded” (meaning over-written with meaningless data) or the device/IT resource storing the data must be physically destroyed.

5.5 Incident Management

5.5.1 All suspected or actual security breaches of university or departmental systems must be reported immediately to the University's Information Security Officer (ISO). The incident must also be reported to the appropriate data steward and data custodian. If the compromised system contains PSI, the incident must be reported to the Assistant Attorney General.

5.5.2 If PSI has been accessed or compromised by unauthorized persons or organizations, the individual who is responsible for the information must consult with their dean, department head, or supervisor; the ISO; their respective vice president; and the Assistant Attorney General to assess the level of threat and/or liability posed to the University and to those whose PSI was accessed. If a threat or liability exists, reasonable effort shall be made to notify the individuals whose PSI was accessed or compromised. If appropriate, those affected shall be referred to the ISO for instructions regarding measures to be taken to protect themselves from identity theft.

5.5.3 One or more members of the Incident Response Team must be technically qualified to respond to information-related incidents. If necessary, additional technical support may be sought from outside the campus community.

5.6 Emergency Action by the ISO and Revocation of Access

5.6.1 The ISO may discontinue access of any individual who violates this policy, or other IT policies, when continuation of such service threatens the security (including integrity, privacy and availability) of the University's IT resources.

5.6.2 The ISO may discontinue access to any network segment or networked device if the continued operation of such segments or devices threatens the security of the University's IT resources.

5.6.3 The ISO shall notify the supervisor, or the appropriate data steward or his or her designee, to assist in the resolution of non-compliance issues before access is discontinued, unless non-compliance is causing a direct and imminent threat to the University's IT resources.

5.6.4 The data steward may discontinue service, or request that the ISO discontinue service, to network segments, network devices, or individuals under his or her jurisdiction, which are not in compliance with this policy. Data stewards shall notify, or request that the ISO notify, affected individuals to assist in the resolution of non-compliance issues before service(s) are discontinued, unless non-compliance is causing a direct and imminent threat to the University's IT resources.

5.6.5 An individual’s access may be restored as soon as the direct and imminent security threat has been remedied and permission has been granted by the appropriate data steward or vice president (in case there is no data steward), unless access is revoked.

5.6.6 The University reserves the right to revoke access to any IT resource for any individual who violates the University's policy, or for any other business reasons, in conformance with applicable university policies. Staff members may appeal to their respective vice president regarding revocation of access.

5.6.7 Violation of the University's policy may result in disciplinary action, up to and including termination of employment. Employees may appeal disciplinary actions taken against them pursuant to university policy and in a manner affording due process to university employees.

5.7 Regular Review of Security Procedures

5.7.1 These procedures shall be reviewed at regular intervals using best practices designated by the campus ISO.

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity