R345, Information Technology Resource Security[1]

R345-1. Purpose: To provide policy to secure the private sensitive information of faculty, staff, patients, students, and others affiliated with USHE institutions, and to prevent the loss of information that is critical to the operation of the institutions and USHE. USHE Information Technology Resources are at risk from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action. Specific institutional policies may be more restrictive depending on the security requirements of the institution.

R345-2. References

2.1. Policy and Procedures R132, Government Records Act and Management Act Guidelines

2.2. Policy and Procedures R341, Computing Systems Programs

2.3. Policy and Procedures R343, Information Management

R345-3. Definitions

3.1. Information Technology Resource (IT Resource): A resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

3.2. Server: A computer used to provide information and/or services to multiple Users.

3.3. Security: Measures taken to reduce the risk of (a) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and/or (b) damage to or loss of IT Resources through any type of disaster, including cases where a violation of security or a disaster occurs despite preventative measures.

3.4. IT Resource Steward: The individual who has policy level responsibility for determining what IT Resources will be stored, who will have access, what security and privacy risk is acceptable, and what measures will be taken to prevent the loss of Information Resources.

3.5. IT Resource Custodian: The organization or individual who implements the policy defined by the IT Resource Steward and has responsibility for IT systems that store, process or transmit IT resources.

3.6. IT Resource Administrator: Institutional staff that, under the direction of the IT Resource Steward and with operational instructions from the IT Resource Custodian, have day-to-day operational responsibility for data capture, maintenance and dissemination.

[1] Approved March 21, 2008.

3.7. User: Any person, including faculty members, staff members, students, patients and anyone else such as contractors, consultants, interns, and temporary employees, who accesses and uses institutional IT Resources.

3.8. Private Sensitive Information: Private information retained by or accessible through IT Resources such as networks and/or computers, including any information that identifies or describes an individual (Information Owner), including but not limited to, his or her name, Social Security number, medical history, and financial matters. 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.

3.8.1. Private Sensitive Information does not include "public information" as defined by the Utah Government Records Access and Management Act (GRAMA), or in the case of student records, "directory information" as defined by the Family Education Rights and Privacy Act (FERPA).

3.9. Critical IT Resource: An IT Resource which is required for the continuing operation of the institution and/or its colleges and departments, including any IT Resource which, if it fails to function correctly and/or on schedule, could result in a major failure of mission-critical business functions, a significant loss of funds, or a significant liability or other legal exposure. For example, General Ledger monthly financial reporting may be considered non-Critical IT Resources by the institution, but financial reporting at fiscal year-end may be considered a Critical IT Resource.

3.10. Disaster: Any event or occurrence that prevents the normal operation of a Critical IT Resource(s).

3.11. Disaster Recovery Plan: A written plan including provisions for implementing and running Critical IT Resources at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster.

3.12. Unauthorized Access to IT Resources: Access to Private Sensitive Information or Critical IT Resources by a User(s) that does not need access to perform his/her job duties.

3.13. Information Security Office(s) (ISO): The Information Security Office(s) is (are) responsible for the development and maintenance of security strategy for the institution's IT Resource systems, risk assessments, compliance with ISO policies and guidelines, and for the resolution of campus IT security incidents. The institution may have ISO functions performed by one or more individuals or offices. If multiple individuals or offices are involved, their respective roles and assignments should be clearly delineated.

3.14. Incident Response Team: Directed by the 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.

3.15. Acceptable Use Policy: Defines User conduct for appropriate use of the Institution's IT Resources.

R345-4. Policy

4.1. Protecting Private Sensitive Information on Institution or Departmental IT Resources: Each institution and its colleges, departments, and divisions, must take measures to protect Private Sensitive Information that is stored, processed or transmitted using IT Resources under their control. These measures should be taken as needed and reviewed at regular intervals using best practices designated by the campus ISO.

4.1.1. Reasonable and appropriate security procedures must be designed to prevent unauthorized individuals or organizations from accessing IT Resources which store, process, or transmit Private Sensitive Information.

4.1.2. Security procedures must be designed for IT Resources that do not store, process or transmit Private Sensitive Information if access to such IT Resources provides the possibility of a breach of security.

4.2. Preventing the Loss of Critical Institution or Departmental IT Resources: At regular intervals using best practices designated by ISO, each institution and its colleges, departments, and divisions, must take measures to identify and prevent the loss of Critical IT Resources that are under their control, and to include Critical IT Resources in college, department or division Disaster Recovery Plans.

4.2.1. Reasonable and appropriate security procedures must be implemented to ensure the availability of institution or departmental Critical IT Resources.

4.3. Protecting Private Sensitive Information on Users' (Faculty, Staff, Students) IT Resources: Users of IT Resources must not knowingly retain on personal computers, servers, or other computing devices, Private Sensitive Information, such as Social Security Numbers, financial information including credit card numbers and bank information, or protected health information, including health records and medical information, except under the following conditions:

4.3.1. The User must have such Private Sensitive Information to perform duties that are necessary to conduct the business of the institution;

4.3.2. The Dean, Department Chair, or Vice President must have granted permission to the User; and

4.3.3. The User must take reasonable precautions to secure the Private Sensitive Information that resides on his/her personal computer or other computing device, e.g., implement an encryption method to protect documents that contain sensitive information.

4.3.4. Permission is not required to retain student grades, letters of recommendation, RPT documents, patentable research findings, etc., 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 User must take reasonable precautions to secure the data.

4.4. Preventing the Loss of Critical IT Resources on Users' (Faculty, Staff, Students) IT Resources: A User must take reasonable precautions to reduce the risk of loss of Critical IT Resources that reside on his/her personal computer or other computing device, i.e., at regular intervals backup critical documents on CDs or other media, or back up documents to a storage device or system which is administered by the User's IT Systems Administrator.

4.5. Identification of Private Sensitive Information and Critical IT Resources: If uncertain whether or not an IT Resource contains Private Sensitive Information or is a Critical IT Resource, a User must seek direction from the IT Resource Steward, the IT Resource Custodian, the campus HIPAA Privacy Office, or the institution's Information Security Officer.

4.6. Reporting of Security Breaches: All suspected or actual security breaches of institutional or departmental systems must immediately be reported to the institution's Information Security Officer. IT

Systems Administrators should report security incidents to the IT Resource Steward and IT Resource Custodian for their respective organization. If the compromised system contains personal or financial information (e.g. credit card information, social security, etc.), the organization must report the event to the institution's legal office.

4.6.1. If Private Sensitive Information has been accessed or compromised by unauthorized persons or organizations:

4.6.1.1. The IT Resource Steward or User who is responsible for the information must consult with the vice president, dean, department head, supervisor, ISO and the legal office to assess the level of threat and/or liability posed to the institution and to those whose Private Sensitive Information was accessed.

4.6.1.2. Individuals Whose Private Sensitive Information was accessed or compromised will be notified and referred to ISO for instructions regarding measures to be taken to protect themselves from identity theft.

4.7. Reporting Loss of Critical IT Resource: If Critical IT Resources are lost, the Data Steward or User must notify those individuals and organizations that are affected by the loss of the resource.

4.8. Physical Security: Users are responsible for assuring that all electronic information, hard copy information, and hardware devices in their possession are physically protected in accordance with their classification level at all times. Users must assure that the security controls for each work area are followed and that access restrictions, sensitive data handling procedures, and the security plan for each area are adhered to.

4.9. Destruction or "Wiping" of Electronic Media: Departments and Users shall destroy private and sensitive information as well as other personal or financial information in a campus IT Resource or on personal computers, servers, or other campus computing devices, when such information is no longer needed to conduct the business of the institution, using established institutional procedures.

R345-5. Roles and Responsibilities: Each institution shall clearly define the roles and responsibilities of persons charged with the security of institutional information resources. The institution may organize the ISO office(s) as one person or multiple groups to fit its needs. Also the institution may choose to use designations other than "IT Resource Steward, IT Resource Custodian, and IT Resource Administrators" to describe the persons charged with the following roles and responsibilities.

5.1. Institutional Information Security Office(s) (ISO): The ISO reports directly to a senior institutional administrator. The ISO is responsible for the coordination, review and approval of procedures used to provide the requisite security for Private Sensitive Information or Critical IT Resources. The ISO is responsible for coordinating compliance with this policy and shall:

5.1.1. Develop and maintain security policies, plans, procedures, strategies, architectures, best practices, and minimum requirements.

5.1.2. Educate and provide assistance in complying with this policy to IT Resource Stewards, IT Resource Custodians, IT Resource Administrators, and Users. Provide guidelines consistent with institutional policies, consultation, and assistance to campus departments and individuals regarding the proper use of computer workstations, servers, applications, group networks and other IT Resources.

5.1.3. Implement and enforce baseline perimeter security practices endorsed for institutions by federal, state, and local government agencies, and national organizations such as Educause, the SANS Institute, and the National Institute of Standards and Technology.

5.1.4. Monitor and analyze campus network traffic information to ensure compliance with institutional security and acceptable use policies, and evaluate, identify, and resolve security vulnerabilities, breaches and threats to the institution's IT Resources.

5.1.5. Conduct security audits as requested by campus departments. Conduct security audits periodically to confirm compliance with this policy.

5.1.6. Direct the campus Incident Response Team, incident response activities, and incident resolution at institutional, departmental, and individual levels. Take appropriate and reasonable remedial action to resolve security incidents.

5.1.7. Assist institutional or third party auditors in the analysis of campus IT Resources to further ensure policy compliance.

5.1.8. Monitor compliance with security policies and procedures and report compliance violations to the relevant cognizant authority.

5.2. IT Resource Custodian: IT Resource Custodians (Computer Services and other IT Resources related work units or individuals) are charged with the responsibility of managing and maintaining the campus backbone network and other IT systems and resources and, as related to their security roles and responsibilities, shall:

5.2.1. Monitor the campus network traffic flows, primarily for the purpose of network maintenance and optimization.

5.2.2. Inform the Information Security Officer of traffic patterns, which pursuant to best practices, procedures and standards, may indicate a potential or actual threat to the network backbone and campus IT Resources.

5.2.3. Apply security policy and procedures to campus network devices as directed by the ISO.

5.3. Incident Response Team: Under the direction of the Information Security Officer, 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.

5.4. IT Resource Steward: The IT Resource Steward is designated by the cognizant authority of the relevant group or work unit, is familiar with data issues, laws and regulations, and shall:

5.4.1. Determine the purpose and function of the IT Resource.

5.4.2. Determine the level of security required based on the sensitivity of the IT Resource.

5.4.3. Determine the level of criticality of an IT Resource.

5.4.4. Determine accessibility rights to IT Resources.

5.4.5. Determine the appropriate method for providing business continuity for Critical IT Resources (e.g., performing Service Continuity at an alternate site, performing equivalent manual procedures, etc.).

5.4.6. Specify adequate data retention, in accordance with the institution's policies, and state and federal laws for IT Resources consisting of applications or data.

5.4.7. Monitor and analyze network traffic and system log information for the purpose of evaluating, identifying and resolving security breaches and/or threats to the IT Resources of the organization for which they have responsibility.

5.4.8. An IT Resource Steward in a work unit, which lacks the professional IT staff or expertise to accomplish items 5.4.1 through 5.4.7, or to fulfill the responsibilities of the IT Resource Administrators, may request assistance from the Information Security Officer.

5.5. IT Resource Administrator: The IT Resource Administrator(s) is responsible for the performance of security functions and procedures as directed by the IT Resource Steward, implementing and administering the security of IT Resources in accordance with institutional and industry best practices and standards.

R345-6. Sanctions and Remedies

6.1. Emergency Action by the ISO: The ISO may discontinue service to any User who violates this policy or other IT policies when continuation of such service threatens the security (including integrity, privacy and availability) of the institution's IT Resources. The ISO may discontinue service to any network segment or networked device if the continued operation of such segments or devices threatens the security of the institution's IT Resources. The ISO will notify the IT Resource Steward or his/her designee 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 institution's IT Resources.

6.2. Emergency Action by the IT Resource Steward: The IT Resource Steward may discontinue service or request that the ISO discontinue service to network segments, network devices, or Users under his or her jurisdiction, which are not in compliance with this policy. IT Resource Stewards will 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 institution's IT Resources.

6.3. Restoration of Access: A User's access may be restored as soon as the direct and imminent security threat has been remedied.

6.4. Revocation of Access: USHE institutions shall reserve the right to revoke access to any IT Resource for any User who violates the institution's policy, or for any other business reasons in conformance with applicable institutional policies.

6.5. Disciplinary Action: Violation of the institution's policy may result in disciplinary action, including termination of employment. Staff members may appeal revocation of access to IT Resources or disciplinary actions taken against them pursuant to institutional policy.