R992, Information and Technology Resource Security[1]

R992-1. Purpose: To provide policy to secure the private sensitive information of employees, borrowers, parents, program participants, and others affiliated with OCHE, and to prevent the loss of information that is critical to the operation of OCHE. OCHE Information Resources are at risk from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action. Specific work unit policies may be more restrictive depending on the security requirements of the work unit.

R992-2. References

2.1. Policy and Procedures R345, Information Technology Resource Security

2.2. Policy and Procedures R926, Use of Office-owned Computer and Software

2.3. Policy and Procedures R927, Use and Security of Property

2.4. Policy and Procedures R952, Discrimination, Harassment, and Staff Employment Grievance

2.5. Policy and Procedures R993, Records Access and Management

R992-3. 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 1) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and 2) 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 work unit 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.

[1] Adopted January 20, 2006, Amended May 30, 2008.

3.6. IT Resource Administrator: OCHE 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.

3.7. User: Any person, including members of the OCHE staff, and anyone else such as contractors, consultants, interns, and temporary employees, who accesses and uses OCHE 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, 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 OCHE, 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 OCHE, but financial reporting at fiscal year-end may be considered Critical IT Resources.

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

3.11. Service Continuity Plan: A written plan including provisions for implementing and running Critical Information Technology 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 Officer (ISO): The Information Security Officer is responsible for the development and maintenance of security strategy for OCHE's computer systems and resolution of office IT security incidents.

3.14. Information Technology Council: Made up of OCHE personnel appointed by the Commissioner, the Council is responsible for recommending OCHE security policies, approving security plans, and designating personnel for the Incident Response Team, as needed.

3.15. Incident Response Team: Directed by the ISO and made up of OCHE 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.

3.16. ISO 27002 Standard: An information security standard published by the International Organization of Standardization (ISO). The standard provides a code of practice for information security which establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

R992-4. Policy

4.1. Adoption of International Standards for Information Security Practices: The Board supports generally accepted standards for information security practices and adopts the ISO 27002 Standard to provide guidelines and general principles for information security management in OCHE.

4.2. Fundamental Principles of Information Security

4.2.1. Users are responsible for safeguarding the integrity and confidentiality of all information to which they have access.

4.2.2. Access to OCHE information is based on an OCHE business need to know. Users must preserve the confidentiality of personal data and other OCHE information, and access information only in a manner consistent with their job function, and must never attempt to circumvent the access or accounting controls in place.

4.2.3. Users must report suspected violations of this policy to their manager, IT Resource Steward, or the ISO.

4.2.4. Users shall make appropriate use of OCHE information systems as set forth in R926, Use of Office-owned Electronic Communications Systems.

4.3 Information Ownership and Classification: All information shall have an identified OCHE Information Technology (IT) Resource Steward, who is responsible for information classification and the implementation of access and protection controls, and an IT Resource Administrator. IT Resource Administrators are responsible for data capture, maintenance, and dissemination, and for protecting information within their business environments. They approve access requests for information based upon policy set by the IT Resource Steward.

4.3.1. IT Resource Stewards approve physical controls, assign classifications to their information, and are responsible for supporting IT Resource Administrators by providing for the development and maintenance of a secure technology infrastructure and the implementation of appropriate information protection controls.

4.4. Information Handling: Sensitive private and confidential information requires specific protections. This includes most client data. Unauthorized access or disclosure could result in reputation, regulatory, and/or financial harm to OCHE, its staff, and/or its clients. OCHE shall adopt minimum standards associated with the handling of sensitive information, which shall include the use of cryptographic controls, as appropriate. IT Resource Stewards may also define additional controls for their data.

4.4.1. Users 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 except if (a) the User requires such Private Sensitive Information to perform duties that are necessary to conduct the business of OCHE, (b) the cognizant associate commissioner or designee grants permission to the User, and (c) the User takes reasonable precautions to secure Private Sensitive Information that resides on a User's personal computer or other computing device, e.g., implements password protection for documents that contain sensitive information.

4.4.2. Encryption methods must be used to protect Private Sensitive Information sent over public computer networks.

4.4.3. Encryption or other strong protections must be used to protect Private Sensitive Information on mobile and other independent devices.

4.4.4. All information systems—automated and manual—used by OCHE must adhere to levels of security consistent with the sensitivity of the information as classified by the IT Resource Steward. In the absence of a specific classification, information should be treated as confidential.

4.5. Release of Information: A nondisclosure agreement must be signed by a third party before OCHE Private Sensitive Information is released. The Information Owner must approve the release of Private Sensitive Information to a third-party or for internal use, unless such release is authorized by law.

4.6. User Authentication: Users are responsible for the confidentiality and selection of passwords to ensure that unauthorized use of their OCHE user accounts does not occur.

4.6.1. Individual user-IDs and passwords should never be shared. No one—administrators, managers, or fellow users—should ever request another person's password.

4.6.2. Passwords should not be written down.

4.6.3. Passwords used on OCHE systems should not be used on non-OCHE systems.

4.6.4. Passwords should be changed regularly, even for applications that do not systematically require the change.

4.7. Electronic Mail: Users are responsible for applying the necessary security controls when sending e-mail, for the proper handling of incoming e-mails, and for appropriate e-mail account management. Users are prohibited from granting access to their e-mails accounts unless there is a legitimate business need and management approval. The automatic forwarding of e-mail to non-OCHE addresses is prohibited. Users are responsible for managing their e-mail accounts, including archiving or saving messages and storage size, encrypting sensitive information that is sent inside or outside of OCHE.

4.7.1. Unsolicited e-mail (spam) and offensive external messages are to be deleted. Users should not respond to unsolicited e-mails, even to request being taken off the mailing list.

4.7.2. Users may be permitted limited personal use of e-mail and the Internet, in accordance with R926. OCHE restricts access to some Internet sites considered inappropriate for the workplace.

4.8. Wireless and Remote Access: Wireless and remote access users shall protect OCHE information and assets while accessing the OCHE network; are responsible for adhering to all OCHE policies while accessing the system; may not connect to multiple networks at the same time without prior IT Resource Steward approval; may not download OCHE Private Sensitive Information to non-OCHE equipment, including home computers, personal storage devices, and PDAs; must protect authentication devices separately from hardware devices; and access the OCHE network only through approved channels.

4.8.1. Private Sensitive Information that leaves OCHE, whether in electronic or hard copy form, shall be protected from unauthorized disclosure. All portable systems storing OCHE Private Sensitive Information shall be password protected and employ hard disk encryption or other approved protection systems.

4.9. Hardware and Software: Users are responsible for assuring the integrity and configuration of the hardware and software they use. OCHE maintains virus protection on servers and workstations to prevent and detect viruses. If a virus is suspected, Users should call Computer Services immediately. Users may not:

4.9.1. Install, reconfigure or remove any hardware or software from OCHE owned equipment.

4.9.2. Download programs or executable type files from the Internet without prior approval of Computer Services.

4.9.3. Connect non-OCHE equipment directly to the OCHE network. (Staff members responsible for contractors must ensure that contractors use OCHE provided hardware/software and get approval from Computer Services for nonstandard software that is to be connected to the OCHE network).

4.9.4. Store personal data files anywhere in the OCHE system, except on his/her workstation, separate from OCHE data, in accordance with R926.

4.10. 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. Users shall follow physical security practices:

4.10.1. Private Sensitive Information—whether in paper reports, floppy disks, CDs, flash drives, etc.—must be kept in locked drawers, filing cabinets, or other secure places when not in use or when the work area is unattended.

4.10.2. Users may not remove Private Sensitive Information from OCHE premises without the cognizant IT Resource Steward's approval.

4.10.3. Users assigned to offices with locks should lock their doors at the end of the workday.

4.10.4. PC workstations should be locked when the User is not at his or her desk.

4.10.5. Information should not be left on printers, copy or fax machines, etc. for extended periods of time. Information should not be left on white boards, flip charts or in conference rooms. Information found in inappropriate areas should be returned to the owner, if known, or removed and stored until such time as the owner is found or identified.

4.10.6. No staff member, contractor, or visitor should compromise or evade physical restriction of access to the OCHE building or work areas.

4.11. Workstation Inspections: All Users' workstations are subject to inspection to verify that they are secured properly. Inspections will be conducted during and after regular business hours in order to verify that workstations are logged off the local area network (LAN) and that all Private Sensitive Information is properly secured.

4.12. Security Incident Reporting: All suspected or actual security breaches of OCHE systems must immediately be reported to the OCHE Information Security Office. IT Resource Administrators should report

security incidents to the IT Resource Steward and the IT Resource Custodian for their respective organization.

4.12.1. If Private Sensitive Information has been accessed or compromised by unauthorized persons or organizations, the IT Resource Steward, IT Resource Custodian or IT Resource Administrator who is responsible for the information must consult with the ISO and the cognizant associate commissioner to assess the level of threat and/or liability posed to OCHE and to those whose Private Sensitive Information was accessed. Based on an assessment of the risk, OCHE may decide to notify individuals whose Private Sensitive Information was accessed or compromised and provide information regarding measures to be taken to protect themselves from identity theft.

4.13. Destruction or "Wiping" of Electronic Media: Work units and Users shall destroy private and sensitive information obtained from credit bureaus and other information providers, as well as other personal or financial information in an OCHE IT Resource or on personal computers, servers, or other office computing devices, when such information is no longer needed to conduct the business of OCHE, using established OCHE procedures.

R992-5. Roles and Responsibilities

5.1. OCHE Information Security Officer (ISO): The ISO reports directly to the Associate Commissioner for Finance and Facilities. The ISO is responsible for the coordination, review and approval of procedures used to provide the requisite security for Private Sensitive Information or Critical Information Technology 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 OCHE policies, consultation, and assistance to work units and individuals regarding the proper use of computer workstations, servers, applications, group networks and other information technology 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 office network traffic information to ensure compliance with OCHE security and acceptable use policies, and evaluate, identify, and resolve security vulnerabilities, breaches and threats to OCHE IT Resources.

5.1.5. Conduct security audits as requested by work units. Conduct security audits periodically to confirm compliance with this policy.

5.1.6. Direct the office Incident Response Team, incident response activities, and incident resolution at OCHE, work unit, and individual levels. Take appropriate and reasonable remedial action to resolve security incidents.

5.1.7. Assist OCHE or third party auditors in the analysis of work unit 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 office backbone network and other IT systems and resources and, as related to their security roles and responsibilities, shall:

5.2.1. Monitor the office 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 OCHE IT Resources.

5.2.3. Apply security policy and procedures to office 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 OCHE 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 OCHE 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 OCHE and industry best practices and standards.

R992-6. 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 OCHE 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 OCHE 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 OCHE 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 OCHE 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: OCHE reserves the right to revoke access to any Information Technology Resource for any User who violates this policy, or for any other business reasons in conformance with applicable OCHE policies.

6.5. Disciplinary Action: Violation of the 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 policy R952.