

November 7, 2018

MEMORANDUM

TO: State Board of Regents

FROM: David L. Buhler

SUBJECT: USHE – Revisions of Policy R345, *Information Technology Resource Security*

Issue

The Board is being asked to review and approve revisions to Regent Policy R345, *Information Technology Resource Security*.

Background

Regent Policy R345, *Information Technology Resource Security* provides minimum security standards for protecting USHE institutions' Personally Identifiable Information (PII) from potential threats. These threats are constantly evolving which requires that we update this policy when necessary. The Chief Information Security Officers, USHE CIOs and Institutional Legal Counsels would like to strengthen the IT security policy, particularly the rules on computer encryption and permissions to have PII retained on personal computing devices.

As originally written, IT security policies suggested best practice, standards and rules almost as if it were optional. This was done because the threat vector was not as high, and users were still learning why IT security was increasingly important. That has now changed. The current policy states in paragraph R345-4: Each institution "should" adopt the policy measures "as needed." In the current threat environment, this needs to be strengthened to state each institution "will" adopt the policy measures (and eliminate "as needed").

Paragraph 4.1.4 in the policy needs to be strengthened by including the phrase "on all institutionally-owned computing devices" after the phrase "Institutions shall implement."

The heading on Paragraph 4.3 which provides the rules for retaining personal information on private computers needs to be changed to "Protecting PII."

To further strengthen the policy, we recommend that all the conditions 4.3.1- 4.3.5 need to be met before any consideration is given to have PII on a private computer. The final phrase in the final sentence in paragraph 4.3 will read "except when all of the following conditions are met" instead of "except under the following conditions."

Commissioner's Recommendation

The Commissioner recommends the Regents review and approve the proposed changes to Regents Policy R345, effective immediately.

David L. Buhler
Commissioner of Higher Education

DLB/KLH/SH
Attachments

R345, Information Technology Resource Security

R345, Information Technology Resource Security

R345-1.Purpose: To provide minimum security standards for protecting USHE institutions' Personally Identifiable Information 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 Access 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. Acceptable Use Policy: Defines User conduct for appropriate use of the Institution's IT Resources.

3.2. Administrative Access: Any account or other access mechanism that permits a Data Steward, Data Custodian, IT Resource administrator, or User to control an IT resource and/or grants functional access to multiple records of Confidential Data.

3.3. 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.

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

3.5. 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.

3.6. Information Security Office(s) (ISO): The Information Security Office develops and maintains security strategies 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.

3.7. Incident Response Team: A team composed of appropriate campus personnel, including an ISO representative; 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 preventive measures that develop as a result of responding to and resolving security breaches.

3.8. 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, Internet-based storage, mobile devices, removable storage, 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.

3.9. 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.

3.10. 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.

3.11. 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.

3.12. Personally Identifiable Information: Personally Identifiable Information (PII) is protected by federal and state laws and regulations, including federal regulations administered by the U.S. the Department of Homeland Security (DHS), and is defined by DHS as “any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.” PII must be protected prior to release in accordance with the Utah Government Records Access Management Act (GRAMA) or other disclosures required by law. PII includes but is not limited to the following:

3.12.1 Full Social Security Number (SSN)

3.12.2 Driver’s license or State ID number

3.12.3 Passport number

3.12.4 Visa number

3.12.5 Alien Registration Number

3.12.6 Fingerprints or other biometric identifiers

3.12.7 Full name in combination with:

3.12.7.1 Mother’s maiden name

3.12.7.2 Date of birth, last 4 digits of SSN

3.12.7.3 Citizenship or immigration status

3.12.7.4 Ethnic or religious affiliation

3.12.8 Protected Health Information, as defined by the Health Insurance Portability and Accountability Act (HIPAA)

3.13. Personally Identifiable 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).

3.14. 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 preventive measures.

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

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

3.17. 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.

R345-4. Policy: Each institution and its colleges, departments, and divisions, shall take measures to protect Personally Identifiable Information that is stored, processed or transmitted using IT Resources under their control. Institutions will adopt these measures and review their security methods with the ISO at regular intervals to ensure they are using best practices.

4.1. Institutions shall design reasonable and appropriate security procedures to prevent unauthorized individuals or organizations from accessing IT Resources which store, process, or transmit Personally Identifiable Information.

4.1.1. Institutions shall design security procedures for IT Resources that do not store, process or transmit Personally Identifiable Information if access to such IT Resources provides a possible vector or avenue to a breach of security of Personally Identifiable Information or critical IT resource.

4.1.2. Institutions and departments shall maintain appropriate controls for administrative or functional access to IT resources containing Personally Identifiable Information and shall regularly audit administrative accounts to ensure only currently valid users and administrators have access.

4.1.3 Institutions shall implement multi-factor authentication for all administrative and functional access to IT resources that store, process or transmit Personally Identifiable Information.

4.1.4 Institutions shall implement on all institutionally-owned computing devices industry-standard encryption that renders the storage media of the device reasonably unrecoverable by a third-party, or other reasonable controls, on any mobile computing or removable storage device that processes, stores, or transmits Personally Identifiable Information.

4.1.5 Institutions and departments that entrust Personally Identifiable Information to third-parties (e.g. hosted and/or “cloud” IT Resources) shall review contracts and/or terms of service to ensure the third-party will implement reasonable protections for Personally Identifiable Information in all stages of its lifecycle, including creation, storage, processing, transmittal and destruction.

4.1.6 Institutions shall maintain an inventory of all internal or third-party IT Resources that store, process or transmit Personally Identifiable Information.

4.2. Preventing the Loss of Critical Institution or Departmental IT Resources: At regular intervals using best practices designated by ISO, each institution shall 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.

4.3. Protecting PII: 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 when all of the following conditions are met:

4.3.1. The User needs Personally Identifiable Information to perform duties that are necessary to conduct the business of the institution;

4.3.2. The appropriate dean, department chair, or vice president must have granted permission to the User

4.3.3. The institutions have installed industry-standard encryption that renders the storage media of the device reasonably unrecoverable by a third-party, or other reasonable controls, on the user's mobile computing or removable storage device that processes, stores, or transmits Personally Identifiable Information; and

4.3.4. The User must take reasonable precautions to secure the Personally Identifiable Information that resides on his/her personal computer or other computing device.

4.3.5 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 back up 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 or otherwise approved by the campus for such use.

4.5. Identification of Personally Identifiable Information and Critical IT Resources: If uncertain whether or not an IT Resource contains Personally Identifiable Information or is a Critical IT Resource, a User shall seek direction from the IT Resource Steward, the IT Resource Custodian, the campus Health Insurance Portability and Accountability Act (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 Numbers, etc.), the organization must report the event to the institution's legal office.

4.6.1. If an unauthorized person or organization has been accessed or compromised personally identifiable information:

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 Personally Identifiable Information was accessed.

4.6.1.2. The Institution shall notify and direct individuals whose Personally Identifiable Information was accessed or compromised to ISO for instructions regarding measures they should take 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. Insurance against Data Loss or Breach: Institutions shall maintain an insurance policy covering loss or breach of Personally Identifiable Information.

4.9. 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 shall follow at all times the security controls for each work area and that they comply with access restrictions, sensitive data handling procedures, and the security plan for each area.

4.10 Destruction or “Wiping” of Electronic Media: Departments and Users shall destroy Personally Identifiable 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 Personally Identifiable 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 ongoing, periodic 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) 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 how critical the 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 that 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

5.5. IT Resource Administrator: The IT Resource Administrator(s) performs 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 as allowed by applicable institutional

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.

R345, Information Technology Resource Security

R345, Information Technology Resource Security

R345-1.Purpose: To provide minimum security standards for protecting USHE institutions' Personally Identifiable Information 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 Access 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. Acceptable Use Policy: Defines User conduct for appropriate use of the Institution's IT Resources.

3.2. Administrative Access: Any account or other access mechanism that permits a Data Steward, Data Custodian, IT Resource administrator, or User to control an IT resource and/or grants functional access to multiple records of Confidential Data.

3.3. 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.

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

3.5. 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.

3.6. Information Security Office(s) (ISO): The Information Security Office develops and maintains security strategies 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.

3.7. Incident Response Team: A team composed of appropriate campus personnel, including an ISO representative; 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 preventive measures that develop as a result of responding to and resolving security breaches.

3.8. 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, Internet-based storage, mobile devices, removable storage, 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.

3.9. 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.

3.10. 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.

3.11. 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.

3.12. Personally Identifiable Information: Personally Identifiable Information (PII) is protected by federal and state laws and regulations, including federal regulations administered by the U.S. the Department of Homeland Security (DHS), and is defined by DHS as “any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.” PII must be protected prior to release in accordance with the Utah Government Records Access Management Act (GRAMA) or other disclosures required by law. PII includes but is not limited to the following:

3.12.1 Full Social Security Number (SSN)

3.12.2 Driver’s license or State ID number

3.12.3 Passport number

3.12.4 Visa number

3.12.5 Alien Registration Number

3.12.6 Fingerprints or other biometric identifiers

3.12.7 Full name in combination with:

3.12.7.1 Mother’s maiden name

3.12.7.2 Date of birth, last 4 digits of SSN

3.12.7.3 Citizenship or immigration status

3.12.7.4 Ethnic or religious affiliation

3.12.8 Protected Health Information, as defined by the Health Insurance Portability and Accountability Act (HIPAA)

3.13. Personally Identifiable 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).

3.14. 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 preventive measures.

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

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

3.17. 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.

R345-4. Policy: Each institution and its colleges, departments, and divisions, shall take measures to protect Personally Identifiable Information that is stored, processed or transmitted using IT Resources under their control. Institutions ~~should~~will adopt these measures ~~as needed~~ and review their security methods with the ISO at regular intervals to ensure they are using best practices.

4.1. Institutions shall design reasonable and appropriate security procedures to prevent unauthorized individuals or organizations from accessing IT Resources which store, process, or transmit Personally Identifiable Information.

4.1.1. Institutions shall design security procedures for IT Resources that do not store, process or transmit Personally Identifiable Information if access to such IT Resources provides a possible vector or avenue to a breach of security of Personally Identifiable Information or critical IT resource.

4.1.2. Institutions and departments shall maintain appropriate controls for administrative or functional access to IT resources containing Personally Identifiable Information and shall regularly audit administrative accounts to ensure only currently valid users and administrators have access.

4.1.3 Institutions shall implement multi-factor authentication for all administrative and functional access to IT resources that store, process or transmit Personally Identifiable Information.

4.1.4 Institutions shall implement on all institutionally-owned computing devices industry-standard encryption that renders the storage media of the device reasonably unrecoverable by a third-party, or other reasonable controls, on any mobile computing or removable storage device that processes, stores, or transmits Personally Identifiable Information.

4.1.5 Institutions and departments that entrust Personally Identifiable Information to third-parties (e.g. hosted and/or “cloud” IT Resources) shall review contracts and/or terms of service to ensure the third-party will implement reasonable protections for Personally Identifiable Information in all stages of its lifecycle, including creation, storage, processing, transmittal and destruction.

4.1.6 Institutions shall maintain an inventory of all internal or third-party IT Resources that store, process or transmit Personally Identifiable Information.

4.2. Preventing the Loss of Critical Institution or Departmental IT Resources: At regular intervals using best practices designated by ISO, each institution shall 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.

4.3. Protecting ~~Private Sensitive Information on Users' (Faculty, Staff, Students) IT Resources~~: PII:

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~~when all of the following conditions are met:

4.3.1. The User needs Personally Identifiable Information to perform duties that are necessary to conduct the business of the institution;

4.3.2. The appropriate dean, department chair, or vice president must have granted permission to the User

4.3.3. The institutions have installed industry-standard encryption that renders the storage media of the device reasonably unrecoverable by a third-party, or other reasonable controls, on the user's mobile computing or removable storage device that processes, stores, or transmits Personally Identifiable Information; and

4.3.4. The User must take reasonable precautions to secure the Personally Identifiable Information that resides on his/her personal computer or other computing device.

4.3.5 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 back up 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 or otherwise approved by the campus for such use.

4.5. Identification of Personally Identifiable Information and Critical IT Resources: If uncertain whether or not an IT Resource contains Personally Identifiable Information or is a Critical IT Resource, a User shall seek direction from the IT Resource Steward, the IT Resource Custodian, the campus Health Insurance Portability and Accountability Act (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 Numbers, etc.), the organization must report the event to the institution's legal office.

4.6.1. If an unauthorized person or organization has been accessed or compromised personally identifiable information:

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 Personally Identifiable Information was accessed.

4.6.1.2. The Institution shall notify and direct individuals whose Personally Identifiable Information was accessed or compromised to ISO for instructions regarding measures they should take 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. Insurance against Data Loss or Breach: Institutions shall maintain an insurance policy covering loss or breach of Personally Identifiable Information.

4.9. 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 shall follow at all times the security controls for each work area and that they comply with access restrictions, sensitive data handling procedures, and the security plan for each area.

4.10 Destruction or “Wiping” of Electronic Media: Departments and Users shall destroy Personally Identifiable 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 Personally Identifiable 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 ongoing, periodic 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) 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 how critical the 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 that 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

5.5. IT Resource Administrator: The IT Resource Administrator(s) performs 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 as allowed by applicable institutional

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.

[1] Approved March 21, 2008, and revised on September 16, 2016.