SOUTHERN UTAH UNIVERSITY
Policies and Procedures

Policy # 5.57
Date Approved: 10/21/11
Date Amended:
Reviewed w/no Changes:
Office of Responsibility: CIO
Page 1 of 18

SUBJECT: INFORMATION TECHNOLOGY RESOURCE SECURITY

I. PURPOSE

University Information Technology (IT) 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:

1. Secure the private sensitive information of faculty, staff, students, and others affiliated with the University
2. Prevent the loss of information that is critical to the operation of the University.
3. Maintain the confidentiality, integrity, and availability of all systems supporting the mission and functions of Southern Utah University.
4. Ensure compliance with all applicable federal, state, and local laws, regulations and statutes, as well as contractual obligations.
5. Ensure the protection of Southern Utah University's IT resources from unauthorized access or damage.

II. REFERENCES

A. SUU Policy and Procedures, 5.51, Information Technology Resources
B. SUU Policy and Procedures, 5.39, Records Access and Management
C. SUU Policy and Procedures, 5.46, Student Responsibilities and Rights
D. SUU Policy and Procedures, 5.8, Computer Software Licensing
E. SUU Policy and Procedures, 5.58, University E-mail
F. SUU Policy and Procedures, 6.22, Faculty Due Process
G. SUU Policy and Procedures, 8.3.5, Termination of Non-Academic Staff Employees and Disciplinary Sanctions
H. SUU Policy and Procedures, 11.2, Student Rights, Responsibilities and Conduct
I. Acknowledgements: University of Utah Information Technology Resource Security Policy (Policy 4-004) and University of Utah Information Security Policy
J. Acknowledgements: USHE Information Technology Resource Security Policy (Policy R345)

III. DEFINITIONS

A. Account: A login ID in combination with a password or other authentication token used to access any of Southern Utah University's IT resources.

B. Assessed Level of Risk: Risk as assessed by the Information Security Office (ISO) or by using a methodology approved by that office (including self-assessments).

C. Availability: Ability of an IT service to perform its agreed function when required.

D. Chief Information Officer (CIO): The Chief Information Officer is responsible for Southern Utah University's IT planning, budgeting, and performance including its information security components. The Associate Vice President for Information Technology is the CIO.

E. Confidential: Any data which is classified as "restricted" or "sensitive" per the data classification model as outlined in Section V.A.

F. Confidentiality: A security principle that requires that data should only be accessed by authorized people.

G. Critical Information Technology (IT) Resource: An IT Resource which is required for the continuing operation of the University 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.

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

I. Disaster Recovery 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.

J. Incident Response Team: Directed by the Information Security Office (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.

K. Information Security Office (ISO): The Information Security Office is responsible for the development and maintenance of security strategy for Southern Utah University's information technology resources and resolution of campus IT security incidents. The Director of IT Security heads the ISO.

L. Information Technology Resource (IT Resource): A resource used for electronic storage, processing or transmitting of data, as well as the data itself. Resources as defined in SUU Policy 5.51, Information Technology Resources.

M. Information Technology Resource Media: Physical media that contains Southern Utah University's data. This definition includes but is not limited to hard drives, backup tapes, CD-ROM, DVD-ROM, Blu-Ray disc, USB drives, recorded magnetic media, photographs, digitized information or microfilm.

N. Integrity: A security principle that ensures data is only modified by authorized personnel and activities. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention.

O. 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.

P. 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.

Q. IT Systems Administrator: University staff that, under the direction of the IT Resource Custodian, have day-to-day operational responsibility for data capture, maintenance and dissemination.

R. Private Sensitive Information: Private information retained by or accessible through IT Resources, including any information that identifies or describes an individual, 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.

   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).

S. 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 preventive measures.

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

U. Southern Utah University: All colleges, divisions, departments, members of the University community, and all students, staff, faculty, temporary employees.

V. System: A functionally related group of software, hardware, and IT resources.

W. Unauthorized Access: Access to any IT resource, user area, controlled physical area, or other private repository, without the permission of the appropriate steward/owner.

X. User: Any person, including faculty, staff, students, temporary employees, contractors, vendors, automated processes (acting as a user), and third party agents, who accesses any Southern Utah University IT Resources.

IV. APPLICABILITY

Compliance with this policy, and all its related rules and procedures, is required for all Southern Utah University colleges, schools, divisions, departments, members of the University community, and all students, staff, faculty, temporary employees, contractors, vendors, and third party agents.

V. POLICY

A. Data Management

1. Southern Utah University shall take measures to protect confidential information that is stored, processed or transmitted using IT resources. These measures shall be implemented commensurate with the assessed level of risk and reviewed at regular intervals.

a. Data Classification – All electronic data shall be classified in accordance with the following requirements:

1. PUBLIC DATA is information that may or must be open to the general public. It is defined as information with no

existing local, national, or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community. By way of illustration only, some examples of public data include:

a. Campus maps
b. Campus events
c. Course descriptions

2. SENSITIVE DATA is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection. Sensitive data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data. By way of illustration only, some examples of sensitive data include:

   a. Internal memos and email, and non-public reports, budgets, plans, and financial information.
   b. Library transactions.
   c. Information covered by non-disclosure agreements.
   d. Donor contact information and non-public gift amounts.

3. RESTRICTED DATA is information protected by statutes, regulations, University policies, or contractual language. Restricted data may be disclosed to individuals on a need-to-know basis only. By way of illustration only, some examples of restricted data include:

   a. Credit card information
   b. Protected Health Information (PHI)
   c. Social security number (SSN)
   d. Student and prospective student information
   e. Export controlled information under U.S. laws

b. Departments should carefully evaluate the appropriate data classification category for their information.

c. Data Handling – All electronic data shall have appropriate handling procedures in accordance with its classification and commensurate with the assessed level of risk.

B. Access Management

1. Only authorized users shall have physical, electronic, or other access to Southern Utah University's IT resources. Access shall be limited to users with a business need-to-know, and limited only to the requirements of their job function. It is the shared responsibility of IT resource administrators and users to prevent unauthorized access to Southern Utah University's systems. Access controls for IT resources shall include effective procedures for granting authorization, tools and practices to authenticate authorized users, and prevention and detection of unauthorized use. IT Systems Administrators and managers are primarily responsible for establishing, documenting, implementing, and managing access control procedures for their IT resources.

a. Account Authorization – Southern Utah University accounts shall be created according to Identity Management (IDM) procedures.

b. Account Authentication – Southern Utah University accounts shall be authenticated at a minimum via unique login ids and passwords.

c. Account Termination – Southern Utah University accounts shall be disabled and/or deleted according to Identity Management (IDM) procedures.

d. Account Reaccreditation – Southern Utah University shall conduct periodic reviews of authorized access commensurate with the assessed level of risk.

C. Change Management

1. Units responsible for information resources will ensure that changes that impact Users and other IT System Administrators will be communicated, and follow approved change management procedures.

D. IT Resource Security

1. Southern Utah University shall protect IT Resources commensurate with the assessed level of risk and utilize security baseline settings to ensure that IT resources are available for use and free from malware. IT System Administrators and users managing IT resources shall:

    a. Protect any IT resource under their management from compromise. This includes installing antivirus and relevant security patches to address security issues.

    b. Implement procedures that lock the User's workstation after a predetermined time of inactivity.

    c. Configure the IT resources to reduce vulnerabilities to a minimum.

    d. Periodically verify audit and activity logs, examine performance data, and generally check for any evidence of unauthorized access, the presence of viruses or other malicious code.

    e. Cooperate with the ISO by providing support for and/or review of administrative activities as well as allowing the performance of more sophisticated procedures such as penetration testing and real-time intrusion detection.

2. Southern Utah University shall physically protect IT Resources commensurate with the assessed level of risk. Users and IT System Administrators shall ensure that controls are planned and implemented for safeguarding physical components against compromise and environmental hazards. Locks, cameras, alarms, redundant power systems, fire detection and suppression systems, and other safeguards as appropriate shall be installed in data centers and technology closets to discourage and respond to unauthorized access to electronic or physical components contained in these areas.

E. Mobile/Remote Access

1. Users who create, access, transmit, or receive Southern Utah University information are responsible for protecting that information in a manner commensurate with risk (i.e., the data's sensitivity, value, and criticality). Appropriate procedures regarding confidentiality and privacy of information should be followed at all times regardless of location on or off-campus.

2. Users who work remotely shall ensure that their remote device (workstation, mobile phone, tablet, etc.) meets the same information security standards as the user's on-site connection (i.e., physical security, antivirus, operating system updates, etc.), as defined by best practices established by the ISO.

3. In addition, any User accessing Southern Utah University IT Resources from a mobile device (netbook, tablet, cell phone, etc.) must follow best practices designated by the ISO for mobile device security and ensure that the device can meet any technological requirements defined in the best practices. By way of illustration only, some device requirements may include:

   a. Passcode lock
   b. Remote wiping capability

F. Vendors and Business Services Agreement

1. Southern Utah University may permit a vendor, or other third party, to create, receive, maintain, or transmit confidential University information when satisfactory assurances are obtained that the vendor will appropriately safeguard the information.

G. Network Security

1. Access to both internal and external networked services shall be controlled, restricted, and protected by IT resource administrators, commensurate with the assessed level of risk. Southern Utah University user and/or IT resource access to networks and network services shall not compromise the security of the network services by ensuring:

   a. Appropriate controls are in place between Southern Utah University's network and networks owned by other organizations, and public networks.

   b. Appropriate authentication mechanisms are applied for users and IT resources.

   c. Control of user and IT resource access to information services is enforced.

H. Log Management and Monitoring

1. IT System Administrators shall configure IT Resources to record and monitor information security incidents, events, and weaknesses. IT resource administrators and the ISO shall regularly review and analyze these logs for indications of inappropriate or unusual activity.

I. Backup and Recovery

1. IT resource administrators shall conduct backups of user-level, application-level, and system-level information commensurate with the assessed level of risk and protect backup information at the storage location. Routine procedures shall be established for taking backup copies of data and testing their timely restoration and recoverability.

2. Measures to protect backup media shall be commensurate with the importance and sensitivity of the data.

3. Measures may include physically secured, encrypted, off-site copies (See Data Management - Data Handling).

J. IT Resource Media Handling

1. Southern Utah University's IT resource media shall be controlled and physically protected by users, commensurate with the assessed level of risk to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. Appropriate operating procedures shall be established to protect documents, IT resource media, input/output data, and system documentation from unauthorized disclosure, modification, removal, and destruction.

   a. IT Resource Media Access - Southern Utah University shall restrict access to IT resource media to authorized individuals.

   b. IT Resource Media Storage - Southern Utah University shall physically control and securely store IT resource media on-site within controlled areas where appropriate, and ensures any authorized off-site storage is, at minimum, secured at the same level as the on-site area.

   c. IT Resource Media Transport - Southern Utah University shall label IT resource media prior to transport, protect and control IT resource media during transport outside of controlled areas, and restrict the activities associated with transport of such media to authorized personnel.

d. IT Resource Media Sanitization and Disposal - Southern Utah University shall appropriately sanitize or destroy IT resource media prior to disposal or release for reuse.

K. Business Continuity and Disaster Recovery Planning

1. Southern Utah University shall develop and periodically review, test, and update a formal, documented contingency plan based on a business impact analysis that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Southern Utah University entities, escalation procedures, as well as develop and periodically review, test, and update formal, documented procedures to facilitate the implementation of the contingency plan.

2. Where appropriate, Southern Utah University must develop contingency plans that allow physical access to facilities in order to recover data and resume operations in the event of an emergency or disaster. For example, if card access to the data center were to fail.

3. As needed, establish (and implement as necessary) procedures to enable continuation of critical business processes for protection of the security of information while operating in emergency mode

L. Information Security Incident Management

1. Southern Utah University shall develop and periodically review, test, and update a formal, documented incident response plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Southern Utah University entities, escalation procedures, as well as develop and periodically review and update a formal, documented procedure to facilitate the implementation of the incident response plan.

2. Southern Utah University may discontinue service as outlined in section VI (Sanctions and Remedies) of this policy.

M. Information Security Awareness Training

1. Southern Utah University's faculty, staff, temporary employees, and, where appropriate, contractors and third party users shall receive information security awareness training and regular updates as mandated for their role at the University.

N. Protecting Private Sensitive Information

1. University colleges, schools, 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 ISO.

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.

3. 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 all of the following conditions:

   a. The User requires such Private Sensitive Information to perform duties that are necessary to conduct the business of the University.

   b. The Dean, Department Chair, or Vice President grants permission to the User.

   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., implement password protection and encryption for documents that contain sensitive information.

O. Preventing the Loss of Critical IT Resources

1. University units must take measures to identify and prevent the loss of Critical IT Resources that are under their control, according to best

practice designated by the ISO, and to include Critical IT Resources in a Disaster Recovery Plan.

2. Reasonable and appropriate security procedures must be implemented to ensure the availability of Critical IT Resources.

3. A User must take reasonable precautions to reduce the risk of loss of Critical IT Resources that reside on a User's personal computer or other computing device, i.e., backup critical documents on CDs or other media, or back up documents to a storage device or system, at regular intervals, which is administered by the User's IT Systems Administrator.

P. 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, or the University ISO.

Q. Reporting of Security Breaches

1. All suspected or actual security breaches of University, college, or departmental systems must immediately be reported to the ISO. 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 University's Office of General Counsel.

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

   a. 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 Office of General Counsel to assess the level of threat and/or liability posed to the University and to those whose Private Sensitive Information was accessed.

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

R. Reporting Loss of IT Resource

1. If IT Resources are lost, the User must notify the ISO who will determine the appropriate course of action.

S. Risk Assessment

1. Southern Utah University must regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of their IT Resources utilizing a methodology approved by the ISO. The ISO will provide guidance or assistance for the risk assessment process as necessary.

2. In addition to regular risk assessments, The University must conduct a risk analysis, in consultation with the ISO, when environmental or operational changes or additions occur (new services, systems, etc.) which significantly impact the confidentiality, integrity, or availability of information systems containing confidential information.

T. Roles and Responsibilities

1. Director of IT Security: The Director of IT Security reports directly to the Chief Information Officer (CIO). The Director of IT Security is responsible for drafting University security policies, plans, and best practices documents. The Director of IT Security 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 Director of IT Security is responsible for coordinating compliance with this policy. Responsibilities and roles include but are not limited to:

    a. Head the Information Security Office (ISO).

    b. Develop and maintain security policy, plans, procedures, strategies, architectures, best practices, and minimum requirements.

    c. Educate IT Systems Administrators, computer professionals, and Users, regarding security. Provide guidelines, consultation, and assistance to colleges, departments, and individuals regarding the proper use of computer workstations, servers, applications, department networks and other IT Resources.

d. Provide assistance in complying with this policy to IT Resource Stewards, IT Resource Custodians, and IT Administrators as requested.

e. Implement and enforce baseline perimeter security practices endorsed for educational institutions by federal, state, and local government agencies, and national organizations such as Educause and SANS.

f. Monitor and analyze campus network traffic information to ensure compliance with University security and acceptable use policies, and to evaluate, identify, and resolve security vulnerabilities, breaches and threats to University IT Resources.

g. Conduct security audits as requested by colleges or departments. Conduct security audits periodically to confirm compliance with this policy.

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

i. Assist University or third party auditors in the analysis of college and departmental IT Resources to further ensure policy compliance.

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

2. Information Technology Department: The Information Technology department has primary responsibility for managing IT Resources, including but not limited to the campus network, servers, storage area networks, the IP phone system, user desktops and notebooks, and all properly licensed software installed on the network. The IT department’s security responsibilities include but are not limited to:

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

b. Inform the ISO of traffic patterns, which pursuant to best practices, procedures, and standards, may indicate a potential or actual threat to the network backbone and University IT Resources.

c. Apply security policy and procedures to IT Resources as directed by the ISO and industry best practices.

3. Incident Response Team: Under the direction of the ISO, 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. The team consists of the Director of IT Security and designated campus IT managers.

4. IT Resource Steward: The IT Resource Steward is designated by the cognizant authority of the relevant organization. Responsibilities include but are not limited to:

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

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

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

d. Determine accessibility rights to IT Resources.

e. Specify adequate data retention, in accordance with University policies, and state and federal laws for IT Resources consisting of applications or data.

f. In rare cases, an organization may need to configure IT Resources in a manner that is not compatible with standard security procedures, best practices, and minimum requirements (i.e., to conduct network and/or systems research, or for other academic purposes). In such cases, the IT Resource Steward, must accept responsibility for alternative security measures that may be implemented. The IT Resource Steward may request, and the ISO may grant, a written exemption from standard security procedures, best practices, and minimum requirements, provided the IT Resource Steward documents the need for an exception, receives a

ISO assessment of the risk and vulnerabilities exposed by the exception, and agrees to make every reasonable effort to prevent the exception from causing potential or actual security threats to the relevant organization and other campus organizations.

g. An IT Resource Steward in a college or department, which lacks the professional IT staff or expertise to accomplish items (a) through (f) in this section may request assistance from the ISO or the assigned IT Resource Custodian.

5. IT Resource Custodian: The IT Resource Custodian is responsible for implementing and maintaining security measures in accordance with the security level identified by the IT Resource Steward. For example, the Administrative Computing Services department would be the IT Resource Custodian of a central student registration system. Responsibilities include but are not limited to:

   a. Ensure proper controls are in place and followed to meet access requirements and security levels as determined by the IT Resource Steward.

   b. Determine the appropriate method for providing business continuity for Critical IT Resources (e.g., performing Disaster Recovery at an alternate site, performing equivalent manual Procedures, etc.).

   c. Prepare for disaster recovery. In the event of a disaster, provide oversight of the implementation of the Disaster Recovery Plan.

   d. 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.

   e. Ensure that data retention requirements are met for IT Resources consisting of applications or data.

6. IT Systems Administrator: The IT Systems Administrator(s) is responsible for the performance of security functions and procedures as directed by the IT Resource Custodian and/or IT Resource Steward. It is the IT Systems Administrator’s responsibility to implement and administer

the security of IT Resources in accordance with Southern Utah University and industry best practices and standards.

U. Exceptions to Policy

1. Exceptions to this policy and any related rules or procedures may be made where the cost to remediate systems and processes that are not compliant with applicable policies, rules, standards, procedures, and guidelines greatly exceeds the risks of non-compliance.

2. Exceptions to policy received and approved by the ISO and IT Resource Stewards will be documented and archived.

3. Exception requests are reviewed and analyzed by the ISO and the IT Resource Steward (or his/her designee), and if the request creates significant risks without compensating controls it may not be approved. If denied, appeals may be made to the CIO.

VI. Sanctions and Remedies

A. The IT department 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 University IT Resources. IT may discontinue service to any network segment or networked device if the continued operation of such segments or devices threatens the security of University IT Resources. The ISO will notify the IT Resource Steward and/or Custodian or their 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 University IT Resources.

B. The IT Resource Steward may discontinue service or request that the ISO discontinue service to network segments, network devices, or Users under their 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 University, college, or department IT Resources.

C. A User’s access shall be restored as soon as the direct and imminent security threat has been remedied.

D. The University reserves the right to revoke access to any IT Resource for any User who violates this policy, or for any other business reasons in conformance with applicable University policies.

E. Violation of the policy may result in disciplinary action in accordance with University policies referenced in Section II of this policy.