SUL ROSS STATE UNIVERSITY

A Member of the Texas State University System

SRSU Policy: Information Security Policy
SRSU Policy ID: APM 7.01
Policy Reviewed by: Chief Information Officer
Approval Authority: Executive Cabinet
Approval Date: 10/1/2020
Next Review Date: 9/30/2025

Sul Ross State University (SRSU) considers information technology to be a critical enabler in meeting its mission and has made significant investments in information technology assets and capabilities. SRSU recognizes the inherent value of these information technology resources to the state, the Texas State University System, and the institution.

Texas Administrative Code Title 1, Part 10, Chapter 202, (TAC 202), requires the institution head of each Texas State agency and public institution of higher education to protect their institution's information resources by establishing an information security program consistent with TAC 202 standards. In compliance with TAC 202, this policy statement and its references reflect the policies comprising the information security program of SRSU. The terms and phrases in this policy statement shall have the meanings ascribed to them in TAC 202.1, unless otherwise provided herein.

Compliance with this policy contributes to the availability, integrity and confidentiality of the information technology resources of Sul Ross State University.

Scope and Applicability

This policy statement applies to all persons and organizations that manage or utilize information technology resources belonging to Sul Ross State University.

Policy Purpose

Sul Ross State University (SRSU) must ensure the confidentiality, integrity, and availability of information technology resources to fulfill its institutional mission and to assure compliance with the security standards.

The purpose of this policy is to provide the university with a description of the plan for achieving compliance with TAC 202. The objectives of this policy are met by addressing security issues in each of the following areas:

- Roles and Responsibilities of the Information Security Organization;
- Risk Management;
- Information Asset Management (Data Classification);
- Human Resources Security
- Physical Security
- Communications and Operations Management
- Identity and Access Management
- Information Systems Acquisition, Development and Maintenance

- Security Incident Management
- Business Continuity and Disaster Recovery
- Compliance

Policy Statements

1. Roles and Responsibilities of the Information Security Organization

   The following section establishes the roles and responsibilities of the various members of the Information Security Organization.

   1.1 SRSU's Executive Cabinet, which includes the President, approves and supports the security policies, roles, and practices necessary to achieve security consistent with business requirements, relevant laws and regulations. The ISO provides frequent opportunity to review any information security issues related to operations, process, policy, or incidents with the intent of maintaining executive level support for the Information Security Program (TAC 202.70(3)).

   1.2 The Information Resource Manager (IRM) as defined in Texas Administrative Code 211 provides executive level oversight for the acquisition and use of information technology within the institution of higher education, and ensures that all information resources are acquired appropriately, implemented effectively, and in compliance with relevant regulations and policies.

   1.3 The ISO is responsible for all aspects of the university's Information Security Plan, reports to executive level management, has authority for information security for the entire institution, possesses training and experience required to administer the functions of the Information Security Officer (ISO), and is charged with the responsibilities as outlined in TAC 202.71.

   - developing and maintaining an institution-wide information security plan as required by §2054.133, Texas Government Code;
   - developing and maintaining information security policies and procedures that address the requirements of this chapter and the institution's information security risks;
   - working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of this chapter and the institution's information security risks;
   - providing for training and direction of personnel with significant responsibilities for information security with respect to such responsibilities;
   - providing guidance and assistance to senior institution of higher education officials, information owners, information custodians, and end users concerning their responsibilities under this chapter;

- ensuring that annual information security risk assessments are performed and documented by information-owners;
- reviewing the institution's inventory of information systems and related ownership and responsibilities;
- developing and recommending policies and establishing procedures and practices, in cooperation with the institution Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure;
- coordinating the review of the data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data;
- verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data;
- reporting, at least annually, to the state institution of higher education head the status and effectiveness of security controls; and
- informing the parties in the event of noncompliance with this chapter and/or with the institution's information security policies.

Exceptions to information security requirements or controls must be documented, justified, and approved by the Information Security Officer.

1.4 Information Owner Role and Responsibilities (TAC 202.72(1)). Information Owners are designated for assets based on business oversight and organizational structure. Ownership responsibility for information resources is assigned based on accountability for the assets, as documented in the university's inventory, procurement, and licensing records. Specific responsibilities as outlines in TAC 202 include:

- classify information under their authority, with the concurrence of the IRM and in accordance with established information classification categories found on the OIT website;
- approve access to information resources and periodically review access lists based on documented risk management decisions;
- formally assign custody of information or an information resource;
- coordinate data security control requirements with the ISO;
- convey data security control requirements to custodians;
- provide authority to custodians to implement security controls and procedures;
- justify, document, and be accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the ISO;

- participate in risk assessments

1.5 Information Custodian Role and Responsibilities (TAC 202.72(2)). In consultation with the Information Owners, Information Custodians provide information asset services to both owners and users. An Information Custodian is the operational entity that implements the procedures and controls that provide the appropriate protection for information technology resources. This is defined at SRSU as the OIT organization. Specific responsibilities as outlines in TAC 202 include:

- implement controls required to protect information and information resources required based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the institution's information security program;
- provide owners with information to evaluate the cost-effectiveness of controls and monitoring;
- adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;
- provide information necessary to provide appropriate information security training to employees; and
- ensure information is recoverable in accordance with risk management decisions.

1.6 User Role and Responsibilities (TAC 202.72(3)). The user role is the default role possessed by all users of Sul Ross State University information technology resources. Users of information technology resources shall use those resources for defined purposes that are consistent with their institutional responsibilities and always in compliance with established controls. Users must comply with the university's published security policies and procedures, as well as with security bulletins and alerts that OIT issues in response to specific risks or threats. The use of Sul Ross State University information technology resources implies that the user has knowledge of and agrees to comply with the university's policies governing such use.

Users are responsible for ensuring the privacy and security of the information they access in the normal course of their work. Users are also responsible for the security of any terminal, workstation, printer or similar electronic device utilized in the normal course of their work. Users are authorized to use only those resources and materials that are appropriate and consistent with their job functions and must not violate or compromise the privacy or security of any data or systems accessible via the university computer network (See APM 7.04, Appropriate Use of Information Technology Resources, for additional information about acceptable and prohibited uses of Sul Ross information technology resources).

Users may not attempt to violate the security or privacy of other computer users on any system accessible via the university network. The attempted violation of information security or privacy is grounds for revocation of access privileges,

suspension or discharge of employees, suspension or expulsion of students, and prosecution to the full extent of the law.

2. Risk Assessment

In accordance with TAC 202.75, the ISO periodically completes or commissions a risk assessment of the information, information systems, and applications considered essential to the university's critical mission and functions and recommends to the information owners and information custodians of these resources appropriate risk mitigation measures, technical controls, and procedural safeguards. The assessment may incorporate self-assessment questionnaires, vulnerability scans, scans for confidential information, and penetration testing. Findings and recommendations are provided to the information owners and information custodians on the information assets and presented to the institution's executive leadership as appropriate.

Information owners and information custodians shall complete these risk assessments of their assigned information technology resources, including departmentally-administered computing resources that store, process and access Confidential information at least biennially or periodically for systems containing sensitive or public data. The assessment must include a classification of their information according to its need for security protection. See section 3, Data Classification, for specific classifications.

The assessment should identify reasonable, foreseeable, internal and external risks to the confidentiality, integrity and availability of those resources. Information owners and information custodians should assess the sufficiency of safeguards in place to control these risks and document their level of risk acceptance (i.e. the exposure remaining after implementing appropriate protective measures, if any). They should also take mitigating measures to protect the resources from unacceptable risks. The risk assessment should include consideration of employee training and management, information system architecture and processes, business continuity planning and prevention, detection and response to intrusion and attack. The assessment results are documented in a written report, protected from unauthorized disclosure, modification or destruction and retained until superseded by a subsequent documented assessment, plus one year.

3. Information Asset Management

To achieve and maintain appropriate protection of campus information assets, assets must be classified according to their need for security protection. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned.

All SRSU data, whether electronic or printed, must be classified as Confidential, Sensitive, or Public, as outlined below. Consistent use of data classification reinforces the expected level of protection of SRSU data assets in accordance with SRSU policies.

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by federal law, state law, Texas State University System Rule and Regulations, university policy, as well as proprietary, ethical, operational and privacy considerations.

Prior to releasing, publishing, or disclosing any information, the information owner shall classify the information according to one of the three levels outlined below.

The information owner shall ensure that disclosure controls and procedures are implemented to afford the degree of protection required by the assigned classification.

Higher education and industry best practices suggest the need for three classifications with respect to data confidentiality. In order from least to most confidential, these are:

a. Public Information is by its very nature designed to be shared broadly, without restriction, at the complete discretion of the information owner. It may or may not have been explicitly designated as public. There is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm to the university, individuals, or affiliates. From the perspective of confidentiality, public information may be disclosed or published by any person at any time.

   Examples: advertising, degree program descriptions, course offerings and schedules, campus maps, published research (within copyright restrictions), job postings, press releases, general information about university products and services, certain types of unrestricted directory information as specified by the Family Educations Rights and Privacy Act of 1974 (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA).

b. Sensitive information is the most difficult to describe as it often presents attributes of both Public and Confidential information. Sensitive information is often considered "public" in the sense that it is releasable under provisions of the Texas Public Information Act, while also requiring assurances that its release is both controlled and lawful. Sensitive information is often intended for use within a specific workgroup, department or group of individuals with a legitimate need-to- know. Likewise, access to Sensitive information is often controlled by identity 5/18/2016 authentication and authorization measures (e.g., LoboID and password). Unauthorized disclosure of Sensitive information could adversely impact the university, individuals or affiliates.

   Examples: some employee records (such as performance appraisals, dates of birth, etc.), departmental policies and procedures that might reveal otherwise restricted information, the contents of e-mail, voicemail, instant messages and memos, unpublished research, information covered by non-disclosure agreements, donor information, etc.

Generally speaking, Sensitive information should not be published or disclosed to the public except by the university's designated owner of the requested information in accordance with the owner's established procedures for processing TPIA requests, or as otherwise authorized by IT Security or the TSUS Associate General Counsel. (See separate list of the university's designated information owners)

c. According to Chapter 202 of the Texas Administrative Code (TAC 202), Confidential information is "information that is excepted from disclosure requirements under the provisions of applicable state or federal law" such as the Texas Public Information Act (TPIA) and the Family Education Rights and Privacy Act (FERPA). Confidential information presents the most serious risk of harm if improperly disclosed. Confidential information is generally intended for a very specific purpose and should not be disclosed to anyone without a demonstrated need-to-know, even within a workgroup or department. Disclosure of Confidential information is generally regulated by specific legal statutes (e.g., TPIA, FERPA, HIPAA), published opinions by the Office of the Attorney General of Texas, the Texas State University System Rules and Regulations, or contractual agreements. Unauthorized disclosure of this information could have a serious adverse impact on the university, individuals, or affiliates.

   Examples: student education records as defined under FERPA, credit card information, bank account numbers, social security numbers, driver license numbers, personally identifiable medical records, passport information, crime victim information, library circulation records, court sealed records, access control credentials (e.g., PINs and passwords), etc.

   Confidential information must not be published or disclosed to the public under any circumstances other than those specifically authorized by law. Any such disclosure should be immediately reported to the CIO for damage mitigation and investigation. Requests for such information received from persons with a questionable need to know should be directed to the TSUS Associate General Counsel.

   Standards for Handling Confidential Information

   Because of the harm that can result from improper disclosure, confidential university information shall be afforded the following special protections by owners, custodians, and users:

   a. A person's social security number, driver license number, or other widely-used government-issued identification number shall not be captured, stored, or used as a person identifier unless such use is required by an external, governmental, or regulatory system that is authorized for use at the university. The LoboID or A-number should be used in lieu of such prohibited identifiers in situations where personal names or other identifiers do not assure uniqueness. Where use of such numbers is required, owners, custodians, and users shall store these numbers in

encrypted form, when possible, or use other compensating controls with the advice and authorization of the ISO.

b. Payment cardholder data (i.e., the primary account number or the magnetic stripe contents together with any one of: cardholder name, expiration date, or the service code) shall not be stored on any device connected to the university's data network for longer than is necessary to authorize a transaction using that information.

c. Confidential information must not be transmitted electronically over a public network (e.g., the Internet) in unencrypted form. Either the information itself must be encrypted prior to transmission or an encrypted connection must be established and maintained for the duration of the transmission. Authorized encrypted connection examples include the university's implementations of: VPN – Virtual Private Network, TLS – Transport Layer Security, and SSH – Secure Shell.

d. Confidential information must not be stored on portable devices or media such as notebook or tablet computers, PDAs, smart phones, USB drives, CDs, DVDs, tape cartridges, etc. If such storage is required, the confidential information must be protected by encryption or by other compensating controls with the advice and authorization of the ISO.

e. Confidential information must not be accessed from remote locations in an unauthorized manner. Examples of authorized remote access solutions include the university's implementations of: VPN, TLS, and SSH. Contact OIT for up-to-date information about the acceptability of other remote access solutions.

f. Confidential information should not be stored on personally-owned devices or media. If such storage is required, the confidential information must be protected by encryption or by other compensating controls with the advice and authorization of the ISO.

g. Confidential information must not be stored on any devices external to the campus network except as provided under contract with an authorized information resource service provider that is contractually bound to properly protect the information.

h. Encryption requirements for information storage and transmission, as well as for portable devices, removable media, and encryption key management, shall be based on documented risk management decisions. Contact OIT for up-to-date information about university-supported encryption solutions.

i. Confidential information must not be shared, exposed or transmitted via any peerto-peer (P2P) file sharing mechanism prior to completion of a comprehensive risk assessment, including penetration testing, of the proposed P2P file sharing mechanism by OIT.

4. Human Resources Security

In any organization, people represent both the greatest information security assets as well as its greatest risk. Consequently, employee awareness and motivation are integral parts of any comprehensive information security program. To ensure that employees, contractors and other users understand their information security responsibilities and to reduce the risk of theft, fraud or misuse of information resources, all employees, contractors, and other users should be fully apprised of their security responsibilities and formerly acknowledge they will comply with SRSU security policies and procedures (TAC 202.72). Their access to information assets is managed consistent with their current institutional status, roles, and qualifications. Information security training should be provided to employees at new employee orientation and annually thereafter.

To emphasize security awareness and the importance of individual responsibility with respect to information security, OIT shall provide information at all new employee orientation sessions, as well as periodic seminars, workshops, and other educational events for existing employees. All such training and events will provide references to relevant university policy, procedures, guidelines, and best practices. Department heads shall continually reinforce the value of security-consciousness in all employees whose duties entail access to sensitive or confidential information technology resources.

Information owners are responsible for implementing the measures necessary to ensure that department members maintain the confidentiality of information resources used in departmental operations. Examples of such information include personnel and payroll records, transcript and grade records, financial aid information, and other sensitive or confidential information. Such information shall not be used for unauthorized purposes or accessed by unauthorized individuals. Department heads are encouraged to obtain and retain signed non-disclosure agreements from their employees prior to granting those employees access to departmental information technology resources.

5. Physical and Environmental Security

Physical access to mission critical information technology resources facilities shall be managed and documented by OIT. The facilities must be protected by physical and environmental controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated within those facilities. Physical access to information technology resources facilities administered by OIT is restricted to individuals having prior authorization from the CIO. A log will be maintained of all persons entering or leaving the university's primary data center, including the date, time, and purpose of the visit. Access to the equipment rooms and the data center shall be secured, visually monitored and recorded when practical.

The responsibility for securing departmentally administered computer facilities or equipment from unauthorized physical access rests with the owner of the facility or

equipment. The facility's owner must review physical security measures annually in conjunction with each facility's risk assessment, as well as whenever facilities or security procedures are significantly modified (see TAC 202.72).

Employees and information technology resources shall be protected from the environmental hazards posed by information technology resources facilities. Employees with duty stations inside information technology resources facilities shall be trained to monitor any installed environmental controls and equipment, and to respond appropriately to emergencies or equipment malfunctions.

Terminals, computers, workstations, communication switches, network components, and other devices outside the university's primary data centers shall receive the level of protection necessary to ensure the integrity and confidentiality of the university information accessible through them. The required protection may be achieved by physical or logical controls, or a combination thereof.

No authenticated work session (i.e., a session in which the user's identity has been authenticated and authorization has been granted) shall be left unattended on any information resource unless appropriate measures have been taken to prevent unauthorized use. Examples of appropriate measures include:

a. activation of password-protected keyboard or device locking;
b. automatic activation of a password-protected screensaver after a brief inactivity period (15 minutes or less, based upon risk assessment); and
c. location or placement of the device in a locked enclosure preventing access to the device by unauthorized parties.

The creator of the work session is responsible for any activity that occurs during a work session logged in under his or her account.

6. Communications and Operations Management

Network resources used to exchange sensitive or confidential information shall protect the confidentiality of the information for the duration of the session. Controls shall be implemented commensurate with the highest risk. Transmission encryption technologies (e.g., VPN, TLS, HTTPS, SSH, IPSEC, etc.) shall be employed to accomplish this objective.

Confidential university information must not be transmitted over a public network (e.g., the Internet) in unencrypted form. Either the information itself must be encrypted prior to transmission or an encrypted connection must be established and maintained for the duration of the transmission. Authorized encrypted connection examples include the university's implementations of VPN, TLS, and SSH, as well as any wireless network connection utilizing the Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES). These restrictions apply regardless of the user's location and include

transmissions over any network accessible to the user. OIT shall establish and maintain a WPA2-AES encrypted (or equivalent or superior) wireless network for use on the university campus.

To facilitate security of the campus network, Information Owners, Information Custodians, and users of information technology resources shall adhere to the provisions of APM 7.05, Network Management Policy.

Information Owners of distributed information technology resources within the campus network shall prescribe sufficient controls to ensure that access to those resources is restricted to authorized users and uses only. Examples of such resources include network equipment rooms, data closets, and the equipment contained within them. Controls shall restrict access to the resources based upon user identification and authentication (e.g., password, smartcard or token), physical access controls, or a combination thereof (see TAC 202.72(2)(A)).

Information Owners of applications containing sensitive or confidential information, or applications involving automated transmission of such information to other applications, shall require authentication of user identity prior to granting access to the applications (see TAC 202.72(1)(B)).

7. Identity and Access Management

Prior to obtaining access to the Sul Ross network, any device connected to that network, any service provided via that network, or any application hosted on that network, individuals must authenticate themselves as authorized users of the network, service, device, or application. This requirement may be waived in situations where a formal risk assessment has determined that access to the resource does not require individual user identification, authorization, or accountability.

A university-assigned network identifier (e.g., LoboID or A-Number) and its corresponding “secret” (e.g., a password/PIN or smartcard or token) shall be used to accomplish the authentication. The network identifier shall be unique to an individual in all cases except for authorized “service” accounts that must be accessible to a team of custodians charged with supporting a breadth of resources.

Users are responsible for the security of any computer account (e.g., LoboID, A-number or username) issued to them and are accountable for any activity that takes place in their account. Users who discover or suspect that the security of their account has been compromised must immediately change their password and report the incident to their supervisor and to OIT.

Self-service systems must incorporate security procedures and controls to ensure the data integrity and protection of sensitive or confidential information. Self-service systems

must authenticate the identity of individuals that utilize the systems to retrieve, create, or modify sensitive or confidential information about them.

To the extent practicable, all initial login and authentication screens should clearly and prominently display the following user advisory or other similar language to ensure users of those assets understand their responsibilities in doing so:

> "*You are accessing a system owned by the State of Texas.*
> *Unauthorized use is prohibited and subject to criminal and civil penalties.*
> *Usage may be monitored, recorded, and subject to audit.*
> *There should be no expectation of privacy except as otherwise provided by applicable privacy laws.*
> *Use of the system indicates consent to monitoring and recording*."

A user's network identifier is deactivated whenever the user's affiliation with the university no longer qualifies the user to possess an active LoboID.

Sensitive and confidential information shall be accessible only to personnel with authorization from the information owner on a strict "need-to-know" basis in the performance of their assigned duties. Such information shall be disclosed only by the Information/Data Owner, as described in the Data Ownership Guide.

Sul Ross systems that employ passwords for authenticating user identities shall comply with the minimum password acceptability standards contained in the Password Guide on the OIT website.

8. Information Systems Acquisition, Development, and Maintenance

Acquisition

Sul Ross State University, in compliance with The Texas State University System Rules and Regulations (III-19.3), mandates review and oversight of all information technology resource from procurement and development through implementation and ongoing maintenance. This includes, but is not limited to computing hardware, software, peripherals, classroom technology, electronic subscriptions, phones, TVs, security equipment and services, regardless of the source of funds and method or location of use. SRSU designates the university's IRM and his/her designee with the oversight for all assets acquired and used by the university. All information technology resource related acquisitions and gifts must be reviewed by OIT and receive approval, prior to a formal submission of request for acquisition or acceptance of gift.

Development

Test functions shall be kept either physically or logically separate from production functions, to the extent possible.

To the extent practicable, the principle of separation of duties and least privilege shall be applied to the system development and acquisition lifecycle. The developer or maintainer of a component should not also have the ability to place the component into production.

Modifications to production data by custodians or developers shall be authorized in advance by the data owner. If advance authorization is not possible in a real or perceived emergency, the owner shall be notified as soon as possible after the fact and the notification logged. The notification log entry shall contain the notification date and time, a description of the data modified, the justification for the modification, and the identities of the owner and the custodian.

Information Owners and Information Custodians will ensure that new and modified Web applications are compliant with SRSU's web application development standards prior to their production deployment.

9. Information Security Incident Management

The ISO is charged with establishing and maintaining an effective Incident Response Plan to ensure that:

a. security events are thoroughly investigated and documented;
b. immediate damage is minimized, latent risks are identified, and subsequent exposures are mitigated;
c. incident reporting and notification are timely and legally compliant; and
d. remedial actions are taken to prevent recurrence.

As part of the Incident Response Plan, the ISO will develop an Incident Response Team (IRT) and procedures for responding to incidents. This plan must include required notifications to impacted parties as described in Texas Business & Commerce Code, Chapter 521, Subchapter B, Identity Theft, when appropriate

The ISO will activate the IRT when, in his or her judgment, sensitive personal information was, or is reasonably believed, to have been acquired by an unauthorized person. The response team associated with the IRP will include, at a minimum:

a. the ISO, as the team lead;
b. the CIO, as the adjutant team lead;
c. members of the OIT Networking and Systems team;
c. the owners of the breached information resource;
d. the SRSU Internal Auditor;
f. other IT and university employees at the discretion of the ISO in collaboration with other members of the team.

Security incidents must be reported immediately to the immediate supervisor and to the ISO.

If criminal activity is suspected, the ISO shall immediately contact the appropriate law enforcement and investigative authorities (see TAC 202.73(b)(1)(B)).

The ISO shall fully document the incident, the investigation itself, and the results of the investigation. A draft incident report will be prepared and shared with the CIO, the Information Owners and Information Custodians of the compromised resources and their respective vice presidents.

If it is determined that:

- The event could propagate to other systems;
- Could result in a criminal violation; or,
- Involves the unauthorized disclosure of Personally Identifying Information (PII), Sensitive Personal Information (SPI) as defined in Texas Business and Commerce Code, Section 521.002, or Confidential Information as defined in the SRSU Data Classification Guide

the Texas Department of Information Resources (DIR), the TSUS associate general counsel, and the Director of Audits and Analysis will be notified within 48 hours of the discovery of the incident.

10. Business Continuity Management

Information technology resources must be available when needed. Continuity of information systems supporting critical university functions must be ensured in the event of a disaster or disruption in normal operations.

Administrative heads responsible for delivering mission critical university services should maintain written business continuity plans (BCP) that provide for continuation or restoration of such services following a disruption in critical information systems, communication systems, utility systems, or similar required support systems. The BCP should incorporate:

a. a business impact analysis that addresses the maximum possible downtime for critical service delivery components and resources including: key personnel, facilities, components of electronic information and communication systems (e.g., voice and data network, hardware, and software), and vital electronic and hard copy records and materials;
b. to the extent practicable, alternate methods and procedures for accomplishing its program objectives in the absence of one or more of the critical service delivery components;
c. a security risk assessment to weigh the cost of implementing preventive measures against the risk of loss from not taking preventive action;
d. a recovery strategy assessment that documents realistic recovery alternatives and their estimated costs; and

e. reference to a disaster recovery plan that provides for the continuation or restoration of electronic information and communication systems as described later in this section.

Key aspects of the BCP should be tested or exercised at least annually and updated as necessary to assure the plan's continued viability. Results of such tests and exercises should be documented and retained until the end of the current fiscal year, plus three years.

OIT shall prepare and maintain a written and cost-effective Disaster Recovery Plan (DRP) that addresses key infrastructure components in its custody. The plan should provide for the prompt and effective continuation or restoration of critical university information technology resources and processes if a disaster were to occur that might otherwise severely disrupt these systems and processes. The plan should provide for the scheduled backup of mission critical information and for the off-site storage of that backup in a secure, environmentally safe and locked facility accessible only to authorized IT staff. The plan should also identify other key continuation and recovery strategies, required resources, alternate sources of required resources, as well as measures employed to minimize harmful impacts. OIT shall exercise or test key aspects of the disaster recovery plan and make periodic updates as necessary to assure its viability.

11. Compliance

The CIO shall commission periodic reviews of the university's information security policy for compliance with TAC 202 standards. Reviews will be conducted at least biennially by individuals independent of the information security program and will be based on business risk management decisions (see TAC 202.76).

Key aspects of the university's information security program shall be a prominent component of any university program designed to encourage or enhance legal and policy compliance by university constituents.

Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of the institution's information technology resources.