**Security of Texas State Information UPPS No. 04.01.01**

**Resources Issue No. 13**

**Effective Date: 10/11/2023**

**Next Review Date: 09/01/2025 (E2Y)**

**Sr. Reviewer: Chief Information Security Officer**

**POLICY STATEMENT**

*Texas State University is committed to protecting the institution’s information resources by establishing and maintaining an information security program.*

**01. BACKGROUND INFORMATION**

01.01 [Title 1, Part 10, Chapter 202, Texas Administrative Code](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), commonly known as [TAC 202](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), requires the institution head of each Texas state agency and public institution of higher education protect their institution’s information resources by establishing an information security program consistent with [TAC 202](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202) standards. In compliance with [TAC 202](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), this policy statement and its references reflect the policies, procedures, standards, and guidelines comprising the information security program of Texas State University. The terms and phrases in this policy statement shall have the meanings ascribed to them in [TAC 202.1](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=1), unless otherwise provided herein.

The Texas State Information Security Program is positioned within the office of the vice president for Information Technology (VPIT) and administered by the university’s Information Security officer (ISO). The ISO’s Information Security team implements the Information Security Program in collaboration with all university constituents that use and support the university’s information resources (see [TAC 202.70(3)](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70) and [TAC 202.71(b)](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=71)).

01.02 Information resources that support the operations of Texas State are strategic and vital assets belonging to the people of Texas. These assets must be available when needed and protected commensurate with their value. All members of the university community, regardless of position or role, share responsibility for protecting the university’s information resources. The Texas State community shall take appropriate measures to protect the university’s information resources against accidental or unauthorized disclosure, contamination, modification, or destruction, and to assure the confidentiality, authenticity, utility, integrity, and availability of university information (see [TAC 202.72](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=T&app=9&p_dir=N&p_rloc=176794&p_tloc=&p_ploc=1&pg=3&p_tac=&ti=1&pt=10&ch=202&rl=70)).

01.03 All individuals are accountable for their use of the university’s information resources. Individuals shall comply with applicable laws, [The Texas State University System (TSUS) Rules and Regulations](https://www.tsus.edu/about-tsus/policies.html), and all university policies in their use of these resources (see [TAC 202.72](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=72)).

 In addition to this policy, the following university policies are particularly relevant and noteworthy:

1. [UPPS No. 04.01.05](https://policies.txstate.edu/university-policies/04-01-05.html), Network Use Policy – describes policy and procedures for administration, maintenance, and operation of the university’s network infrastructure;

b. [UPPS No. 04.01.07](https://policies.txstate.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources – describes both intended and prohibited uses of information resources;

c. [UPPS No. 04.01.09](https://policies.txstate.edu/university-policies/04-01-09.html), Server Management Policy – describes policies and standards for administration, maintenance, and operation of the university’s computer servers;

d. [UPPS No. 04.01.10](https://policies.txstate.edu/university-policies/04-01-10.html), Information Security Incident Management – establishes incident response procedures and reporting requirements;

e. [UPPS No. 04.01.11](https://policies.txstate.edu/university-policies/04-01-11.html), Risk Management of Information Resources – describes the process and procedures to manage risk to information resources;

f. [UPPS No. 05.01.02](https://policies.txstate.edu/university-policies/05-01-02.html), University Surplus Property (Equipment and Consumable Supplies) – provides guidance in the appropriate disposal of computer equipment and digital media; and

g. [UPPS No. 05.02.06](https://policies.txstate.edu/university-policies/05-02-06.html), Acquisition of Information Technology Products and Services – provides guidance regarding the purchase, rental, lease, or free acceptance of information technology products or services from third-party providers.

01.04 Information that is sensitive or confidential must be protected from unauthorized access or modification. Data that are essential to critical university functions must be protected from loss, contamination, or destruction (see [NIST SP 800-53 AC-2](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

01.05 Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected, considering value of the asset to the university, regulatory agencies, the public, potential intruders, and any other person or organization with an interest in the assets (see [NIST SP 800-53 PM-9, RA-3](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf) and [UPPS No. 04.01.11](https://policies.txstate.edu/university-policies/04-01-11.html), Risk Management of Information Resources).

01.06 The integrity of data, its source, its destination, and processes applied to it are critical to its value. Changes to data must be made only in authorized and acceptable ways (see [TAC 202.70(5)](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70)).

01.07 Information 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 (see [TAC 202.70(6)](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70)).

01.08 Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources (see [NIST SP 800-53 SA-3](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

01.09 Security awareness of employees must be introduced during the onboarding process and continually emphasized and reinforced at all levels of management. All individuals must be accountable for their actions relating to information resources (see [NIST SP 800-53 AT-2](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf) and [TAC 202.24(b)](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=24)).

01.10 The Information Security Program must be responsive and adaptable to changing vulnerabilities and technologies affecting information resources. Its components shall be reviewed and modified in a timely fashion to meet emerging and evolving threats.

01.11 The university must ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity (see [NIST SP 800-53 AC-5](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

**02. INFORMATION SECURITY ORGANIZATION**

02.01 The VPIT is the university’s information resources manager (IRM), as defined in the Information Resources Management Act (IRMA) ([Tex. Government Code § 2054](https://statutes.capitol.texas.gov/SOTWDocs/GV/htm/GV.2054.htm)). The IRM oversees the acquisition and use of information technology within a state agency or university.

IRMA and TAC (see [TAC, Title 1, Part 10, Chapter 211](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=211)) establish rules and responsibilities for the designated IRM that include executive level oversight for security and risk management of the university’s information resources. Consequently, the office of the VPIT directs the university’s IT security function.

02.02 The ISO is the designated administrator of the Information Security Program. The ISO must report to executive level management, has explicit authority for information security for the entire institution, and is responsible for all aspects of the university’s Information Security Program (see [TAC 202.71](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=71)).

The ISO is specifically charged with the following responsibilities:

a. develop, recommend, and establish policies, procedures, and practices as necessary to protect the university’s information resources against unauthorized or accidental modification, destruction, or disclosure;

b. identify and implement proactive and reactive technical measures to detect vulnerabilities and to defend against external and internal security threats;

c. provide consulting and technical support services to owners, custodians, and users in defining and deploying cost-effective security controls and protections;

d. establish, maintain, and institutionalize security incident response procedures to ensure that security events are thoroughly investigated, documented, and reported; that damage is minimized; that risks are mitigated; and that remedial actions are taken to prevent recurrence;

e. establish and publicize a security training and awareness program to achieve and maintain a security-conscious user community;

f. document, maintain, and obtain ongoing support for all aspects of the Information Security Program;

g. monitor the effectiveness of strategies, activities, measures, and controls designed to protect the university’s information resources;

h. assure executive management awareness of legal and regulatory changes that might impact the university’s information security and privacy policies and practices;

1. serve as the university’s internal and external point of contact for information security matters; and

j. report directly to the president, at least annually, on the adequacy and effectiveness of the Information Security Program (see [TAC 202.73(a)](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=73)).

02.03 As stated in Section 01.02, all members of the university community share responsibility for protecting the university’s information resources and, as such, are essential components of the university’s Information Security Program. Nonetheless, individual responsibilities can vary significantly according to an individual’s relationship with any given information resource. In recognition of those variances, the university has defined and assigned three generic roles with respect to the security of information resources: the owner role, the custodian role, and the user role. Each individual assumes one or more of these roles with respect to each information resource they use, and as a result, are accountable for the responsibilities attendant to their roles (see [UPPS No. 04.01.11](https://policies.txstate.edu/university-policies/04-01-11.html), Risk Management of Information Resources).

**03. HUMAN RESOURCES SECURITY PROCEDURES**

03.01 In any organization, people represent both the greatest information security assets, as well as the greatest information security threats. Consequently, employee awareness and motivation are integral parts of any comprehensive information security program.

03.02 To emphasize security awareness and the importance of individual responsibility with respect to information security, all Texas State employees shall explicitly affirm their agreement to abide by the university’s information security, copyright, and appropriate use policies annually (see [TAC 202.70(3)](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70)).

03.03 Information Security shall provide training and literature during the employee onboarding process, as well as recurring information security education through periodic workshops, educational events, and online training. All such training and events will provide references to relevant university policy and procedure documents and promote the [Information Security website](http://infosecurity.txstate.edu/) as a valuable repository of information security policies, 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 resources (see [NIST SP 800-53 AT](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

03.04 Department heads are responsible for implementing the measures necessary to ensure that department members maintain the confidentiality of information 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 resources. [Template non-disclosure agreements](https://infosecurity.txstate.edu/services-tools/security-tools.html) are available, together with other [policies, standards, and guidelines](https://infosecurity.txstate.edu/work/law-policy.html), on the [Information Security website](http://infosecurity.txstate.edu/) (see [TAC 202.70](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70) and [TAC 202.72](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=72)).

03.05 Department heads are responsible for ensuring that access privileges are revoked or modified, as appropriate, for any employee in their charge who is terminating, transferring, or changing duties. Department heads should immediately notify IT Assistance Center (ITAC) to prepare for phone and IT access change or removal using the online form found on the [ITAC Employee Separations website](https://itac.txst.edu/support/separations). The emergency separation request option for involuntary termination must be used. Department heads must make sure to revoke access for any departmentally managed resources or third-party systems not covered by ITAC (see [TAC 202.72](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=72)).

03.06 Owners of information resources shall obtain and retain signed non-disclosure agreements from all temporary employees, consultants, contractors, and other external parties prior to them obtaining access to Texas State information resources. The agreements shall affirm their compliance with Texas State’s security policies and procedures. [Template non-disclosure agreements](https://infosecurity.txstate.edu/services-tools/security-tools.html) are available, together with other [policies, standards, and guides](https://infosecurity.txstate.edu/work/law-policy.html), on the [Information Security website](http://infosecurity.txstate.edu/) (see [TAC 202.72](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=72)).

**04. PHYSICAL AND ENVIRONMENTAL SECURITY PROCEDURES**

04.01 Physical access to mission critical information resources facilities shall be managed and documented by the facility’s custodian. 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 (see [NIST SP 800-53 PE-1](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

04.02 Physical access to information resources facilities administered by the IT division is limited to individuals with prior authorization from the associate vice president of Technology Resources (AVPTR), or designee, responsible for the facility. The AVPTR, or designee, will periodically review and update the access control lists to validate that only approved and appropriate staff retain access (see [TAC 202.72](https://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=72)). The responsibility for securing departmentally-administered computer facilities or equipment from unauthorized physical access ultimately rests with the designated owner and designated custodian of the facility or equipment.

A log will be maintained of all persons entering or leaving the university’s primary data centers, including date, time, and purpose of the visit. Access to the equipment rooms in these data centers shall be electronically secured and visually monitored and recorded.

04.03 Employees and information resources shall be protected from the environmental hazards posed by information resources facilities. Employees with duty stations inside information resources facilities shall be trained to monitor any installed environmental controls and equipment, and to respond appropriately to emergencies or equipment malfunctions. Emergency procedures shall be developed, documented, and regularly tested in collaboration with the university’s Office of Environmental, Health, Safety, Risk and Emergency Management (see [NIST SP 800-53 PE](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

04.04 Terminals, computers, workstations, mobile devices (e.g., laptops, portable storage devices, smart phones, etc.), 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 (e.g., a session in which the user’s identity has been authenticated and authorization has been granted) shall be left unattended on one of these devices unless appropriate measures have been taken to prevent unauthorized use. Examples of appropriate measures include:

a. manually locking the device to be left unattended through use of a password-protected lock screen;

b. automatic activation of a password-protected screensaver after a brief inactivity period (15 minutes or less, based upon risk assessment); and

1. 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 their account.

**05. CONTINUITY OF OPERATIONS MANAGEMENT PROCEDURES**

05.01 Administrative heads responsible for delivering mission critical university services should maintain documented continuity of operations plans (COOP) 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 plan should be reviewed and updated at least annually.

05.02 Key aspects of the COOP 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 (see [NIST SP 800-53 CP](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

05.03 Technology Resources shall prepare and maintain a written disaster recovery plan that addresses key infrastructure components in its custody. The plan should provide for the prompt and effective continuation or restoration of critical university information systems 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, physically 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. Technology Resources shall exercise or test key aspects of the disaster recovery plan and make periodic updates as necessary to assure its viability (see [NIST SP 800-53 CP](https://dir.texas.gov/sites/default/files/2023-05/Security%20Control%20Standards%20Catalog%20Version%202.1.pdf)).

05.04 Owners and custodians of departmental information resources are responsible for disaster recovery plans associated with those resources. The plans should include regular schedules for making backup copies of all data and software resident in their systems and for ensuring that the backups are stored in a safe location. Users are responsible for ensuring that the data and software resident on their personal computers are backed up as required by their individual circumstances. The security controls over the backup resources should be as stringent as the protection afforded to the primary resources (see the [Server Backup and Recovery Guide](https://infosecurity.txstate.edu/services-tools/security-services/server-management/server-backup-and-recovery-guide.htm) available from the [Information Security website](http://infosecurity.txstate.edu/) or [ITAC](http://itac.txstate.edu/) for assistance in the design of backup and recovery solutions).

**06. COMPLIANCE**

06.01 The VPIT shall commission periodic reviews of the university’s Information Security Program for compliance with [TAC 202](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=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 202.70](http://texreg.sos.state.tx.us/public/readtac%24ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70)).

06.02 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.

**07. REVIEWERS OF THIS UPPS**

07.01 Reviewers of this UPPS include the following:

 Position Date

Chief Information Security Officer Sept 1 E2Y

Director for Environmental, Health, Sept 1 E2Y

Safety, Risk and Emergency

Management

Associate Vice President for Sept 1 E2Y

Technology Resources

Vice President for Information Sept 1 E2Y

Technology

**08. CERTIFICATION STATEMENT**

This UPPS has been approved by the following individuals in their official capacities and represents Texas State policy and procedure from the date of this document until superseded.

Chief Information Security Officer; senior reviewer of this UPPS

Vice President for Information Technology

President