**Risk Management of Information UPPS No. 04.01.11**

**Resources Issue No. 3**

**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 the management of security risks posed to information resources.*

**01. BACKGROUND INFORMATION**

01.01 This policy establishes the basis for management of security risks posed to information resources, including risk assessment, risk mitigation, and common configuration requirements across most information resources, including information systems and information system components.

01.02 The frameworks outlined in this policy are not intended to be the sole source of configuration requirements, as technical requirements for individual information resources will be dependent on the category of the resource, context surrounding the resource’s implementation and use, and current trends and best practices.

01.03 This document also outlines individual role types (i.e., user, owner, custodian, privileged) and typical responsibilities associated with each type of role.

01.04 Data gathering and security assessment requirements pertaining to the acquisition of information technology (IT) products and services are outlined in this document. These requirements are not intended to be used in lieu of other asset selection procurement procedures, including [UPPS No. 05.02.06](https://policies.txstate.edu/university-policies/05-02-06.html), Acquisition of Information Technology Products and Services. Rather, these requirements provide additional information pertaining to proactive risk mitigation measures that function within the overall procurement process for such information resources.

01.05 Terms included in this policy have the meaning ascribed in the [Information Security Glossary](https://infosecurity.txstate.edu/work/information-security-glossary.html) if included in the glossary and not explicitly defined otherwise.

01.06 Statements in this policy reference standards, procedures, and guideline documents published on the [Information Security Office’s (ISO) website](https://infosecurity.txstate.edu/). Such documents are to be considered as authoritative as the respective statement in this policy. Due to their technical, operational, and detailed nature, contents of such documents require frequent revision and are ill-suited for full inclusion in long-lived policies.

**02. INFORMATION ASSET MANAGEMENT PROCEDURES**

02.01 As stated in Section 01.02 of [UPPS No. 04.01.01](https://policies.txstate.edu/university-policies/04-01-01.html), Security of Texas State Information Resources, Texas State University’s information resources are “strategic and vital assets” that must be available when needed and protected “commensurate to their value” (i.e., category as defined in Section 02.11 f. of this policy). In this policy, the university has identified specific actions required to achieve these objectives. The university has also articulated the owner, custodian, user, and privileged roles to clearly distinguish the parties responsible and accountable for taking those actions, in consultation with the Information Resources Manager (IRM) and the Chief Information Security Officer (CISO).

02.02 Owner Role

 The university (and consequently the state of Texas) is the legal owner of all the university’s information resources. As a practical matter, the university delegates specific ownership responsibilities to those with day-to-day oversight of the information resource. For example, ownership is split for departmental file shares hosted on Technology Resources’ servers in the data center. The shared directories and their logical contents are owned by the department, and the host computer and related disk storage are owned by Technology Resources.

Owners have been designated for information resources based upon the general subject matter of the data. For example, Human Resources and Faculty and Academic Resources are the designated owners of staff and faculty employee information, respectively (see the Data Ownership Guide on the [ISO website](http://infosecurity.txstate.edu/) for more information).

Ownership responsibility for certain information resources, including networks, hardware, and software, is assigned to the party accountable for the resource, as documented in the university’s inventory, procurement, and licensing records. Owners generally occupy director- or higher-level positions that grant oversight of operations within a given area or institutional function (see [UPPS No. 04.01.01](https://policies.txstate.edu/university-policies/04-01-01.html), Security of Texas State Information Resources, Section 03.04). In other cases, the principal investigator for a research grant may be contractually designated as the information owner.

In consultation with the IRM and CISO, owners are specifically responsible for:

a. keeping abreast of laws and policies related to the information resources they own and classifying and categorizing these resources according to their need for security protection (see Section 02.08 and Section 02.11);

b. determining the value of, classification of, categorization of, authorizing user access to, and establishing procedures for authorized disclosure of their information resources;

c. specifying data control requirements for their information resources and conveying those requirements to co-owners, custodians, and users;

d. specifying appropriate controls, based on risk assessment, to protect their information resources from unauthorized use, modification, deletion, or disclosure;

e. selecting and assigning custody of information resources, in consultation with the CISO or appropriate IT staff, to custodians capable of implementing the necessary security controls and procedures. In cases of split custodianship responsibilities, the owner is responsible for ensuring that all custodianship obligations are fulfilled by their respective assignees (e.g., ensuring appropriate infrastructure maintenance for cloud-hosted services and application- and user-level permission management are both fulfilled);

f. contractually binding non-university custodians to implement and comply with security controls deemed commensurate to the classification of university information that will be accessed, transmitted, used, or stored on behalf of the institution and other applicable risks to the institution and its information resources (see [Texas Government Code §2054.138](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm#2054.138));

g. confirming the implementation of and compliance with the specified controls by the custodians;

h. reviewing and maintaining access authorization lists based on documented security risk management decisions. This includes reviewing the access authorization lists for their resources to ensure that authorization is promptly revoked from those whose roles no longer justify the specified access (see [TAC 202.72 (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=72)). Authorization lists reviewed should be comprehensive and include all components of the information resource (e.g., system, application, and database accounts); and

i. reviewing access authorization lists, which shall be conducted on a recurring basis (at least annually). The frequency of review shall be determined by the information owner in consultation with the CISO, or designee, and based on risk assessment methodology. The review must be documented, reviewed, and approved by appropriate owner management. Records necessary to support the reviews shall be maintained and should not contain confidential or sensitive information.

02.03 Custodian Role

 In consultation with the IRM and CISO, custodians provide information asset services to both owners and users. A custodian may be a person (such as a departmental system support specialist), a team or department (such as Technology Resources), or an authorized third-party provider of an information resource (such as a developer or distributor of a cloud-hosted product or service).

Regardless of how the role is filled, custodians are expected to:

a. assist the owner in identifying cost-effective controls, along with monitoring techniques and procedures for detecting and reporting control failures or violations;

b. implement the controls and monitoring techniques and procedures specified by the owner and as specified by university policies, procedures, and standards;

c. provide and monitor the viability of physical and procedural safeguards for the information resources in accordance with the Information Security program;

d. provide appropriate information security training to employees; and

e. ensure information is recoverable in accordance with risk management decisions (see [TAC 202.72 (2)](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)).

02.04 User Role

The user role is the default role possessed by all users of Texas State information resources. Users of information 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 the ISO or other IT units issue in response to specific risks or threats. The use of Texas State information resources implies that the user has knowledge of and agrees to comply with the university’s policies governing such use (see [TAC 202.72 (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=72)).

Employee users are responsible for ensuring the confidentiality and security of the information they access in the normal course of their work. Employees are also responsible for the security of any terminal, workstation, printer, mobile device, or similar electronic device used in the normal course of their work. Employees are authorized to use only those resources and materials that are appropriate, necessary, and consistent with their job functions and must not violate or compromise the confidentiality or security of any data or systems accessible via the university’s information resources (see [UPPS No. 04.01.07](https://policies.txstate.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources, for additional information about acceptable and prohibited uses of Texas State’s information resources).

Except as provided in Sections 02.05 and 02.06, users may not attempt to violate the security or confidentiality of the university’s information resources. The attempted violation of information security or confidentiality is grounds for revocation of computer access privileges, suspension or discharge of employees, suspension or expulsion of students, and prosecution to the full extent of the law.

Users are responsible for the security of any computer account (e.g., NetID or username) issued to them and are accountable for any activity that takes place under 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 the Information Technology Assistance Center (ITAC) for initial investigation. ITAC shall escalate the incident to the ISO if the compromise may increase the risk to other university information resources (see [UPPS No. 04.01.10](https://policies.txstate.edu/university-policies/04-01-10.html), Information Security Incident Management). Any suspected or attempted violation of system security should be reported immediately to ITAC at 512.245.4822 or itac@txstate.edu; or ISO at 512.245.4225 or infosecurity@txstate.edu.

02.05 Privileged Roles

 By virtue of their job duties (e.g., the review and monitoring activities described in Section 02.06), designated employees may require and may be entrusted with elevated access privileges to specified information resources. These employees normally function in custodial or security-related roles with respect to the specified information resources. Users entrusted with elevated access privileges shall:

a. use those privileges solely for the purpose intended by the information resource owner; and

b. access, disclose, and discuss the information only to the extent required to perform the job duty for which the privileges were granted.

02.06 Review and Monitoring

 Texas State’s information resources are subject to review, monitoring, and disclosure, as provided in Section 06. of [UPPS No. 04.01.02](https://policies.txstate.edu/university-policies/04-01-02.html), Information Resources and Access Management. Consequently, users should not expect privacy in their use of Texas State's information resources (see [NIST SP 800-53 AC-8, AR-4](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

02.07 Interagency Operations

 When confidential information from another university or state agency is received by Texas State in connection with the transaction of official business, Texas State shall maintain the confidentiality of the information in accordance with the conditions imposed by the providing agency or university.

02.08 Data Classification

 Prior to releasing, publishing, or disclosing any university information, the designated university owner of the information, in consultation with the IRM and CISO, shall classify the information as public, sensitive, or confidential, according to its need for confidentiality. Moreover, the information resource’s owner should ensure that disclosure controls and procedures are implemented and followed to afford the degree of protection required by the assigned classification. Information shall be assigned one of the following three classifications:

a. Public (Level 1) information is by its very nature designed to be shared broadly, without restriction, at the complete discretion of the owner. It may or may not have been explicitly designated as public. Public information 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 of public information include: advertising and marketing literature, degree program descriptions, course offerings, campus maps, job postings, press releases, descriptions of university products and services, and certain types of unrestricted directory information, as specified by the [Family Educations Rights and Privacy Act of 1974](http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html) (FERPA), the [Health Insurance Portability and Accountability Act](https://www.hhs.gov/hipaa/for-professionals/privacy/) (HIPAA), and the [University Registrar](https://www.registrar.txstate.edu/legislative-policies/ferpa.html).

b. Sensitive (Level 2) information can be difficult to classify as it often presents attributes of both public and confidential information. Sensitive information may be deemed “public” in the sense that, under certain circumstances, disclosure may be required under provisions of the [Texas Public Information Act](https://comptroller.texas.gov/about/policies/open-records/public-information-act.php) (TPIA). However, the disclosure of sensitive information also requires 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 may be controlled by identity authentication and authorization measures (e.g., NetID and password). Unauthorized disclosure of sensitive information could adversely impact the university, individuals, or affiliates.

Examples of sensitive information include: some employee records (such as performance appraisals, home address, home telephone number, and personal email addresses), departmental policies and procedures that might reveal otherwise protected information, the contents of email, voice mail, instant messages and memos, unpublished research, information covered by non-disclosure agreements, and donor information.

Generally speaking, sensitive information should not be published or disclosed to the public except by the university’s designated owner of the information in accordance with the owner’s established practices, or after consultation with The Texas State University System (TSUS) associate general counsel and the Public Information Coordinator (PIC) (see the Data Ownership Guide on the [Information Security website](http://infosecurity.txstate.edu/) for more information).

c. Confidential (Level 3) information is defined by [TAC 202](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202) to be “information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement,” such as the [TPIA](https://comptroller.texas.gov/about/policies/open-records/public-information-act.php) and [FERPA](http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html).

Confidential information is generally intended for a very specific purpose and shall 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](https://comptroller.texas.gov/about/policies/open-records/public-information-act.php), [FERPA](https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html), [HIPAA](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html)), contract agreements, published opinions by the Office of the Attorney General of Texas, and the TSUS [Rules and Regulations](https://www.tsus.edu/about-tsus/policies.html). Unauthorized disclosure of this information could have a serious, adverse impact on the university, individuals, or affiliates, and presents the most serious risk of harm if improperly disclosed.

Examples of confidential information include: student education records, as defined under [FERPA](https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html), personally-identifiable medical records, passport information, crime victim information, library transactions (e.g., circulation records), court-sealed records, individually identifiable biometric information, individually identifiable location information gathered via Global Positioning System (GPS) technology, and access control credentials (e.g., PINs, passwords, and multi-factor authentication devices). Confidential information also includes any of the following when combined with other personally-identifying information: social security number, driver’s license number or other government-issued identification number, date of birth, payment cardholder information, or financial account information (see [Business and Commerce Code Chapter 521, Unauthorized Use of Identifying Information](https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm)).

Confidential information must not be disclosed to the public under any circumstances other than those specifically authorized by law. Any such disclosure should be immediately reported to the Information Security Office for incident mitigation and investigation (see [UPPS No. 04.01.10](https://policies.txstate.edu/university-policies/04-01-10.html), Information Security Incident Management). Requests for such information received from persons with a questionable need to know should be directed to the TSUS associate general counsel.

02.09 Standards for Handling Sensitive and Confidential Information

 Because of the harm that can result from improper disclosure, sensitive and confidential university information shall be afforded the special protections by owners, custodians, and users as detailed in the institutional standard “[Standards for Handling Sensitive and Confidential Information](https://infosecurity.txstate.edu/work/spg/standards-information-management.html)” published on the Information Security Office’s website.

02.10 Transfer, Disposal, or Destruction of Information Assets

 The sale, transfer, or disposal of old, obsolete, damaged, nonfunctional, or otherwise unneeded electronic devices and media pose information risks for the university. These risks are related primarily to the contents of storage media within these devices, which may expose sensitive or confidential information, licensed and non-transferable software, copyrighted intellectual property, or other protected information. Modern computer forensic techniques may allow for the recovery of data even after it has been moved, deleted, wiped, or otherwise logically removed from a storage device.

Under [Texas Government Code §2054.130](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2054.htm#2054.130), state agencies and institutions of higher education are required to permanently remove data from data processing equipment before disposing of or otherwise transferring the equipment to an entity that is not a state agency or other agent of the state. The Texas Department of Information Resources (DIR) recommends that “state agencies shall assess whether to remove data from any associated storage device. Electronic state records shall be destroyed in accordance with [§441.185, Government Code](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.441.htm#441.185)” (see [NIST SP 800-53 MP-7](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

Owners, custodians, and users shall contact ITAC for media sanitization assistance prior to transferring ownership or otherwise disposing of any magnetic media (e.g., hard disk drives, USB drives, backup tape cartridges, DVDs, CDs, etc.) or any devices containing such media (e.g., computers, laptops, PDAs, tablets and smart phones, printers, copiers, etc.). ITAC will securely sanitize or destroy the media, at its sole discretion, and maintain appropriate records of the action taken (see [UPPS No. 05.01.02](https://policies.txstate.edu/university-policies/05-01-02.html), University Surplus Property (Equipment and Consumable Supplies), for additional information regarding proper disposal procedures).

Owners, custodians, and users shall not repurpose or reassign any electronic device or electronic media contained within a device without first fully sanitizing the media using a tool sanctioned by the CISO, or designee. Reformatting the media does not constitute, by itself, a satisfactory sanitization process.

02.11 System Categorization and Impact Designation

1. Prior to implementing, using, or configuring any university information system, the designated university owner of the system, in consultation with the IRM and CISO, shall categorize the information system based on the institutional impact of an incident affecting the confidentiality, integrity, or availability of the information system or the university information stored, processed, or transmitted by the information system.
2. The owner of the information system and related information resources should ensure that appropriate controls and procedures are implemented and followed to afford a degree of protection that is commensurate to the system’s category and subsequently, the potential impact of an incident affecting the system and effects to the institution.
3. Impact values used to categorize an information system are different than those used to describe actual incidents, as detailed in [UPPS No. 04.01.10](https://policies.txstate.edu/university-policies/04-01-10.html), Information Security Incident Management, Section 02.03. More granular impact values are used in system categorization in order to better inform institutional planning and risk management based on probable scenarios and applied safeguards.
4. The institutional impact of a potential incident that could affect an information system or university information it stores, processes, or transmits shall be classified by one of five values. Care should be exercised to consider the institutional perspective rather than the effects on an individual team or user.

An institutional standard, “[Standards for System Categorization](https://infosecurity.txstate.edu/work/spg/standards-system-categorization.html),” has been published and contains the criteria used to determine information system impact values.
5. Three separate impact values shall be determined for each information system. Each impact value assesses the institutional impact of an incident affecting, respectively, the confidentiality, integrity, and availability of the system or the information it stores, processes, or transmits. Further descriptions of these impact values are available in the institutional standard "[Standards for System Categorization](https://infosecurity.txstate.edu/work/spg/standards-system-categorization.html)."
6. The highest of the three impact values for each information system will determine the category of the information system:

|  |  |
| --- | --- |
| **Impact Value** | **System Category** |
| Severe (5) | Essential (V) |
| Major (4) | Critical (IV) |
| Moderate (3) | Moderate (III) |
| Minor (2) | Low (II) |
| Insignificant (1) | Insignificant (I) |

1. A table providing a translation between institutional system categories and the three-tiered definitions specified in [TAC 202.1 (15), (25), and (26)](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=1), is included in the institutional standard “[Standards for System Categorization](https://infosecurity.txstate.edu/work/spg/standards-system-categorization.html).”

**03. COMMUNICATIONS AND OPERATIONS MANAGEMENT PROCEDURES**

03.01 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) shall be employed to accomplish this objective (see [NIST SP 800-53 SC-8](http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf)).

03.02 For on-campus wireless network access, Technology Resources shall establish and maintain a wireless network for use on the university campus. The specific technologies used to establish these networks shall be established in consultation with the CISO, or designee.

03.03 To facilitate security of the campus network, owners, custodians, and users of information resources shall adhere to the provisions of [UPPS No. 04.01.05](https://policies.txstate.edu/university-policies/04-01-05.html), Network Use Policy.

03.04 Owners of distributed information 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 202.70](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 [NIST SP 800-53 PE](http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf)).

**04. ACCESS CONTROL PROCEDURES**

04.01 Prior to obtaining access to the Texas State 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., NetID or Texas State ID number) and its corresponding “secret” (e.g., a password, PIN, smartcard, or token) shall be used to accomplish the authentication. Based upon security risk assessment, information resources that contain sensitive or confidential information may require the use of multi-factor authentication where one factor is provided by a device separate from the computing device gaining access. 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 (see [NIST SP 800-53 AC](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

Based upon security and risk assessments, owners and custodians shall implement and maintain audit trails and transaction logs as necessary to provide accountability on a per-account basis for changes to mission critical information, hardware, software, and automated security or access rules (see [NIST SP 800-53 AC](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

04.02 Self-service systems must incorporate security procedures and controls to ensure data integrity and protection of sensitive or confidential information. Self-service systems must authenticate the identity of individuals that use the systems to retrieve, create, or modify sensitive or confidential information about them (see [NIST SP 800-53 AC](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

04.03 To the extent practicable, all initial login and authentication screens should clearly and prominently display the following user advisory: “Use of computer and network facilities owned or operated by Texas State University requires prior authorization. Unauthorized access is prohibited. Usage may be subject to security testing and monitoring and affords no privacy guarantees or expectations except as otherwise provided by applicable privacy laws. Abuse is subject to criminal prosecution. Use of these facilities implies agreement to comply with the policies of Texas State University” (see [NIST SP 800-53 AC](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

04.04 A user's NetID shall be deactivated whenever the user’s affiliation with the university no longer qualifies the user to possess an active NetID. See [UPPS No. 04.01.02](https://policies.txstate.edu/university-policies/04-01-02.html), Information Resources Identity and Access Management, Section 04.02 e., for specifics regarding the deactivation of employee accounts upon separation from service (see [NIST SP 800-53 AC](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

04.05 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 owner, as described in the Data Ownership Guide on the [Information Security website](http://infosecurity.txstate.edu/) (see [NIST SP 800-53 AC-6](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

04.06 All Texas State information resources that employ passwords for authenticating user identities shall be configured to comply with the sets of standards below (see [NIST SP 800-53 IA](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)):

a. General Requirements – the following criteria apply to all instances where passwords are used for authentication

1) passwords must be case-sensitive;

2) passwords must not be re-used following password resets within the same system or service;

3) password history shall be enforced to the system’s maximum available setting;

4) authentication systems must utilize one-way encryption and, once assigned, the password must not be retrievable by anyone. Thus, when a password is lost or forgotten, the existing password will not be retrieved and instead a new password will be assigned or set by the user;

5) password change logs shall be maintained by custodians who issue passwords. The log entries should reflect the date and time of the password change and the username associated with the changed password, but neither the new nor the old password;

6) passwords must be changed if compromised;

7) authentication systems must support user-initiated, self-service reset processes OR upon creation of user account, a temporary password must be delivered in a confidential manner and be reset upon first log on by the account owner;

8) passwords shall be changeable by their owners at will;

9) passwords should be unique (i.e., a user must not set their NetID password to the same password as their personal email address);

10) passwords should not be set to credentials obtained from previous, known breaches, commonly used passwords, dictionary words, repetitive or sequential characters (e.g., “aaaaaaaa” or “abcd1234”), or context-specific words (including the name of the service, user’s name, or derivatives thereof);

11) information resource owners and custodians may require more frequent password changes based upon risk assessment results; and

12) authentication systems must support the use of special characters in passwords (see [NIST SP 800-63B, Section A.3](https://pages.nist.gov/800-63-3/sp800-63b.html)).

04.07 In addition to the requirements outlined in Section 04.06, authentication systems must also incorporate one of the following standards outlined below:

a. Modern Authentication System Standards – It is the expectation that new information resources will use modern authentication standards and will support multi-factor authentication.

1) passwords must be at least 15 characters in length (though complex passwords and passphrases are strongly encouraged); and

2) services should support multi-factor authentication.

b. Legacy Authentication System Standards:

1) passwords must be at least eight characters in length (though longer passwords and passphrases are strongly encouraged);

2) passwords must include at least one character from at least three of the following four-character sets:

(a) uppercase characters (A, B, C … Z);

(b) lowercase characters (a, b, c … z);

(c) numeric characters (0, 1, 2 … 9);

(d) special characters or symbols (e.g., #, $, %, ^, &, -); and

3) passwords must be changed at least annually.

04.08 In the event that an information resource is incapable of enforcing all requirements for passwords as specified in Sections 04.06 and 04.07, alternative mitigating security controls shall be implemented in place of these requirements with approval from the CISO, or designee.

04.09 Information resources that contain, access, transfer sensitive, or confidential information shall require authentication of user identity prior to granting access to the applications (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 [NIST SP 800-53 AC](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)). Owners of such information resources are responsible for mandating and ensuring fulfillment of this requirement.

04.10 To the extent practicable, all information systems that require users to authenticate their identities should be configured to leverage Single-Sign On (SSO) systems maintained by IT.

04.11 To the extent practicable, all information systems that require users to authenticate their identities should be configured to leverage Multi-Factor Authentication (MFA) systems maintained by IT.

**05. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE PROCEDURES**

05.01 In addition to requirements outlined in [UPPS No. 05.02.06](https://policies.txstate.edu/university-policies/05-02-06.html), Acquisition of Information Technology Products and Services, many IT products and services to be used by the university must undergo assessment by the ISO prior to acquisition. These resources include, but are not limited to, software, hosting services, cloud-hosted products and services, and some non-standard hardware acquisitions.

Factors that influence the applicability and scrutiny of such assessments are based primarily on the classification of information involved, impact designation and category of the information system or component, and potential risks to other university information resources. The monetary cost of an IT product or service is not a significant factor in this decision, meaning any university acquisition of IT products or services, including acceptance of free or no-cost items, may be subject to this policy.

1. Information systems and information system components that meet one or more of the following criteria will be subject to additional scrutiny and background information gathering requirements in order to better assure the confidentiality, integrity, and availability of Texas State’s information and information resources.

	1. The information system or system component is intended to process, store, or otherwise transmit institutional data.
	2. The information system or system component is intended to be accessed via the internet.
	3. The information system or system component has been determined to present significant potential risk to university information resources.
2. As a matter of practicability, insignificant-, low-, and some moderate-impact information systems and information system components are generally not subject to rigorous forms of this assessment except in extraordinary circumstances, such as scenarios in which centralized, operationalized controls will not be available or other exceptions to normal operations are required. For example:
	1. ISO assessment is not required prior to a department’s purchase of a new laptop for employee use via acquisition and deployment processes managed by ITAC; however, an assessment would be required for the acquisition of networking hardware intended to be deployed or managed by personnel other than authorized IT staff.
	2. Similarly, rigorous ISO assessment would generally not be required prior to the purchase of additional licenses of locally installed software that has been previously assessed and determined to pose an insignificant or low level of risk to the institution; however, a security assessment would be required for new applications and for cases in which the use case or service delivery model has significantly changed (e.g., transitioning from software installed on individual workstations or hosted in a university data center to a cloud-only service offering).

05.02 A security assessment of an information resource (i.e., information system or information system component) must be performed by the CISO, or designee. This process must be completed before such information resources will be authorized for acquisition, procurement, renewal, new or continued use, proofs of concepts, demonstrations, trials, or exposure to institutional data.

a. The level of scrutiny applied to an information resource during a security assessment is influenced by several factors, including:

1. the type of information resource (e.g., information system, information system component, locally installed applications, cloud-hosted Software as a Service (SaaS)) under assessment;
2. the security categorization of the information resource;
3. the classification of institutional data processed, stored, or otherwise transmitted by the information resource;
4. whether the information resource is a cloud computing service, as defined by [NIST SP 800-145](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf), and whether the cloud computing service is determined to be within the scope of the Texas Risk and Authorization Management Program (TX-RAMP) as specified by the DIR;
5. the intended scope of use described by the information resource owner and custodian; and
6. whether business justification provided by the information resource owner and custodian is commensurate to the qualities of the information resource (e.g., the degree to which the resource contributes to institutional goals; whether risks associated with the use of redundant systems or system components outweigh incremental benefits to the institution).

b. Factors that influence the level of scrutiny applied during a security assessment also influence the information required about the item under assessment. Information required to conduct the security assessment of an information resource must be submitted in a timely fashion to the Information Security Office in order to facilitate the assessment.

Specific information required to conduct security assessments is published in the institutional standard “[Standards for Pre-Procurement Security Assessment](https://infosecurity.txstate.edu/work/spg/standards-preprocurement-assessments.html).”

1. Under [Texas Government Code §2054.0593](https://statutes.capitol.texas.gov/SOTWDocs/GV/htm/GV.2054.htm#2054.0593), cloud computing services within the scope of the TX-RAMP must attain and maintain the appropriate level of TX-RAMP certification from the DIR prior to any acquisition or re-acquisition of such services.

In addition to procurement and acquisition restrictions, a failure to attain or maintain the appropriate level of TX-RAMP certification may result in the revocation of authorization to continue using a cloud computing service independent of its respective contract or procurement status (e.g., months or years remaining in a contract, remainder of an annual subscription).
2. While required for many cloud computing services, TX-RAMP certification does not guarantee ISO authorization or exempt an information system or system component from the requirements of this or other policies. Similarly, cloud computing services that are not in scope of the TX-RAMP must still undergo assessment by the ISO prior to authorization.

e. The following statement is only valid during the period of time TX-RAMP provisional certification status may be requested (i.e., January 1, 2022, to January 1, 2023):

TX-RAMP provisional certification status will be requested as necessary from the DIR by the CISO, or designee, on behalf of the institution only for cloud computing services within scope of the TX-RAMP that were assessed and authorized by the ISO prior to January 1, 2022.

Request of provisional certification status is conditioned upon

1) the information resource owner accepting the risks and obligations associated with the subject cloud computing service not attaining sufficient TX-RAMP Certification by the DIR within the TX-RAMP provisional certification status window; and

2) whether information from the prior assessment of the cloud computing service is deemed satisfactory by the CISO, or designee, for the category of the system and the classification of institutional data it will store, process, or transmit.

Cloud computing services within scope of the TX-RAMP that have not been assessed and authorized by the ISO on or prior to January 1, 2022, must obtain the commensurate level of TX-RAMP certification prior to ISO consideration for assessment. Exceptions to this requirement as it pertains to new (unassessed) cloud computing services shall not be granted except under extenuating circumstances and deemed essential to university operations and authorized by the vice president of IT.

f. Prior to renewal or reimplementation of existing systems that have not undergone the security assessment process, appropriate CISO-led assessment measures shall be taken at the discretion of the CISO, or designee.

g. At the discretion of the CISO, or designee, renewals and continued use of “grandfathered” systems that have been determined to present acceptable levels of risk may be authorized, contingent on the completion of a formal security assessment and absent other factors outlined above (e.g., requirements for TX-RAMP certification).

h. The continuance of authorization for renewals and continued use of such “grandfathered” information systems and system components is not perpetual. Reassessment of information systems and information system components will be required on a basis determined by the CISO, or designee.

05.03 In addition to ordinary security assessment procedures, prior to acquiring, implementing, using, renewing or freely accepting any cloud computing service (as defined by [NIST SP 800-145](https://csrc.nist.gov/publications/detail/sp/800-145/final)) to store, transmit, or process any institutional data, a determination must be made as to whether a contract shall be established that includes the Information Security & Accessibility Standards Exhibit ([ISASE](https://gato-docs.its.txst.edu/jcr%3A73f7f5f3-724e-421b-a1f7-3db1d6d9f00c/Information%20Security%20Standards%20Exhibit%20.pdf)).

05.04 Test functions shall be kept either physically or logically separate from production functions. Copies of production data shall not be used for testing unless all personnel involved in testing are authorized access to the production data or all confidential information has been removed from the test copy (see [NIST SP 800-53 SC](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

05.05 Appropriate information security and audit controls shall be incorporated into new systems. Each phase of systems acquisition or development shall incorporate corresponding development or assurances of security controls. The movement of system components through various life cycle phases shall be tracked, and, more specifically, the movement of any software component into production shall be logged (see [NIST SP 800-53 SA](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)).

05.06 After a new system has been placed into production, all program changes shall be authorized and accepted by the system owner, or designee, prior to implementation (see [NIST SP 800-53 SA](https://gato-docs.its.txst.edu/jcr%3A9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf)). The system owner’s authorizations to make changes and acceptances of those changes shall be documented and maintained.

05.07 To the extent practicable, the principles of separation of duties and least privilege shall be applied to the system development, acquisition, and production life cycle. For example, the developer or maintainer of a component should not also have the ability to place the component into production.

05.08 Modifications to production data by custodians or developers shall be authorized in advance by the system owner. If advanced 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 documented. 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.

05.09 Owners and custodians shall ensure that new and modified web applications are compliant with Technology Resources’ web application development standards prior to their production deployment.

**06. RISK ASSESSMENT PROCEDURES**

06.01 Risk assessment is a vehicle for systematically identifying and evaluating the vulnerabilities of and threats to an information resource. Risk assessment is an essential component of any security and risk management program. Absolute security must assure protection against all threats. Risk assessment provides a framework for weighing losses that might occur in the absence of an effective security control against the costs of implementing the control. Risk management is intended to ensure that reasonable measures are employed to protect against the most probable and impactful threats.

06.02 Owners and their designated custodians shall complete risk assessments as provided by the CISO, or designee, most often occurring biennially, depending on the classification of data or the information resource and category of the information system or system component. The scope of this assessment may include departmentally-administered information resources that store, process, or access information in addition to information resources administered by IT.

The assessment should identify reasonable, foreseeable, internal, and external risks to the security, confidentiality, integrity, and availability of those resources. Owners and custodians should assess the sufficiency of safeguards in place to control these risks and take mitigating measures to protect the resources from unacceptable risks. They should also document their acceptance of residual risk (i.e., the exposure remaining after implementing appropriate protective measures, if any). The risk assessment should also include consideration of employee training and management, information systems architecture and processes, business continuity planning and prevention, and detection and response to intrusion and attack. The assessment results shall be documented in a written report, protected from unauthorized disclosure, modification, or destruction, and retained until superseded by a subsequent documented assessment (see [TAC 202.73](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)).

06.03 Owners may opt to commission additional risk assessments as necessary. For example, the Student Health Center may commission a third party to conduct a risk assessment pertaining to [HIPAA](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html) compliance in addition to recurring, CISO-led assessments. Third-party risk assessors are subject to evaluation by the CISO, or designee.

06.04 The CISO, or designee, shall periodically (at least biennially) complete or commission a risk assessment of the information resources considered essential to the university's critical mission and functions and shall recommend to the owners and 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 shall be provided to the owners and custodians of the information assets.

06.05 The CISO shall periodically (at least annually) report on the adequacy and effectiveness of security controls and residual institutional risks to information resources (see [TAC 202.73(a)](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=73)). This report shall be presented to the president and President’s Cabinet.

**07. REVIEWERS OF THIS UPPS**

07.01 Reviewers of this UPPS include the following:

Position Date

Chief Information Security Officer Sept 1 E2Y

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