**Information Resources Identity UPPS No. 04.01.02**

**and Access Management Issue No. 10**

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

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

**Sr. Reviewer: Associate Vice President for Technology Resources**

**POLICY STATEMENT**

*Texas State University is committed to maintaining appropriate information resources identity and access management.*

**01. BACKGROUND INFORMATION**

 01.01 Information resources residing at or administered by Texas State

University are strategic and vital assets belonging to the people of Texas. [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 university to appropriately manage access to these information resources. Texas State shall afford an individual access to these resources in a manner consistent with the individual’s institutional affiliations and roles. Individuals shall access these resources only as necessary to fulfill their institutional roles and always in compliance with established laws, regulations, policies, and controls. The university shall hold individuals accountable for their actions relating to such access (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 202.71](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)).

01.02 This policy applies to all Texas State information resources and to all individuals whose affiliation with Texas State requires or permits their access to those resources, without regard to the manner, form, or location of access.

**02. DEFINITIONS AND RESPONSIBILITIES**

02.01 Account – a relationship between an information resource (e.g., computer, network, or online service) and a user of that resource. The university assigns and administers a variety of account types, the vast majority being individual user domain accounts. In this policy, the term account refers to accounts of all types, unless a specific type is referenced. The university account types include the following:

1. Authentication-Only Account – issued to convey domain-authenticated, application-level information resource access. Typically, these accounts are created for individuals with limited access needs to web-based application information resources.
2. Domain Account – assigned to a single, authorized individual to facilitate access to the Texas State network domain and information resources within that domain; the owner of an individual user domain account is the only authorized user of that account;

c. Group and Shared Accounts – have more than one authorized user. Individual accountability is often difficult to ascertain with group accounts. Consequently, group accounts present additional management challenges and should be employed only in low risk or team support situations (e.g., service and privileged accounts). The administrative head of a unit with a group account must establish procedural controls consistent with the risk posed by improper use of the account. Examples of such controls include the maintenance and frequent review of separate activity logs and diligent management of group membership;

d. Privileged (or Super User) Account – assigned to a single university employee for use in administering university information resources;

e. Resource Account – assigned to a specific resource (e.g., meeting room) rather than an individual or group of individuals; resource accounts facilitate the reservation and use of shared resources; and

f. Service Account – assigned to a specific information resource or resource group to facilitate services by an external support provider (a support service account) or to authenticate one system or resource to another (a system service account). Service accounts shall be unique to the applicable resource or resource group. Support service accounts shall be enabled only after notice to the information resource owner and only for the duration of an active maintenance engagement.

02.02 Account Owner – the individual to whom an account is assigned, generally represented by a network identifier (NetID) or username. University affiliation (see Section 03.) determines account eligibility. Knowledge of the account’s password and other related personally identifiable information (PII) demonstrates account ownership. The account owner is the only authorized user of the account and is responsible for all computing and network activities attributable to that account. For group accounts, the administrative head of the unit to which the account is issued owns the account. As such, the administrative head shall authorize group membership and hold group members accountable for their use of the account (see also Section 02.01 c.).

02.03 Affiliation – an association between an individual and the university (e.g., student, faculty member, employee, guest, etc.). Individuals may enjoy multiple concurrent affiliations with the university.

02.04 Identity and Access Management (IAM) – the policies and processes that identify individual users and control access to information resources.

02.05 Information Resources – Texas State’s information resources are explicitly defined in [UPPS No. 04.01.07](http://policies.txstate.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources. Most Texas State information resources are non-public, meaning that the university must first validate an individual’s identity and university affiliation before affording the individual access to the resources. Unless specifically stated otherwise, the phrase “information resources” in this policy refers to the university’s non-public information resources. Examples of non-public information resources include the university’s encrypted wireless network and its electronic mail system. Examples of public resources include the university’s open wireless network, which allows general internet access, and public kiosks within the Alkek Library.

02.06 Information Technology Assistance Center (ITAC) – an information technology services organization that provides the university’s user community with a variety of technology support services, including user authentication (e.g., account creation, activation, and deactivation) and authorization (e.g., user role assignment and revocation).

02.07 Multi-Factor Authentication (MFA) – a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

02.08 Network Identifier (also known as NetID or Username) – a unique identifier assigned by the university to an account and its owner. The NetID is used with its associated password to authenticate the account owner’s identity when accessing Texas State information resources (see Section 05. for additional specifics regarding NetID assignment and administration).

02.09 Password – a character string associated with an account and known only to the account owner, used to prove identity or gain access to an information resource. Presenting the account’s NetID and password proves (or authenticates) the NetID owner’s identity (see Sections 04.06 and 04.07 in [UPPS No. 04.01.11](https://policies.txstate.edu/university-policies/04-01-11.html), Risk Management of Information Resources, for more information about password creation and management).

02.10 Role – a defined set of access privileges, generally associated with a user’s responsibilities or position within an organization or group, which defines the tasks a user can perform. Many automated functions and online services require more finely-tuned access controls than the university’s identification and authentication credentials can afford. In such situations, the designated owner or application administrator should employ additional authorization controls, such as role definitions and assignments, to determine and enforce the access and activity controls applicable to an authenticated user.

02.11 Semester – one of three periods of instruction during the academic year, identified as fall, spring, and summer, each of which ends with its last commencement date and begins with the day immediately following the last commencement date of the prior period.

02.12 Texas State ID Number – a unique and permanent university identifier that identifies an individual within the university’s identity repository and other internal university databases. The Texas State ID number is used in conjunction with other PII to assert the owner’s identity with a limited set of university information resources.

**03. AFFILIATION ELIGIBILITY**

03.01 User Affiliations

 Texas State provides restricted access to its information resources to persons with the following university affiliations:

a. students (as described in Section 04.01);

b. faculty members (as described in Section 04.02);

c. regular and non-student, non-regular-staff employees (as described in Section 04.02);

d. retired faculty, administrators, and staff (as specified in [UPPS No. 04.04.53](http://policies.txstate.edu/university-policies/04-04-53.html), Honors and Benefits for Retired Faculty and Staff);

e. consultants and contractors (as described in Section 04.03);

f. regents, administrators, staff, and other members of The Texas State University System (TSUS) administration (as described in Section 04.04);

g. guests (as described in Section 04.05); and

h. authentication-only users (as described in section 04.06).

Individuals may possess multiple concurrent university affiliations (e.g., a staff member enrolled in courses is also a student affiliate). The scope of authorized access and use will vary over time in accordance with the user’s affiliations.

03.02 In accordance with this policy, ITAC will make the initial determination regarding an individual’s eligibility to obtain or retain an active Texas State account. In appropriate situations, software administered by Technology Resources automates these processes for ITAC. ITAC will escalate cases where eligibility is disputed or unclear to the associate vice president for Technology Resources or the vice president for Information Technology (VPIT) for review and resolution.

03.03 The university has established procedures for verifying the identity and affiliations of persons seeking to access and use university information resources. Section 04. describes responsibilities for these procedures, which vary according to the person’s purported affiliation. The university shall revoke a person’s access to a university information resource when the person no longer has an affiliation that is eligible to use that resource. The university automatically and periodically validates the eligibility of all users with official university sources, such as faculty and staff personnel records and student enrollment records. The university may use other sources, when necessary, to accurately assess the status of a person’s ongoing affiliation.

03.04 Unless eligible through another affiliation, Texas State alumni are not eligible to maintain an active university NetID for use in accessing the university’s information resources. Texas State alumni may forward emails from their official university address to an alternate email address at their own risk. The university cannot guarantee and is not responsible for the delivery or protection of emails forwarded from the official university address to any other address. Individuals who forward university emails assume personal responsibility for their timely delivery and their protection from improper disclosure once it leaves the university network.

**04. PROCEDURES FOR AFFILIATION-SPECIFIC CONDITIONS AND RESTRICTIONS**

04.01 Students

Students are eligible to use information resources for the duration of their enrollment. Eligibility is based on information present in the university’s student information system or an authorized department or program equivalent approved by the associate vice president for Technology Resources.

1. Organizations that admit students into university educational programs that require or expect students to access the university’s information resources shall, as part of their intake process:
2. verify the identity of the students they admit;
3. ensure that the identifying information of each admitted student is recorded in the university’s identity database; and
4. obtain and securely issue an official Texas State ID number for each student they admit.

 Examples of such organizations include Undergraduate Admissions, The Graduate College, Distance and Extended Learning, and Continuing Education.

1. New students create and activate their domain accounts through a self-service process. Students with deactivated domain accounts use the same process to reactivate their domain accounts. Students who cannot validate their identity through the self-service process must contact ITAC to have their identities validated before the account can be accessed.
2. Students generally retain their eligibility at the end of a semester with the expectation of continued enrollment for the ensuing semester. The university will deactivate the account of any student who fails to enroll over the course of three consecutive semesters, unless the student has a current non-student affiliation (e.g., holds faculty, staff, or retiree status).

04.02 Faculty and Staff

 Faculty and staff employees with current appointments (either paid or unpaid), or agreements for impending employment, are eligible to use the university’s information resources.

1. Eligibility must be supported by official employment records maintained by Faculty and Academic Resources or Human Resources, as appropriate to the position. Organization heads shall notify Faculty and Academic Resources or Human Resources, as appropriate, about personnel changes in a timely manner.
2. ITAC generates domain accounts for new faculty and staff in response to completed online [NetID requests](https://tim.txstate.edu/netidrequest/Home/tabid/2046/ctl/Login/Default.aspx?returnurl=%2fnetidrequest%2fHome.aspx) from hiring departments and Human Resources.
3. Hiring departments, Faculty and Academic Resources, and Human Resources must verify new faculty and staff identities as part of their hiring processes and prior to requesting domain accounts for new hires.
4. A domain account may be activated based on impending employment. In the event employment is denied prior to the anticipated start date, it is the responsibility of the hiring department to contact ITAC to request immediate deactivation. Hiring departments, Faculty and Academic Resources, and Human Resources must establish up-to-date employment records for the employee prior to 45 days beyond the anticipated start date to prevent automatic deactivation of the account. There is no retention guaranteed of user or account specific data for expired domain accounts (see Section 05.08).
5. Generally speaking, faculty and staff employees retain their eligibility until official employment records indicate that their employment with the university has ceased, and they have no other authorized affiliation with the university. Because employment separation transactions may be processed after the official separation date, and to ensure that separating employees do not retain access beyond that date, department heads shall notify ITAC of any separating faculty or staff prior to their official separation date, as directed in [UPPS No. 04.04.50](http://policies.txstate.edu/university-policies/04-04-50.html), Separation of Employment and Interdepartmental Transfers.

04.03 Consultants and Contractors

 Consultants and contractors are eligible to use the university’s information resources as specified in and restricted by their contracts, federal and state law, this policy, and other applicable university policies.

1. The applicable Texas State department contract administrator shall ensure that the relevant contracting documents include appropriate provisions for mitigating risk to university information accessible to consultants, contractors, and other external parties under the contract. The Office of the VPIT provides sample, non-disclosure agreements and data security and privacy provisions, along with guidance and assistance in their use.
2. The university shall assign each individual consultant or contractor an individual domain account that is unique to that user and active for the duration of the contract. The department contract administrator shall request consultant or contractor domain accounts from ITAC at least 10 business days before the accounts will be needed. The request shall include:
	1. the sponsor’s and sponsor’s supervisor NetIDs;
	2. the expected activation period (start and end dates) for the account, which should not begin before nor extend beyond the expected duration of that individual’s participation in contract activities;
	3. a business justification stating the intended use and function of the account by the contractor or consultant user; and
	4. required PII for each contractor or consultant.
3. The department contract administrator shall immediately notify ITAC whenever a consultant or contractor ceases to need access to the university’s information resources.
4. ITAC will set the domain accounts of consultants and contractors to expire upon the expected completion date of the contract or one year from issuance, whichever comes sooner. The department contract administrator is responsible for renewing the domain accounts of consultants and contractors through ITAC prior to their expiration date.

04.04 Members of the TSUS Administration

 Members of the TSUS Board of Regents and members of the TSUS administration staff are eligible to use the university’s information resources for the length of their TSUS affiliation.

1. ITAC assigns domain accounts to these individuals upon request from the assistant to the chancellor, or designee. In submitting the request, the assistant to the chancellor, or designee, affirms the identities of the persons named in the request.
2. Unless directed otherwise by the VPIT, TSUS Board of Regents domain accounts will expire at the end of a board member’s current term. TSUS administration staff domain accounts will expire annually. The assistant to the chancellor shall notify ITAC whenever a TSUS account owner ceases to need access to information resources, such as when a TSUS staff member separates from employment.

04.05 Guests

 Texas State may assign guest domain accounts to individuals not otherwise affiliated with the university if the accounts are required to support functions directly associated with the university mission. A current faculty or staff account owner must sponsor each guest user.

a. Sponsors must ascertain the guest user’s identity and affirm their intent to serve as the university contact regarding issues associated with the guest user’s access and use of information resources.

1. Sponsors should request guest accounts or provide ITAC with advance notice of an impending need for guest accounts, at least 10 business days before the accounts are needed. When requesting or renewing guest accounts, the sponsor will include:
	1. the sponsor’s and sponsor’s supervisor NetIDs;
	2. the expected activation period (start and end dates) for the account;
	3. a business justification stating the intended use and function of the account by the guest user; and
	4. required PII for the guest;
2. ITAC will ensure that guest domain accounts are set to expire no more than one year from the date of request or the end of the expected activation period, whichever comes sooner. The sponsor shall notify ITAC of the need:
	1. for an extension of their guest’s account at least 10 business days prior to the account expiration date; and
	2. whenever a guest account owner ceases to need their account for access to the university’s information resources.

Guest domain accounts are granted basic network access only. Entitlement to services beyond basic network access are at the discretion of the resource owner and subject to all applicable university policies, licensing agreements, and state or federal statutes.

04.06 Authentication-Only Users

 Texas State may assign authentication-only domain accounts to individuals requiring limited access to application resources in support of functions directly associated with the university mission. This access is intended to exclude access to network or domain device resources. A designated faculty or staff account owner must sponsor each authentication-only user.

1. Sponsors must ascertain the authentication-only user’s identity and affirm their intent to serve as the university contact regarding issues associated with the user’s access and use of information resources.
2. Sponsors should request authentication-only accounts or provide ITAC with advance notice at least 10 business days before the accounts are needed. When requesting or renewing authentication-only accounts, the sponsor will include:
3. the sponsor’s and sponsor’s supervisor NetIDs;
4. the expected activation period (start and end dates) for the account;
5. a business justification stating the intended use and function of the account by the authentication-only user; and
6. required PII for the authentication-only identity.
7. ITAC will ensure that authentication-only accounts are set to expire no more than one year from the date of the request or the end of the expected activation, whichever comes sooner. The sponsor shall notify ITAC of the need:
8. for an extension of the authentication-only account at least 10 business days prior to the account expiration date; and
9. whenever an authentication-only account owner ceases to need their account for access to the university’s information resources.

Authentication-only domain accounts are granted application-level authorizations separately. Entitlement to services beyond application authentication are at the discretion of the resource owner and subject to all applicable university policies, license agreements, and state or federal statutes.

**05. USER ACCOUNT AND NETID ADMINISTRATION PROCEDURES**

05.01 Technology Resources shall utilize a university standard naming convention in constructing account NetIDs in order to assure their uniqueness and suitability as identifiers. Account owners may not specify or personally choose their NetIDs. The university permanently and irrevocably assigns the NetID to the account owner and will never re-assign that same NetID to another domain account owner except where appropriate for accounts designated as group, shared, and resource accounts (see Section 02.01).

Individuals may not possess more than one concurrently active NetID. Technology Resources will issue a replacement NetID to an account owner if, and only if, the existing NetID represents a credible danger to the health or safety of the account owner.

05.02 The university will track each domain account assignment using either the account owner’s Texas State ID number or the account sponsor’s NetID or Texas State ID number.

05.03 Only the owner of an individual domain account is authorized to know and use the password for that domain account and may not disclose the password to another party. No university component, employee, representative, or agent may ask the owner of a Texas State domain account to divulge their password.

05.04 Whenever the university newly activates or reactivates a domain account, it will randomly generate a new, pre-expired password for the associated NetID to force a password change by the account owner upon initial login.

05.05 Account owners shall affirm their knowledge and understanding of their responsibilities relative to information security and the appropriate use of information resources each time they change their account password.

05.06 Authorized Information Technology personnel may unilaterally suspend or block access by an account when, in their professional judgment and in the course of their assigned duties, such action is necessary to:

a. protect the confidentiality, integrity, availability, or functionality of university information resources;

b. protect the university from harm or liability; or

c. prevent use or abuse of the account by a person or persons other than the account’s legitimate owner.

Authorized Information Technology personnel may block access to a domain account without advance notice when presented with a written request from appropriate university authorities, the department head of an employee’s organizational unit, or the sponsor of the account. Reasons for such a block include involuntary employee termination, elevated concern for the security of information resources, and reasonable belief that the account is being used in activities that are prohibited by applicable law, [TSUS Rules and Regulations](https://www.tsus.edu/about-tsus/policies.html), or university policy.

05.07 The university will deactivate the domain accounts of individuals who, based upon an automated review of the account owner information from its official information sources, no longer qualify for ownership of a domain account under the terms of this policy. Owners of deactivated domain accounts must re-validate their identity and possess an eligible university affiliation before they may reactivate their NetID and regain access to the university’s information resources.

05.08 The university may delete, without any notification or recovery obligation, files or other information resources attributable to any domain account that is in a deactivated state and no longer possesses an eligible university affiliation.

**06. PROCEDURES REGARDING ACCOUNT ACCESS WITHOUT CONSENT**

06.01 The university generally prohibits access to electronic records and communications by anyone other than:

a. the designated owner of the account or electronic resource containing the records or communication; or

b. the sender or recipient of a particular communication without prior consent from the applicable account owner, sender, or recipient. However, as a Texas public institution, the university must monitor, review, and disclose electronic records and communications stored or transmitted using the university’s information resources as necessary to:

* 1. comply with the provisions of the [Texas Public Information Act](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm), other pertinent laws, [TSUS Rules and Regulations](https://www.tsus.edu/about-tsus/policies.html), and university policies;
	2. satisfy other legal obligations, such as subpoenas and court orders;
	3. protect and sustain the operational performance and integrity of university information systems and business processes;
	4. facilitate security reviews, audits, and investigations by authorized individuals in the performance of their assigned duties; and
	5. protect and support the legitimate interests of the university and other users, as determined by the VPIT, in consultation with the TSUS associate general counsel.

Users of the university’s information resources expressly consent to monitoring and review by the university for these purposes. If such monitoring or review reveals evidence of possible criminal activity, university administration may provide that evidence to law enforcement officials without notice to the user. Further, all users should understand that while the university takes reasonable precautions, as evidenced by its information security program, it is unable to guarantee the protection of electronic files, data, or emails from unauthorized or inappropriate access or disclosure.

Consequently, consistent with [TAC 202.76](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=76), users should not expect privacy in their use of Texas State information resources.

06.02 Individuals seeking non-consensual access to electronic records or communications residing within a user account or university information resource assigned to another user shall make such requests in writing to the VPIT. The requests must fully describe the requested records by type and date and must specify the authorization (see Section 06.01 b.) that permits the access. The VPIT, or designee, in consultation with the TSUS associate general counsel and other university officials, as appropriate to the circumstances, will approve or deny the request. This provision applies to all user accounts and information resources, including those assigned to deceased, incapacitated, or otherwise unreachable individuals.

**07. EXEMPTIONS AND EXCEPTIONS**

07.01 Individuals desiring an exemption or exception from any provision in this policy shall make the request in writing to the associate vice president for Technology Resources. The written request must specify the provision to be waived and demonstrate a compelling need or unique circumstance that clearly justifies a waiver. The associate vice president for Technology Resources will communicate a decision to the requestor within 10 business days of the request. The requestor may appeal the associate vice president’s decision to the VPIT, whose decision is final.

**08. REVIEWERS OF THIS UPPS**

08.01 Reviewers of this UPPS include the following:

Position Date

Associate Vice President for Sept 1 E2Y

Technology Resources

Associate Vice President for the Sept 1 E2Y

Information Technology

Assistance Center

Chief Information Security Officer Sept 1 E2Y

Vice President for Information Sept 1 E2Y

Technology

**09. 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.

 Associate Vice President for Technology Resources; senior reviewer of this UPPS

 Vice President for Information Technology

 President