Appropriate Use of Information Resources

UPPS No. 04.01.07

Issue No. 10

Effective Date: 7/18/2022

Next Review Date: 6/01/2025 (E3Y)

Sr. Reviewer: Chief Information Security Officer

POLICY STATEMENT

Texas State University is committed to establishing appropriate use of information resources for the university community.

01. BACKGROUND INFORMATION

01.01 This document establishes policies and procedures for the appropriate use of information resources to:

a. achieve university-wide compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

b. establish prudent and appropriate practices regarding the use of information resources; and

c. educate individuals about the responsibilities they assume when using Texas State University's information resources.

02. RELATED DOCUMENTS

02.01 UPPS No. 01.04.11, Guidelines for Use of Texas State Logos and System Statement Graphic

02.02 UPPS No. 01.04.27, Intellectual Property: Ownership and Use of Copyrighted Works

02.03 UPPS No. 04.01.01, Security of Texas State Information Resources

02.04 UPPS No. 04.01.02, Information Resources Identity and Access Management

02.05 UPPS No. 04.01.05, Network Use Policy

02.06 UPPS No. 04.01.06, University Websites

02.07 UPPS No. 04.01.08, Texas State Domain Name and URL Policy

02.08 UPPS No. 04.01.10, Information Security Incident Management

02.09 UPPS No. 04.01.11, Risk Management of Information Resources

02.10 UPPS No. 04.01.12, Email Account Management

03. DEFINITIONS

03.01 Terms in this policy have the meaning ascribed by the Information Security Glossary. Some terms have been included in this section for emphasis and ease

Glossary. Some terms have been included in this section for emphasis and ease of reference. Definitions of terms in the Information Security Glossary should be considered authoritative in the event of differences between the glossary and language in this policy.

03.02 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 (see UPPS No. 04.01.02, Information Resources Identity and Access Management, for additional information).

03.03 Authenticator – the means used to confirm the identity of a user, process, or device (e.g., user password or token).

03.04 Information Resources – as described in UPPS No. 04.01.01, Security of Texas State Information Resources and the Information Security Glossary, the term information resources has the meaning ascribed in TAC 202.1. In addition to the term's ascribed definition, information resources may include the following examples:

a. all physical and logical components, wired or wireless, of the institutional network;

b. any device that connects to or communicates electronically via the institutional network, including computers, printers, and communication devices, both portable and fixed;

c. any fixed or portable storage device or media, regardless of ownership, that contains institution data;

d. all data created, collected, recorded, processed, stored, retrieved, displayed, or transmitted using devices connected to the institutional network;

e. all computer software and services licensed by the institution;

f. support staff and services employed or contracted by the institution to deploy, administer, or operate the above-described resources or to assist the community in effectively using these resources;

g. devices, software, or services that support the operations of the institution, regardless of physical location (e.g., SAAS, PAAS, IAAS, cloud services); and

h. telephones, audio and video conferencing systems, phone lines, and communications systems provided by the institution.

03.05 Network Identifier (NetID) – 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.

03.06 User – an individual, process, or automated application authorized to access an information resource in accordance with federal and state law, institution policy, and the information owner's procedures and rules.

04. GENERAL PRINCIPLES

04.01 Texas State provides each of its authorized users with a Texas State NetID that facilitates access to the university's information resources. In accepting a Texas State NetID or any other account, the recipient agrees to abide by all applicable Texas State policies and legal statutes, including all federal, state, and local laws. Texas State reserves the right at any time to limit, restrict, or deny access to its information resources and to take disciplinary or legal action against anyone in violation of these policies or statutes.

04.02 Applicable university policies and procedures include all Texas State university policy and procedure statements (UPPSs), departmental policies and procedures, and standards, procedures, and guidelines on the Information Security Office's website (as referenced in section 01.06 of UPPS No. 04.01.11, Risk Management of Information Resources) that address the usage of Texas State information resources. Also applicable are university policies prohibiting harassment, plagiarism, or unethical conduct. Laws that apply to the use of Texas State's information resources include laws pertaining to theft, copyright infringement, insertion of malicious software into computer systems, and other computer-related crimes. This policy applies to all university information resources, whether administered centrally or departmentally, and regardless of where they reside.

04.03 Texas State provides information resources for the purpose of accomplishing tasks related to the university's mission. Texas State expects its users, particularly its faculty, staff, and other employees, to use these resources as their first and preferred option for satisfying institutional business, research, or instructional needs. Thus, users, in collaboration with the vice president for Information Technology (VPIT) and chief information security officer, should only seek new information resources after determining that existing, university-provided resources do not adequately satisfy the institution's business, research, or instructional needs.

The university may restrict the use of or access to its information resources to specific research, teaching, or other purposes in keeping with Texas State's mission. Texas State's computer information resources are not a public forum.

04.04 Consistent with the provisions of UPPS No. 04.01.12, Email Account Management, Texas State considers email a significant information resource and an appropriate mechanism for official university communication. The university provides official university email addresses and services to its students, faculty, staff, retirees, and organizational units for this purpose and to enhance the efficiency of educational and administrative processes. In providing these services, the university anticipates that email recipients will access and read university communications in a timely fashion.

04.05 Consistent with the provisions of UPPS No. 04.01.02, Information Resources Identity and Access Management, and other applicable policies and statutes, students who have an active affiliation are allowed to use Texas State's information resources for school-related and personal purposes. Personal use must not result in any additional expense to the university or violate restrictions detailed in Section 05.

04.06 Consistent with the provisions of UPPS No. 04.01.02, Information Resources Identity and Access Management, and other applicable policies and statutes, employees of Texas State are allowed to use Texas State's information resources

employees of Texas State are allowed to use Texas State's information resources in the performance of their job duties. State law and university policy permit incidental personal use of Texas State information resources, subject to review and reasonable restrictions by the employee's supervisor. Such personal use must not violate any applicable policies and statutes, must not interfere with the employee's job performance, must not result in any additional expense to the university, and must not violate restrictions detailed in Section 05.

04.07 Censorship is not compatible with the goals of Texas State. The university will not limit access to any information due to its content, as long as it meets the standard of legality. The university reserves the right, however, to impose reasonable time, place, and manner restrictions on expressive activities that use its information resources. Furthermore, the university reserves the right to block or impose necessary safeguards against files and other information, such as malicious software and phishing emails, that are inherently malicious or pose a threat to the confidentially, integrity, or availability of information resources for the university and its stakeholders.

04.08 Texas State's information resources are subject to monitoring, review, and disclosure, as provided in UPPS No. 04.01.02, Information Resources Identity and Access Management. Consequently, users should not expect privacy in their use of Texas State's information resources, even in the case of users' incidental, personal use.

04.09 Intellectual property laws extend to the electronic environment. Users should assume that works communicated through Texas State's institutional network and any of its information resources are subject to copyright laws, unless specifically stated otherwise.

04.10 The state of Texas and Texas State consider information resources as valuable assets. Further, software and other information resources acquired or licensed by the university are the property of the university or the company from whom it is licensed. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime, punishable under Texas and federal statutes.

05. INAPPROPRIATE USES OF INFORMATION RESOURCES

05.01 The following activities exemplify inappropriate use of the university's information resources. These and similar activities are strictly prohibited for all users:

a. use of university information resources for illegal activities or purposes. The university will address instances of such misuse appropriately, which may include reporting to law enforcement authorities. Examples of illegal activities or purposes include unauthorized access, intentional corruption or misuse of information resources, theft, and child sexual abuse materials;

b. failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the university's information resources;

c. the abuse of information resources including any willful act that:

1) endangers or damages any information resource regardless of physical or logical location;

logical location;

2) disrupts or degrades the availability of information resources;

3) introduces malicious software or data into information resources intended to affect the information resource's confidentiality, integrity, or availability;

4) sends a message with the intent to disrupt university operations or the operations of outside entities;

5) intentionally occupies or monopolizes information resources for an unreasonable time period to the detriment of other authorized users; or

6) consumes an unreasonable amount of communications bandwidth, either on or off campus, to the detriment of other authorized users.

d. use of university information resources for personal financial gain or commercial purpose;

e. failure to protect an account or authenticator from unauthorized use;

f. falsely representing one's identity through the use of another individual's account, including their Texas State NetID, or permitting the use of an account or authenticator by someone other than its owner;

g. unauthorized attempts to use, access, duplicate, disclose, alter, damage, or destroy any physical or electronic data repository or other information resources;

h. use of unauthorized external or cloud-hosted information resources for the purposes of accomplishing university business, research, or instructional purposes that would involve the storage, processing, or transmission of sensitive or confidential university data;

i. unauthorized duplication, use, or distribution of software and other copyrighted digital materials (including copyrighted music, graphics, videos, etc.). All software and many other digital materials are covered by some form of copyright, trademark, license, or agreement with potential civil and criminal liability penalties. The copyright or trademark holder must specifically authorize duplication, use or distribution, or a specific exception of the Copyright Act, such as the Fair Use exception, the Library exception, or exceptions under the TEACH Act, must apply (see also UPPS No. 01.04.27, Intellectual Property: Ownership and Use of Copyrighted Works);

j. participating or assisting in the deliberate circumvention of any security policy, procedure, or control that pertains to university information resources;

k. using university information resources in a manner that violates other university policies, such as UPPS No. 04.04.46, Prohibition of Discrimination, The Texas State University System (TSUS) Sexual Misconduct Policy), or UPPS No. 01.04.07, Civility Policy and Procedures;

l. using university information resources for the transmission of spam mail, chain letters, malware, phishing, or personal advertisements, solicitations, or promotions;

m. attempting to or actually modifying or extending the Institutional Network (e.g., adding hubs, switches, wireless access points, or similar devices) in violation

of the university's network use policy (see section 01.02 of UPPS No. 04.01.05, Network Use Policy);

n. using Texas State's information resources to affect the result of a local, state, or national election or to achieve any other political purpose (consistent with Texas Government Code §556.004);

o. using Texas State's information resources to state, represent, infer, or imply an official university position without appropriate authorization;

p. unauthorized network scanning, foot printing, eavesdropping, or conducting other reconnaissance activities on information resources; and

q. unauthorized alteration or relay of network traffic (e.g., "man-in-the middle" attacks).

06. RESPONSIBILITIES OF USERS

06.01 Each user shall use university information resources responsibly and respect the needs of other users.

06.02 Users are responsible for any usage of their Texas State accounts, including their NetID, and must maintain the confidentiality of their passwords and other authenticators.

06.03 A user must report any abuse or misuse of information resources or violations of this policy to the Information Security Office or to the Information Technology Assistance Center (see UPPS No. 04.01.10, Information Security Incident Management).

06.04 In keeping with Texas State's core values, all uses of its information resources should reflect high ethical standards, mutual respect, and civility consistent with UPPS No. 01.04.02, Ethics Policy and UPPS No. 01.04.07, Civility Policy and Procedures.

06.05 In using Texas State information resources, users shall adhere to applicable provisions of the university's network use policies (see UPPS No. 04.01.05, Network Use Policy) and guidelines regarding the design and content of official communications and publications (see brand.txst.edu).

06.06 Administrative heads and supervisors must report ongoing or serious problems regarding the use of Texas State information resources to the Office of the VPIT or the Information Security Office as appropriate.

06.07 Each user shall immediately notify Materials Management of the loss of any university-owned computer, mobile devices, or storage media (see Section 04.02 of UPPS No. 05.01.01, Texas State University Property and Equipment).

06.08 Each user shall immediately notify the Information Security Office of the loss of any personally owned computer, mobile devices, or storage media that contains or may contain any sensitive or confidential university data.

07. ACCESS TO UNIVERSITY INFORMATION RESOURCES BY AUDITORS

07.01 Consistent with Chapter III, Paragraph 7.5 of The TSUS Rules and Regulations, the TSUS director of Audits and Analysis and auditors reporting to them, either

the TSUS director of Audits and Analysis and auditors reporting to them, either directly or indirectly, while in the performance of their assigned duties, shall have full, free, and unrestricted access to all university information resources, with or without notification or consent of the assigned owner of the resources. The university shall afford this access consistent with UPPS No. 04.01.02, Information Resources Identity and Access Management.

07.02 The university shall provide state, federal, and other external auditors with access to university information resources with prior authorization by the VPIT.

08. LIABILITY FOR FAILURE TO ADHERE TO POLICY

08.01 Failure to adhere to this policy may lead to the revocation of a user's Texas State NetID, suspension of elevated access privileges, suspension, dismissal, or other disciplinary action by the university, as well as referral to legal and law enforcement agencies.

09. REVIEWERS OF THIS UPPS

09.01 Reviewers of this UPPS include the following:

Position	Date
Chief Information Security Officer	June 1 E3Y
Associate Vice President for Technology Resources	June 1 E3Y

10. 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