TEXAS STATE ®

Information Security Office

Policy Reference Sheet

Note: This handout provides a limited summary of Texas State University Procedure and Policy Statements that pertain to information security. This document focuses on some of the most important parts of the university's InfoSec policy statements; however, it is not a substitute for the policies it summarizes. Please review the policies and procedures on your own to ensure you have a firm understanding – after all, security is everybody's responsibility.

Good-to-know terms

- ***Information Resource.*** a broad term that encompasses physical and logical university assets such as computers and storage media, data and other information created or used on the university network or by university personnel, cloud-hosted applications and services, and technology support services and the person hours of the personnel who provide those services. For full definition, see UPPS 04.01.07 § 03.01
- ***Information Resource Owner.*** The university employee to whom day-to-day oversight of an information resource has been delegated and the person who is ultimate responsible for the protection of an information resource. Owners generally occupy director- or higher-level positions. For full definition and responsibilities, see UPPS 04.01.11 § 02.02
- ***Information Resource Custodian.*** The person who provides asset support services to both owners and users of information resources. For full definition and responsibilities, see UPPS 04.01.11 § 02.03
- ***Information Resource User.*** The default role possessed by all users of Texas State information resources, users are the people who use information resources. All users are responsible for complying with the university's policy. Owners and custodians are almost always also users. For full definition and responsibilities, see UPPS 034.01.11 § 02.04.
- ***Confidential Information.*** Confidential information is defined by TAC 202 as "information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement." Confidential information is the highest-value and highest-risk information that the university may process, and if disclosed unduly, confidential information poses the greatest harm to both the data subjects and the institution. For full definition, see UPPS 04.01.11 § 02.08.c
- ***Sensitive Information.*** Sensitive information is the broadest category of information, usually presenting attributes of both public and confidential information. While potentially subject to

controlled disclosure through public information requests, sensitive information must still be protected from undue disclosure to those without a legitimate need to know. For full definition, see UPPS 04.01.11 § 02.08.b

- ***Public Information.*** Public information is, by its nature, intended to be shared broadly, without restriction. For full definition, see UPPS 04.01.11 § 02.08.a

04.01.01 – "Security of Texas State Information Resources"

- https://policies.txstate.edu/university-policies/04-01-01.html
- The overarching information security policy
- §01 references additional policies and legislative requirements.
- §02 establishes the ISO in policy per Texas Administrative Code (TAC chapter 202).
- §03 obligates department heads and information resource owners to be responsible for:
    - activities in their department and collecting NDAs (03.04); and for
    - users in their department and their and permissions (03.05).
- §04 outlines physical and environmental security requirements for facilities (04.01 to 04.04) and includes some requirements for workstations and other devices (04.05).
- §05 outlines the Continuity of Operations Plan (COOP) (akin to a BCP/DRP in the private sector). Owners and custodians of information resources have a part to play in COOPs for resources under their care (05.04).

04.01.02 – "Information Resources Identity and Access Management"

- https://policies.txstate.edu/university-policies/04-01-02.html
- Defines how identities, accounts, and access shall be managed.
- §03 includes definitions of pertinent terms
- §04 defines who is eligible for a NetID
- §05 details affiliations (student, faculty & staff, etc.)
- §06 details NetID administration procedures.
    - Only the owner of a NetID is authorized to know the password (06.03);
    - the owner of the NetID is responsible for protecting access to the account (06.06).
- §07 outlines procedures for scenarios in which university information may be accessed without the owner or data subject's consent.

04.01.03 – "Computer Equipment Repair Services"

- https://policies.txstate.edu/university-policies/04-01-03.html
- Outlines ITAC's computer repair services. Listed adjacent to ISO policies, though this isn't an ISO-specific UPPS.

04.01.05 – "Network Use Policy"

- https://policies.txstate.edu/university-policies/04-01-05.html
- Explains how the university network may be used.

- §01 gives an overview of policy requirements, including the prohibition of extending the university network (01.02) by most people other than authorized IT staff.
- §03 includes definitions of relevant terms.
- §04 continues the general networking procedures.
    - Devices connected to the university network must support the university mission (04.01);
    - The university network cannot be extended (04.02);
    - Servers connected to the network require additional authorization and oversight (04.05).
- §05 outlines the wireless networks provided on campus, including a guest network (05.01) and encrypted wireless network (05.02), the latter of which should be used instead of the guest network when possible (05.03), though neither are intended to entirely preplace wired connectivity (05.03).
- §06 outlines "ResNet" network connectivity provided in the residence halls for students.
- §07 goes over network related incident response procedures related to network connectivity.

04.01.06 – "University Websites"

- https://policies.txstate.edu/university-policies/04-01-06.html
- Covers standards for websites related to the university. This is not an InfoSec-specific policy, but employees, particularly technical staff, should be aware of its contents.

04.01.07 – "Appropriate Use of Information Resources"

- https://policies.txstate.edu/university-policies/04-01-07.html
- Outlines what is (and isn't) appropriate to do with university information resources.
- §03 contains some pertinent definitions
- §04 provides general guidelines for appropriate use, including:
    - requirements to abide by applicable university policies, federal/state/local laws, and intellectual properly laws (04.01, 04.02, 04.09);
    - information resources need to be used to accomplish tasks related to the university's mission (04.03);
    - users must check their university email for important communications (04.04);
    - incidental use of information resources by employees must neither violate applicable policies and statutes nor cause additional expense to the university nor interfere with employees' job performance (04.06);
    - the university will not censor materials based on content alone as long as it's legal. However, the university may impose some reasonable restrictions on expressive activities that use its information resources, and some safeguards may be implemented to block inherently malicious files and other threats (04.07);
    - Software purchased or licensed by the university remains the property of the university, and unauthorized copying/distribution/etc. is prohibited (04.10).
- §05 provides examples of prohibited activities, including:

    - Using information resources for illegal activities (05.01.a);
    - Abusing or intentionally damaging information resource (05.01.c);
    - Using university information resources for personal financial gain or commercial purpose (05.01.d);
    - Failing to protect a password or NetID from unauthorized use or using someone else's NetID (05.01.e, f);
    - Deliberately circumventing any security measure or administrative access control that pertains to information resources (05.01.j);
    - Sending spam, chain letters, malware, and advertisements via university resources or using those resources to affect elections or other political purposes (05.01.l, m)
- §06 outlines responsibilities of users, which include reporting abuse or misuse of resources to the ISO or ITAC (06.03) and reporting the loss of any storage devices that contains university data (06.07).
- §07 outlines access to information resources by auditors
- §08 specifies potential consequences for not adhering to this policy (08.01) and includes references to relevant state and federal statues (08.02).

04.01.08 – "Texas State Internet Domain Name Policy"

- https://policies.txstate.edu/university-policies/04-01-08.html
- Summarizes base requirements for managing the txstate.edu domain, its subdomains, and top-level folders.
- §01 describes DNS (the domain name system) and its importance to the university, and that both IT and University Marketing are responsible for the assignment of URLs.
- §02 provides some relevant definitions.
- §03 provides procedures for obtaining a txstate.edu subdomain or top-level folder. Most third-level domain names or top-level folders should align with the name of the responsible organizational unit (03.01-03.03), however some exceptions can be made (03.04). It also outlines some requirements of domain names (03.05-08).
- §04 provides guidance for domain names outside of txstate.edu, including those used by external entities (04.03) and internal entities (04.01 – 04.02, 04.04 – 04.06).

04.01.09 – "Server Management Policy"

- https://policies.txstate.edu/university-policies/04-01-09.html
- Establishes policy-level guidance for server administration.
- §03 provides some relevant terms and definitions.
- §04 provides general requirements, including:
    - The need to comply with other university policies and procedures (04.01);
    - Recommendations to meet industry-standard benchmark security standards (04.02);
    - The need to register servers with IT (04.03);
    - The need to contact ITAC prior to acquiring server hardware so alternative hosting arrangements can be explored (04.05);

    - The need to install updates (04.07)
- §05 advises server owners that their systems are subject to scans and tests by the ISO that may result in findings that must be remediated, and if those issues are not remediated, network connectivity may be disabled (05.01). Similarly, network connectivity may be terminated if a server becomes an imminent threat to the university (05.02).

04.01.10 – "Information Security Incident Management"

- https://policies.txstate.edu/university-policies/04-01-10.html
- Describes how (cyber) incidents are managed at Texas State.
- §01 charges the ISO with handling information insecurity incidents.
- §02 defines events (02.01) and incidents (02.02), and how incidents are classified based on impact (02.03).
- §03 outlines how the ISO responds to incidents of varying impact levels.
- §04 specifies reporting requirements for owners, custodians, and users (04.01) and how the ISO must document and report incidents.

04.01.11 – "Risk Management of Information Resources"

- https://policies.txstate.edu/university-policies/04-01-11.html
- Describes how risk to information resources is managed and in-part mitigated at Texas State.
- §02 defines how assets and other information resources are to be managed, including:
    - Definitions of information resource owner, custodian, and user roles (02.02, 02.03, and 02.04);
    - Information resources are subject to review and monitoring, and that users should not expect privacy when using Texas State's information resources (02.06);
    - How data are classified as public, sensitive, or confidential (02.08, a-c)
    - Standards for handling sensitive and confidential information (02.09), which specifies in part:
        - PII such as SSNs and driver's license numbers must not be stored unless required by external powers, and instead, NetIDs or Texas State ID numbers should be used (02.09.a);
        - PCI (payment cardholder information) data can't be stored any longer than necessary to authorize a transaction using that information (02.09.b);
        - Confidential data must be transmitted electronically over a public network (e.g., the internet) in unencrypted form (02.09.c);
        - Confidential data must not be stored on portable devices or media (02.09.d), or on personally owned devices or media (02.09.f), or on devices external to the campus network (02.09.g). If it must be stored on these media, it must be encrypted or protected by other compensating controls with advice and authorization of the ISO;
        - Confidential or sensitive data may only be retained as long as needed in alignment with the records retention schedule (02.09.h);

        - All computing devices must employ whole-disk encryption provided by ITAC and the ISO regardless of their intended use unless they have a documented and approved exemption (02.09.j, k);
    - How assets may be transferred or disposed of (02.10), including:
        - ITAC must be contacted to collect/remove data (i.e., storage media) from computers and other devices prior to the equipment being transferred outside of Texas State;
        - Storage devices or media (e.g., a laptop and its hard drive) must be fully sanitized prior to re-use or re-assignment, even within a department.
- §04 outlines what controls need to be implemented to limit access to information resources, including:
    - The need to deactivate a user's NetID when they no longer require one (04.04);
    - The need to limit access to sensitive and confidential information based on a user's need-to-know (04.05);
    - Requirements for passwords (04.06, 04.07) and recommendation to leverage single-sign on and multi-factor authentication services provided by the Division of IT (04.10, 04.11).
- §05 outlines information gathering requirements for internet-connected resources (e.g., SaaS Apps) that will handle sensitive or confidential information (05.02), the need to separate test and production functionality and that all users who may engage in testing with real data needing authorization to access that information (05.03).
- §06 outlines the risk assessment procedures implemented by the ISO and conducted in part by information resource owners and their designated custodians.

04.01.12 – "Email Account Management"

- https://policies.txstate.edu/university-policies/04-01-12.html
- Includes policy-level procedures for managing university email accounts.
- §03 defines pertinent terms
- §04 specifies that eligible users will receive a Texas State email account (04.01), that it is the responsibility of individual account owners to manage the contents of their mailboxes (04.03), and that email is not an authorized electronic repository for university records (04.07).
- §05 outlines how long email accounts are retained following a user's separation, when accounts are granted to various affiliation types, and who may continue to be granted access to their email accounts after leaving the university (i.e., retirees).