Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Access Control**
Regulation and Procedure Number:	**URP: 04.710**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

The establishment of Access Control regulations and procedures provides a mechanism for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access through the establishment of an Access Control program. The Access Control program helps Texas Woman's University ("TWU") implement security best practices regarding logical security, account management, and remote access.

The scope of these regulations and procedures is applicable to all Information Resources owned or operated by TWU. All Users are responsible for adhering to these regulations and procedures. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures. The Policy Owner, as defined in URP 01.320: University Policy Development and Implementation, is responsible for managing the development, documentation, and dissemination of this URP.

APPLICABILITY

This policy is applicable to TWU Students, Employees, University Affiliates, and Guests.

DEFINITIONS

1. "Access Control ("AC")" means the selective restriction of access to a TWU location or resource.

2. "Accounts" means an established relationship between a user and a computer, network, or information service.

3. "Confidential Data" applies to the data that is private, confidential by law or otherwise exempt from public disclosure (i.e. exemptions under the Texas

Public Information Act, Social Security Numbers, personally identifiable Medical and Medical Payment Information subject to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, 45 C.F.R. 160, Driver's License Numbers and other government-issued identification numbers, Education Records subject to the Family Educational Rights & Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99), financial account numbers or credit or debit card number in combination with any required security code or Access code permitting Access to an individual's financial account, and/or other University Data about an individual likely to expose the individual to identity theft).

4. "Employee" means any individual at TWU who is hired in a full-time, part-time, or temporary capacity in a faculty or staff position, or in a position where the individual is required to be a student as a condition of employment.

5. "External Information System" means any Information System that is not owned or operated by TWU.

6. "Guests" means any individual not affiliated with TWU.

7. "Information Flow" means the movement of information through TWU's organization's information systems.

8. "Information Resources" means an element of infrastructure that enables the transaction of data, designed to provide content and information services to Users. Information Resources include information in electronic, digital, or audiovisual format and any hardware or software that store and use such information (i.e., electronic mail, local databases, externally accessed, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, voice mail, faxes). This definition also includes computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, cloud services, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, Information Resources includes the procedures, equipment, facilities, software, and

data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

9. "Information System" means a discrete set of Information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

10. “Information System Owner” means the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an Information System.

11. “Mobile Device” does not have a single definition; however, a Mobile Device is commonly a portable electronic device with at least one wireless network interface, local built-in (non-removable data storage), and an operating system that is not a full-fledged desktop or laptop operating system.

12. “Network Device” means a device that controls the flow of information in a network (e.g., router, switch, wireless access point). A network device does not include a device that uses a network (e.g., computers, mobile device, etc.).

13. “National Institute of Standards and Technology (NIST)” means a non-regulatory agency of the United States Department of Commerce that works in cooperation with various industries to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology.

14. “Public Data” applies to Information that has been approved by TWU management or the State of Texas for release to the public. There is no such thing as unauthorized disclosure of this Information and it may be disseminated without potential harm.

15. “Separation of Duties” means a security principle that ensures that no single individual has the capability of executing, approving and/or auditing a particular task/set of tasks.

16. “Session Lock” means when an information system prevents a user from further activity after the user has been inactive for some predefined time.

17. “Student” means a person taking courses at TWU, a person who is not currently enrolled in courses but who has a continuing academic relationship with TWU, or a person who has been admitted or readmitted to TWU.

18. “University Affiliate” means any individual associated with TWU in a capacity other than as a Student or Employee who has access to TWU resources through a contractual arrangement or other association. This includes the following individuals:

    a. Contractors and Vendors: an individual, business, or governmental entity that has a fully executed contract to provide goods or services to TWU. This includes employees of contractors or vendors and independent contractors.

    b. Employee of a Governmental Agency: an individual employed by a federal or Texas state agency.

    c. Employee of a TWU-Affiliated Institution: an individual who works for organizations that are tightly aligned with the University.

    d. Pre-Employment Individual: an individual who will be hired by the University and the hiring department has sponsored their access to TWU resources.

    e. Other University Affiliate: any individual who does not fit into any other category and needs access to TWU resources.

19. “Users” means TWU Employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. Account Management

1. A uniquely identifiable account will be assigned to each User upon the User submitting an account creation request.

2. Account types that are permitted include individual (named) User accounts, privileged (elevated), system accounts, service accounts, and emergency accounts.

a. Users requesting administrative privileges or elevated accounts receive additional review by appropriate TWU personnel (e.g., Information System Owner, mission/business owner, or Information Security Officer) responsible for approving such accounts and privileged access.

b. Emergency accounts may only be established in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency accounts may only be created under authorization by the Chief Information Officer and Information Security Officer.

3. Generic accounts and Guest accounts are restricted and not permitted unless approved through the Request an Exception for Information Technology URP, Security Control, Standard or Procedure process (*See* Forms and Tools Section).

4. Account managers shall define and document types of accounts used within an Information System. For University-wide Information Systems using IT Solutions ("ITS") managed credentials, an ITS administrator shall serve in the custodian role and serve as account manager. The Information System Owner may fulfill the role of account manager for Information Systems that are isolated to specific business-functional or academic units.

   a. Account managers shall:

      i. Maintain appropriate levels of communication with the Data Owners to determine the level or degree of access granted to an individual;

      ii. Determine the technical specifications needed to set access privileges;

      iii. Create and maintain procedures used in managing accounts; and

      iv. Perform all account administrator duties as required including periodic account User review, account termination, or account access changes.

5. Individuals are not permitted to use account credentials for which they are not a designated User; therefore, credential or password sharing is prohibited.

6. ITS shall implement and utilize role-based access to ensure Users only have access to the resources and information required to perform job-related functions.

7. Access outside of that granted by default to new Users must be requested through the Service Request System. Approval for new access must be given by the User's supervisor or director and

by the Data Owner of the Information System for which they are requesting access.

8. Users requesting access to Information Systems that contain Confidential Data may be required to complete training before access is approved. Users requesting new or additional access to an Information System that contains student information are required to complete Family Educational Rights and Privacy Act ("FERPA") training and have approval from the current FERPA manager.

9. Users requesting new or additional access to an Information System that contains health-related information shall receive access from the appropriate business functional area in accordance with the regulations and procedures outlined in URP 01.270: HIPAA Privacy and Security Policy and Procedures.

10. Upon separation of employment with TWU, access to Information Resources must be terminated. Employee accounts are stripped of privileges upon resignation or termination of employment through a daily, automated process. This automated process is backed up by the Office of Human Resources practice to have all terminating Employees and management complete the Employee Checklist for Separation, and Management Checklist for Faculty/Staff Separation, respectively.

11. Employees changing assignments or departments will have their access reviewed by ITS. Where appropriate, access will be removed.

12. User accounts may be deactivated due to prolonged inactivity, or evidence that the account is no longer valid or actively in use.

13. TWU Information Security shall regularly monitor the use of accounts managed by ITS and review accounts for compliance with account management requirements.

B. Access Control | Disable Accounts

ITS shall disable accounts in accordance with TWU-defined standards, including when the accounts:

1. Have expired;

2. Are no longer associated with a User or individual;

3. Are in violation of University policy; or

4. Have been inactive in accordance with TWU-defined standards.

C. Access Enforcement

1. ITS utilizes an access control procedure to help identify and select only those accounts which require access to perform job-related functions. Each approved account will be assigned a unique identifier (username), and identification is authenticated before a User may access any Information Resources. ITS will enforce controls to ensure that only authorized accounts can access Information Resources.

2. ITS may prevent further access to workstations by initiating a session lock after a specified period or upon receiving a request from a User. In addition, ITS may retain the session lock until the User reestablishes access using established identification and authentication procedures.

D. Separation of Duties

Business functional areas (TWU departments or academic components) shall establish rules that ensure adequate controls and separation of duties of those individuals responsible for tasks that are susceptible to fraudulent or other unauthorized activity to Information Resources.

E. Least Privilege

Business functional areas (TWU departments or academic units) shall create accounts with least privilege for routine tasks. Privileges will be escalated only as needed, consistent with the regulations and procedures regarding separation of duties.

F. Unsuccessful Logon Attempts

1. Users will be locked out of their accounts if there are a number of unsuccessful login attempts.

2. User accounts locked out due to multiple incorrect logon attempts must wait until the account is unlocked before attempting to login again.

3. Any User account may be locked by ITS in the event of a security incident. The account may remain locked until the incident has been investigated.

4. User accounts may be deactivated if there is a violation of TWU policies, regulations or procedures.

G. System Use Notification

ITS will ensure that the following system use notification banner is displayed on all authentication portals:

1. “Texas Woman's University – Disclaimer

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged. Violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device.

WARNING: You are about to connect to a secured information system. Access to this system is for official business only. Unauthorized access is prohibited. Any misuse of this information system or the data that it contains will be prosecuted to the full extent of the law.

a. Unauthorized use is prohibited;

b. Usage may be subject to security testing and monitoring;

c. Misuse is subject to criminal prosecution; and

d. Users have no expectation of privacy except as otherwise provided by applicable privacy laws.”

H. Permitted Actions without Identification or Authentication

1. The rules established by ITS will ensure that no actions may be performed on Information Resources without specific User identification or authentication, except for:

a. Read-only access to Public Data;

b. Submission of information through publicly accessible forms.

I. Remote Access

1. Remote access to Information Resources shall be through Virtual Private Network (“VPN”) technology, available only to authorized Users.

2. Users with authorized access to TWU VPN should only connect using authorized TWU-owned devices. Personally-owned devices are not permitted unless an exception is documented and approved in accordance with URP 04.797: Information Technology Exceptions. If personally-owned equipment must be used for telecommuting, the equipment must be enumerated, and rationale or justification documented as part of the alternate work agreement (*See* URP 05.620: Alternative Work Arrangements for Staff Employees). Users that connect to TWU VPN using personally-owned devices acknowledge that their personal equipment is an extension of TWU's network and are subject to the same rules and regulations that apply to TWU-owned equipment.

3. All personally-owned devices connected to TWU internal networks via VPN should be configured to comply with TWU policies and standards.

4. Users must use secure network and access control mechanisms. It is the responsibility of TWU Employees, Affiliates, contractors and vendors with VPN access to TWU networks to ensure that their remote access connection is given the same consideration as an on-site connection to Information Resources.

5. It is the responsibility of Employees with VPN access to ensure that unauthorized individuals are not allowed access to TWU internal networks.

6. Authorized VPN Users must log into TWU VPN at least once every six (6) months to retain access to TWU VPN. If Users do not log into VPN at least once every six (6) months, their access will be revoked. To regain access, a new VPN request must be submitted (*See* Offsite Network Connection (Virtual Private Network) Request).

J. Wireless Access

1. TWU provides secured, internal wireless to Employees and authorized University Affiliates on a case-by-case basis. Requests for access to secured, internal wireless shall be submitted to the service request system for approval and documentation. Guest wireless (“twunet”) does not have access to TWU internal resources and therefore does not require identification or authentication.

2. ITS will ensure that Service Set Identifiers (“SSID”) values are changed from the manufacturer default setting.

3. Unauthorized access points and network attached wireless devices are prohibited on the TWU network. Periodic monitoring will be conducted to identify unauthorized networks. ITS (or their

designee) is the only authorized entity that may install wireless devices on TWU networks. Information owners (i.e., device owners or owners of Information Resources) will be contacted and requested to comply with this Control.

4. Users are prohibited from extending the TWU network through means of wireless technologies.

5. Only Public Data may be transmitted via unencrypted wireless networks and devices. Confidential, Sensitive and Business Functional Data may only be transmitted via secure means, such as encryption or VPN.

K. Access Control for Mobile Devices

1. ITS will manage and maintain all TWU-owned Mobile Devices and network connections through a central mobile device management platform.

2. ITS permits personally-owned Mobile Devices on the Guest wireless network.

3. Users are responsible for ensuring any personally-owned Mobile Device is properly configured.

4. Users are responsible for protecting Mobile Devices from unauthorized access by properly securing the devices with passwords or other security measures.

L. Use of External Information Systems

1. ITS will evaluate External Information System integrations through the project management and risk assessment processes.

2. Users must receive documented authorization before accessing an External Information System. Requests for connections to External Information Systems must be submitted through the Service Request System. The authorization to access an External Information System must address how the External Information System will:

a. Access the Information Resource;

b. Process, store, and/or transmit organization-controlled information using the External Information Systems;

c. Maintain the security of Information Resources.

3. Users should follow TWU URP 04.795: Data Access and Use Policy when accessing and using Data with External Information Systems.

4. Users should establish terms and conditions within contracts or agreements with external information resources providers.

M. Publicly Accessible Content

1. Only Employees authorized by TWU may post information onto an Information Resource that is publicly accessible. Authorized Employees will be trained to ensure that publicly accessible information does not contain nonpublic information.

a. All Employees authorized to write reports will be trained by ITS or the Office of Institutional Research and Data Management before posting information.

b. All Employees authorized to post information onto the TWU website will be trained by TWU Marketing and Communication.

2. Authorized Employees will review the proposed content of publicly accessible information and remove nonpublic information prior to posting onto an Information Resource.

3. Authorized Employees will review published content for nonpublic information regularly and remove such information, if discovered.

II. Regulatory Compliance

A. The State of Texas has chosen to adopt a select number of Access Control ("AC") principles established in NIST SP 800-53 "Access Control" guidelines. The NIST AC controls have been assigned a number; however, the State of Texas has not adopted every NIST AC control, so there are gaps in the numbering sequence. The following subsections outline the AC standards included in TWU's regulations and procedures.

1. AC-1, AC-2, AC-2(3), AC-3, AC-5, AC-6, AC-7, AC-8, AC-11, AC-14, AC-17, AC-18, AC-19, AC-20, and AC-22.

III. Compliance

Employees that violate this policy are subject to corrective and disciplinary action, including and up to dismissal, in accordance with URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes and URP 05.600: Staff Standards of Conduct and Disciplinary Process. TWU may also take

corrective action against interns, volunteers, contract employees, contractors, and/or consultants that violate this policy, including and up to termination of TWU's relations or access with that individual or entity. Students that violate this policy are subject to corrective and disciplinary action, including and up to suspension or expulsion, in accordance with TWU's URP 06.200: Student Code of Conduct.

REVIEW

This policy will remain in effect and published until it is reviewed, updated, or archived. This policy is to be reviewed once every six years. Interim review may be required as a result of updates to federal and state law or regulations, Board of Regents policies, or internal processes or procedures.

REFERENCES

Tex. Admin. Code, Ch. 202

Department of Information Resources Security Standards Catalog

Information Security Standard: Disabling Accounts

Model Security Plan for Prohibited Technologies

Section 2054.138, Texas Government Code

NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations

URP 01.320: University Policy Development and Implementation

URP 01.270: HIPAA Privacy and Security Policy and Procedures

URP 04.795: Data Access and Use

URP 04.797: Information Technology Exceptions

URP 05.620: Alternative Work Arrangements for Staff Employees

URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes

URP 05.600: Staff Standards of Conduct and Disciplinary Process

URP 06.200: Student Code of Conduct

FORMS AND TOOLS

Request an Exception for Information Technology URP, Security Control, Standard or Procedure

Service Request System

Offsite Network Connection (Virtual Private Network) Request

Publication Date: **07/02/2021**

Revised: **10/08/2021; 03/26/2025**