Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Resource Personnel Security**
Regulation and Procedure Number:	**URP: 04.705**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This document establishes personnel security regulations and procedures in relation to the use of Information Resources. The purpose of these regulations and procedures is to manage Texas Woman's University's ("TWU" or "University") risks from inadequate and ineffective personnel screening, termination processes, and management of external 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 University Regulation and Procedure ("URP").

APPLICABILITY

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

DEFINITIONS

1. "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.

2. "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.

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

4. "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.

5. "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.

6. "User" means TWU Employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. Position Risk Designation

1. The Office of Human Resources ("OHR") has designated all positions to be security sensitive; therefore, all applicants will be subject to a background check.

B. Personnel Screening

1. TWU shall screen individuals prior to authorizing access to Information Systems. TWU OHR has designated all positions to be security sensitive and requires every Employee to go through the same pre-screening and background check process that is further outlined in URP 05.205: Employment Practices and URP 05.255: Criminal Background Checks.

2. A minimum criminal background check will be completed on all final employment candidates (Staff, Faculty, and Student Employees) by TWU OHR.

3. University Affiliates that need access to Information Resources shall have background checks filed with OHR.

4. As applicable, re-screening will be done in accordance with OHR URP 05.255: Criminal Background Checks and URP 04.440: University Affiliate Criminal Background Checks.

C. Personnel Termination

1. Personnel Termination is managed in OHR and supported by an automated Information System account process managed by IT Solutions ("ITS"). Account access is automatically disabled when employment is ended.

2. Upon termination, Employees must follow the Guide for Exiting Employees provided by TWU OHR and both Employee and supervisor must complete their respective "Employee Checklist for Separation" and "Management Checklist for Faculty/Staff Separation" documents referenced in the Guide for Exiting Employees. These documents serve as post-employment discussion points for the supervisor and exiting Employee and checklists for removing User possession or security access including but not limited to; Keys, Access Cards, Computer Equipment, ID Cards, Access Codes, and any passwords for additional systems/networks

accessed by the Employee (*See* Office of Human Resources Guide for Exiting Employees).

3. ITS shall terminate or revoke any Information Resource account associated with the terminated Employee.

4. The exiting Employee and supervisor shall retrieve and turn in all security-related TWU system-related property including but not limited to: Keys, Access Cards, Computer Equipment, ID Cards, Access Codes, authentication devices, and any passwords for additional systems or networks accessed by the Employee.

5. ITS shall retain access to TWU Information and Information Systems formerly controlled by the terminated individual, and ITS or the business functional area shall provide appropriate personnel with access. The business functional area supervisor shall request access to the records via the Service Request System.

D. Personnel Transfer

1. An automated process via the Service Request System notifies TWU Information Security of Employee departmental transfers within twenty-four (24) hours of Employee reassignment.

2. Employees changing assignments or departments will have their access reviewed and confirmed by TWU Information Security within five (5) business days of service request generation. Where appropriate, access will be modified or removed.

3. The Employee and appropriate personnel will be notified of access changes by TWU Information Security at the close of the Service Request.

4. For Information Resources administered outside of ITS (such as building access and software administered by business functional areas), it is the responsibility of the Information Resource owner or business functional area supervisor, to modify access authorization (or request modification), as needed, to correspond with any changes in operational need due to reassignment or transfer.

E. Access Agreements

1. TWU Information Security shall develop and document the TWU Data Use Agreement. The purpose of the TWU Data Use Agreement is to inform Employees with Information Resource access of their principal obligations concerning the use of TWU Information Resources, and to document their agreement to abide by these obligations.

2. The TWU Data Use Agreement shall be periodically reviewed and updated as needed by TWU Information Security.

3. To access and use TWU Information Resources, Employees and University Affiliates must agree that they are aware of, read, and will comply with the policies concerning Information Resources set out in TWU URPs and accept and agree to the TWU Data Use Agreement.

4. Employees with access to TWU Information Resources shall review and sign the TWU Data Use Agreement annually.

5. TWU Information Security shall verify that Employees requiring access to Information Resources have signed the TWU Data Use Agreement each year.

6. Where appropriate, additional access agreements may be required prior to Information System access.

F. External Personnel Security

1. University Affiliates utilized by TWU must complete the Affiliate Access Form prior to being granted User credentials for use on TWU Information Systems. This form shall be documented and provided to OHR and TWU Information Security. TWU Information Security will grant access based on least privilege.

2. University Affiliates shall have a set begin and end date for Information Resource access. Access shall be automatically disabled after the end date.

3. TWU Information Security shall monitor University Affiliate access end dates through reporting tools. Extensions to University Affiliate access shall be requested via the Service Request System by the Information Resource owner or business functional area supervisor.

4. University Affiliates are required to follow all information security policies, regulations, and procedures established by TWU when connected to any TWU Information System.

5. The business functional area supervisor of the University Affiliate must notify OHR and ITS of any personnel transfers or terminations of external personnel who possess organizational credentials or badges, or who have Information System privileges. This notification should be provided as soon as feasible, not to exceed the last day of employment. TWU Information Security will

make appropriate access modifications or terminations at notification of personnel transition.

6. Exiting University Affiliates and the business functional area supervisor of the University Affiliate shall retrieve and turn in all security-related TWU system-related property including but not limited to: Keys, Access Cards, Computer Equipment, Access Codes, authentication devices, and any passwords for additional systems or networks accessed by the University Affiliate.

7. It is the responsibility of the TWU Information Resource owner or business functional area supervisor of the University Affiliate to monitor compliance with all applicable information security controls.

G. Personnel Sanctions

1. Non-compliance with URPs and information security controls are subject to corrective and disciplinary action in accordance with URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes, URP 05.600: Staff Standards of Conduct and Disciplinary Process, and URP 06.200: Student Code of Conduct.

II. Regulatory Compliance

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

1. PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, and PS-8.

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, 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

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

Office of Human Resources Guide for Exiting Employees

URP 01.320: University Policy Development and Implementation

URP 04.710: Information Security Access Control

URP 05.205: Employment Practices

URP 05.255: Criminal Background Checks

URP 04.440: University Affiliate Criminal Background Checks

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

Office of Human Resources Employee Checklist for Separation

Office of Human Resources Management Checklist for Faculty/Staff Separation

IT Solutions Affiliate Access Form

Service Request System

Publication Date: 07/02/2021

Revised: 03/03/2022; 09/13/2023