Texas Woman's University
University Regulation and Procedure

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

POLICY STATEMENT

This document establishes the information personnel security regulations and procedures. The purpose of these regulations and procedures are to manage Texas Woman's University's ("TWU") risks from inadequate and ineffective: personnel screening; termination processes; and management of third-party access through the establishment of an effective security planning program.

APPLICABILITY

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

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

3. "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, 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.

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

5. "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, and a person who has been admitted or readmitted to TWU.

6. "Third-party" means a person who is not paid through TWU's payroll system or an organization that is not directly governed by TWU's Board of Regents.

REGULATION AND PROCEDURE

I. Scope

The scope of these regulations and procedures are 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.

II. General Guidelines

The State of Texas has chosen to adopt the personnel security principles established in NIST SP 800-53 "Personnel Security," Control Family guidelines. The following subsections outline the personnel security standards that constitute TWU's regulations and procedures.

A. PS-1 Personnel Security

1. Regulations

TWU Information Systems must develop, adopt or adhere to a formal, documented personnel security regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. Procedures

IT Solutions (“ITS”) will maintain regulations and procedures for personnel security regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

B. PS-2 Position Risk Designation:

1. Regulations

TWU must:

a. Assign a risk designation to all positions; and

b. Establish screening criteria for individuals filling those positions.

2. Procedures

The Office of Human Resources (“HR”) has designated all positions to be security sensitive; therefore, all applicants will be subject to background check.

C. PS-3 Personnel Screening

1. Regulations

TWU must screen individuals prior to authorizing access to information systems.

2. Procedures

a. TWU HR has designated all positions to be security sensitive and requires every individual to go through the same pre-screening and background check process that is further outlined in the URP 05.205: Recruitment, Search, and Selection.

b. A minimum criminal background check (information already available in the public domain) will be completed on all final employment candidates (Staff and Faculty) by TWU HR employment personnel. Out of state background checks are required for all candidates that have lived in states other than Texas within the last 7 years. Out of state background checks may take longer to complete.

c. TWU HR has developed a Notification and Authorization to Obtain (“NAO”) information liability release form (included in

the application packet) for employment information gathered during the background and selection process for all applicants. Details are provided in the Human Resources URP 05.255: Background Investigations, Employment and Credential Verifications, and Reference Checks.

D. PS-4 Personnel Termination

1. Regulations

Upon termination of individual employment, TWU must:

a. Disable Information System access;

b. Terminate/revoke any information security account associated with the individual;

c. Retrieve all security-related organizational information system-related property; and

d. Retain access to organizational information and Information Systems formerly controlled by terminated individual.

2. Procedures

a. Personnel Termination is managed in HR and supported by automated Information system account process managed by ITS. Account access is automatically disabled when employment is ended.

b. Upon termination, employees must follow the Guide for Exiting Employees provided by TWU HR 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 checklists for removing user possession or access including but not limited to; Keys, Access Cards, Computer Equipment, ID Cards, Access Codes, Long Distance Codes, and any passwords for additional systems/networks accessed by the employee.

E. PS-7 Third-Party Personnel Security

1. Regulations

TWU must:

a. Establish personnel security requirements including security roles and responsibilities for third-party providers;

b. Require Third-Party providers to comply with personnel security regulations and procedures established by the university;

c. Document personnel security requirements;

d. Require Third-Party providers to notify TWU of any personnel transfers or terminations of Third-Party personnel who possess organizational credentials and/or badges, or who have information system privileges; and

e. Monitor provider compliance.

2. Procedures

a. Third Parties, including contractors and Third Party application providers ("ASP"), are required to follow all information security policies, regulations, and procedures established by TWU when connected to any TWU information system.

b. TWU requires that all ASP disclose who amongst their personnel will have access to the environment hosting the application used by TWU.

c. TWU requires that all ASP disclose the background check procedures they use prior to being utilized by TWU as an ASP.

d. All contractors being utilized by Texas Woman's University must complete the Guest Access form prior to being granted user credentials for use on TWU Information Systems.

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 Standards of Conduct Corrective Action Guidelines 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

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 04.710: Information Security Access Control

URP 05.205: Recruitment, Search, and Selection

URP 05.255: Background Investigations, Employment and Credential Verifications, and Reference Checks

URP 02.330: Faculty Standards of Conduct Corrective Action Guidelines

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 Guest Access Form

Publication Date: 07/02/2021

Revised: 07/02/2021