Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Configuration Management**
Regulation and Procedure Number:	**URP: 04.730**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

Defined configuration management protects Texas Woman's University's ("TWU" or "University") Production Systems from disruption. The purpose of this University Regulation and Procedure ("URP") is to establish policy and procedures for controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after Information System implementation.

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

4. "Information System Component" means a discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an Information System.

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

6. "Production System" means a system being used for current operations. A production system is different than a test or development system, which are not used for operational purposes.

7. “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.

8. “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.

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.

9. "User" means an individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

REGULATION AND PROCEDURE

I. Security Standards

A. Baseline Configuration

1. TWU establishes baseline configuration of Information Systems to ensure changes to Information Systems are executed consistently in the Production environment.

2. The Information System Owner, or designee, shall develop, document, and maintain a current baseline configuration for the Information System.

3. Each type of platform or device may have its own particular baseline security configuration and maintenance protocols. Custodians of Information Systems shall seek and implement recommended configurations (based on manufacturer recommendations or industry best practices) for securing the particular system platforms under their control.

4. Baseline configurations shall be reviewed periodically including when Information System components are installed or upgraded.

B. Configuration Change Control

1. IT Solutions ("ITS") management determines the types of changes to the Information System that are configuration-controlled.

2. ITS coordinates and provides oversight for configuration change control activities through the ITS Change Advisory Board ("CAB") that convenes weekly to review proposed changes to production Information Systems.

3. The CAB reviews proposed configuration-controlled changes to the Information System and approves or disapproves such changes with explicit consideration for security impact analyses.

4. The CAB documents configuration change decisions associated with the Information System.

5. The implementer documented on the change request implements CAB approved configuration-controlled changes to the Information System.

6. The CAB shall retain records of configuration-controlled changes to the Information System for as long as the production Information System is in place.

7. ITS audits and reviews activities associated with configuration-controlled changes to the Information System as needed.

C. Security Impact Analyses

1. All security-related Information System changes in the Production environment shall be approved by the CAB through the change control process.

2. CAB approval shall occur prior to implementation by the TWU change implementer or University Affiliate.

D. Access Restrictions for Change

1. The Information System Owner, or designee, shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the Information System complying with existing University Regulations and Procedures and Security Controls. Information System Owners shall permit only qualified and authorized individuals to access Information Systems for purposes of initiating changes, including upgrades and modifications.

E. Configuration Settings

The Information System Owner, or designee, shall:

1. Establish and document mandatory configuration settings for components employed within the Information System;

2. Configure the security settings of Information System Components to the most restrictive mode consistent with operational requirements;

3. Identify, document, and approve any deviations from established configuration settings;

4. Implement and enforce the configuration settings in all components of the Information System; and

5. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

F. Least Functionality

The Information System Owner, or designee, shall:

1. Configure the Information System to provide only essential capabilities; and

2. Prohibit or restrict the use of unnecessary ports, protocols, or services.

G. Information System Component Inventory

The Information System Owner, or designee, shall:

1. Develop and document an inventory of Information System Components that:

   a. Accurately reflects the current Information System;

   b. Includes all Components within the authorization boundary of the Information System;

   c. Does not include duplicate accounting of components assigned to any other Information System;

   d. Is at the level of granularity deemed necessary for tracking and reporting; and

   e. Includes enough information deemed necessary to achieve effective Information System Component accountability; and

2. Review and update the Information System Component inventory annually.

H. Software Usage Restrictions

The Information System Owner, or designee, shall:

1. Use software and associated documentation in accordance with contract agreements, copyright laws, and TWU URP 04.700: Computer & Software Acceptable Use Policy;

2. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

3. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

I. User-Installed Software

1. Per TWU's URP 04.700: Computer & Software Acceptable Use Policy, Users shall only use standard and approved software included on the TWU standard software list and respect the licensing agreements of all software. Any use of non-standard shareware or freeware software requires ITS approval.

2. Installation of software shall be limited to ITS Employees and Users with authorized administrative privileges. Unauthorized software installation is prohibited.

3. ITS shall monitor installed software on TWU assets annually.

4. For instances in which the TWU department or academic component is the owner or custodian of the Information System hosting the software, the department or academic component is responsible for monitoring User installation of software and ensuring compliance with this Control.

II. Regulatory Compliance

A. The State of Texas has chosen to adopt a select number of Configuration Management ("CM") principles established in NIST SP 800-53 "Configuration Management" guidelines. The NIST CM controls have been assigned a number; however, the State of Texas has not adopted every NIST CM control, so there are gaps in the numbering sequence. The

following subsections outline the CM standards included in TWU's regulations and procedures.

1. CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-10, and CM-11.

III. Compliance

Employees that violate this policy are subject to corrective and disciplinary action, including and up to dismissal, in accordance with TWU's 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

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

Texas Government Code § 2054.068

Texas Labor Code § 412.054

URP 01.320: University Policy Development and Implementation

URP 04.700: Computer & Software Acceptable Use Policy

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

None

Publication Date: 07/02/2021

Revised: 03/03/2022; 01/08/2024