Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Supply Chain Risk Management**
Regulation and Procedure Number:	**URP: 04.783**
Policy Owner:	**Information Technology Solutions and Finance and Administration**

POLICY STATEMENT

This policy establishes Texas Woman's University's ("University" or "TWU") information security supply chain risk management regulations and procedures. The purpose of these regulations and procedures is to detail the controls used to manage TWU's information security supply chain risk.

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, 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 Websites, 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 Security Officer (“ISO”)” means a designated position required by the State of Texas for each institution of higher education. The ISO is responsible for monitoring the effectiveness of Information Resources security Controls and for administering the Information security program. The designated ISO at TWU is the Associate Director of Information Security.

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

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

6. “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.

7. “Supplier” means an organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of Information Systems, system components, or Information System services;

Information System integrators; vendors; product resellers; and third party partners.

8. "Supply Chain" means a linked set of resources and processes between multiple tiers of Suppliers or developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

9. "Supply Chain Risk Management" means a systematic process for managing cybersecurity supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products and services, or the supply chain.

10. "System Component" means a discrete identifiable information technology that represents a building block of an Information System and may include hardware, software, and firmware.

11. "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:

    1. 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.

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

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

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

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

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

REGULATION AND PROCEDURE

I. Security Standards

A. Supply Chain Risk Management Plan

1. The ISO shall develop and implement a plan for managing Supply Chain cybersecurity risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of Information Systems, System Components, or Information System services.

2. The Supply Chain Risk Management Plan shall be reviewed and updated annually, or as required, to address threats and organizational or environmental changes.

3. The Supply Chain Risk Management Plan shall be protected from unauthorized disclosure and modification.

B. Supply Chain Controls and Processes

1. The ISO shall:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of Information Systems and System Components in coordination with personnel responsible for Supply Chain activities;

b. Employ security controls to protect against supply chain risks to the Information System, System Component, or Information System service to limit the harm or consequences from supply chain-related events; and

c. Document the selected and implemented supply chain processes and controls in the Supply Chain Risk Management Plan.

C. Acquisition Strategies, Tools, and Methods

The Information System Owner, or their designee, shall employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks. *See* URP 04.765: Information Security for System and Services Acquisition for additional security controls that pertain to acquisitions.

D. Notification Agreements

The ISO, in coordination with Procurement and Contract Services and the Office of General Counsel, shall establish agreements and procedures with entities involved in the supply chain for the Information System, System Component, or Information System service for the notification of supply chain compromises and the results of assessments or audits.

E. System Component Disposal

The Information System Owner, or their designee, is responsible for the disposal of data, documentation, tools, or system components using techniques and methods outlined in security controls URP 04.743: Media Protection.

II. Regulatory Compliance

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

1. SR-1, SR-2, SR-3, SR-5, SR-8, and SR-12.

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 Control Standards Catalog

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 04.743: Media Protection

URP 04.765: Information Security for System and Services Acquisition

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: 11/01/2024

Revised: (MM/DD/YYYY)