Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security for System and Services Acquisition**
Regulation and Procedure Number:	**URP: 04.765**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This University Regulation and Procedure ("URP") establishes the information security for system and services acquisition regulations and procedures. The Controls within this URP help Texas Woman's University ("TWU") define security requirements for acquisitions and manage risks associated with the acquisition of security system and services that are incompatible with existing systems, expose existing systems to additional risk, or are otherwise not aligned with TWU's mission.

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. "Data Owner" means an individual who can authorize or deny access to certain data, and who is responsible for that data's accuracy, integrity, and timeliness.

2. "Control" means a safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e. confidentiality, integrity, and availability) that may be specified for an Information Resource. Controls may include security features, management

constraints, personnel security, and security of physical structures, areas, and devices.

3. “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.

4. “Guests” means any individual not affiliated with TWU.

5. “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.

6. “Information Resource Manager (IRM)” is responsible to the State of Texas for management of the agency’s Information Resources. The designation of an agency Information Resources manager is intended to establish clear accountability for setting policy for Information Resources management activities, provide for greater coordination of the state agency’s information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the

agency. The designated IRM at TWU is the Chief Information Officer ("CIO").

7. "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. The ISO also administers the institution's information security program. The designated ISO at TWU is the Associate Director of Information Security .

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

9. "Information System Component" means a discrete, identifiable technology asset (e.g., hardware, software, or firmware) that represent the building blocks of an Information System.

10. "Information System Service" is a capability provided by an information system that facilitates information processing, storage, or transmission.

11. "Privacy Officer ("PO") means the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals. The designated PO at TWU is the Data Management Officer.

12. "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.

13. "System Development Life Cycle (SDLC)" is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.

14. "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.

15. "University Data" is all data or information held on behalf of TWU, created as a result and/or in support of TWU business, or residing on TWU's Information Resources, including paper records.

16. "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. Allocation of Resources

IT Solutions ("ITS") shall follow the following process in determining information security and privacy requirements for the Information System or Information System Service in mission and business process planning:

1. Business functional areas may request to procure or acquire an Information System or Service in line with URP 04.360: Purchase of Goods and Services. Acquisitions must align with the University mission which may include capital planning (*See* URP 04.570: Capital Planning).

2. Depending on the nature of the Information System requested, the acquisition may be reviewed by the Information Security Officer ("ISO") and the Privacy Officer ("PO") for additional recommendations regarding security and privacy resources.

3. ITS will determine, document, and allocate resources to an acquisition once security and privacy requirements have been defined to protect the Information System or Information System Service as part of the organizational capital planning and investment control process.

4. Risk assessments are conducted for all Information System or Information System Service requests to identify potential security risks. Risk levels will be assigned as low, medium, and high. High risk requests require approval and signature of the Information Security Officer ("ISO"), Information Resource Manager ("IRM"), Data Owners, and Chancellor and President before proceeding to the next step in the process. If a request involves services to be provided by a third-party vendor whose product is designed to store TWU Data, a Higher Education Community Vendor Assessment Toolkit ("HECVAT") will be requested.

5. A discrete line item for information security and privacy in organizational programming and budgeting documentation will be established.

6. ITS will prioritize acquisition goals based on requirements, highest priority, and the current budget. When new resources are needed, ITS will submit a proposal to the Vice President for Finance and Administration, including a budget justification.

7. ITS will submit the proposed budget to the Finance and Administration Budget Office. The Finance and Administration Budget Office presents the budget for consideration to the Vice President for Finance and Administration and Board of Regents. Once the operating budget is adopted, ITS adjusts the proposed budget to reflect the approved financial plan.

B. System Development Life Cycle ("SDLC")

ITS will establish a SDLC to manage Information Systems.

1. The SDLC will:

   a. Ensure the confidentiality, integrity, and availability throughout the Information System life cycle;

b. Assess information security risks, security testing and audit controls to be included in all phases of the SDLC or acquisition process;

c. Define and document information security and privacy roles and responsibilities;

d. Identify individuals with information security and privacy roles and responsibilities;

e. Apply security and privacy controls appropriate to the University Data that is stored or processed by the information system;

f. Integrate security and privacy risk management protocols into all stages;

g. Ensure documentation of all activities associated with the SDLC;

h. Require certification by the Data Owner that the Information Resource is operationally secure and acceptable for use; and

i. Provide for security and privacy reviews to be conducted when an Information System has been modified or updated to ensure that the security of the Information System has not been compromised.

C. Acquisition Process

ITS shall include security and privacy requirements and specifications, either explicitly or by reference, in the evaluation of acquisition contracts for any Information System, Information System Component, or Information System Service during the risk assessment and acquisition processes. Possible security and privacy requirements and specifications may also be included in the contract in accordance with applicable laws and standards.

Risk assessment may include:

1. A description of the security and privacy functional and strength requirements of the Controls to be implemented;

2. A description of the environment in which the Information System is intended to operate; and

3. Security-related and privacy-related documentation for the Information System, Information System Component, or Information

System Service and the requirements for protecting the documentation.

Acquisition contracts may include:

1. Security and privacy functional requirements;

2. Strength of mechanism requirements;

3. Security and privacy assurance requirements;

4. Controls needed to satisfy the security and privacy requirements;

5. Security and privacy documentation requirements;

6. Description of the system development environment and environment in which the system is intended to operate;

7. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management;

8. Privacy requirements for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function;

9. Certification of security posture for cloud service providers (such as Software-as-a-Service ("SaaS"), Infrastructure-as-a-Service ("IaaS") or Platform-as-a-Service ("PaaS")) in accordance with the Texas Risk and Authorization Management Program ("TX-RAMP"); and

10. Any other applicable acceptance criteria.

B. Information System Documentation

ITS is responsible for obtaining or creating required documentation and ensuring distribution to appropriate individuals by:

1. Obtaining or developing administrator documentation for the Information System, Information System Component, or Information System Service that describes:

   a. Secure configuration, installation, and operation of the system, component, or service;

b. Effective use and maintenance of security functions/mechanisms; and

c. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

2. Obtaining or developing User documentation for the Information System, Information System Component, or Information System Service that describes:

a. User-accessible security and privacy functions and mechanisms and how they effectively use those security functions and mechanisms;

b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

c. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

3. Documenting attempts to obtain Information System, Information System Component, or Information System Service documentation when such documentation is either unavailable or nonexistent and take appropriate action in response;

4. Protecting documentation and limiting access to only those authorized; and

5. Distributing documentation to authorized personnel.

C. Security and Privacy Engineering Principles

1. ITS shall apply Information System security and privacy engineering principles in the specification, design, development, implementation, and modification of the Information System and Information System Components. These principles may include:

a. Layered protections;

b. Sound security and privacy policy, architecture, and controls as the foundation for design;

c. Security and privacy requirements incorporated into the System Development Life Cycle;

d. Physical and logical security boundaries;

e. System developers that are trained to build secure software;

f. Security controls tailored to meet organizational and operational needs;

g. Threat modeling used to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and

h. Informed risk management decisions.

D. External Information System Services

The following security controls will govern all external information system services implemented outside of TWU informational systems.

1. General Security

a. ITS may periodically request an audit of the application infrastructure assigned to TWU by the Application Service Provider ("ASP") or SaaS/IaaS/PaaS to ensure compliance with TWU policy and information security standards. The results of these audits may be requested by TWU. The ASP may limit the disclosure of these results to only include infrastructure that pertains to TWU.

b. ITS may request that the ASP or SaaS/IaaS/PaaS provide a proposed architecture document that includes a full network diagram of the TWU application environment, illustrating the relationship between the environment and any other relevant networks. The document may also include a full data flowchart that details where TWU data resides, what data will be collected, data fields required, the applications that manipulate it, and the security methods used to protect the data.

c. ITS will verify that the ASP or SaaS/IaaS/PaaS is able to remediate security issues in a timely fashion and/or have incident response procedures in place.

d. A current System and Organization Controls ("SOC") 2 Type 2, ISO 27001, or HITRUST certification report provided by the vendor may be accepted as a substitute for a HECVAT, with approval of the ISO. If the vendor fails to provide the requested report(s) and/or assurances, they will be required to execute a HECVAT.

e. The ASP or SaaS/IaaS/PaaS must maintain the appropriate TX-RAMP (or equal) certification throughout the life of the contract.

f. The ASP or SaaS/IaaS/PaaS must provide a written statement that upon contract termination, the hosting facility storage device containing TWU data will be degaussed, physically destroyed, or deleted using the destruction methods described in the DoD 5220.22-M data erasure standard. Upon completing data destruction, the ASP or SaaS/IaaS/PaaS must provide attestation to TWU certifying the data was destroyed.

2. Physical Security

a. The equipment hosting the application for TWU should be located in a physically secure facility, which requires logged access at a minimum.

3. Network Security

a. Sensitive information transmitted over the ASP or SaaS/IaaS/PaaS network must be encrypted at all times.

4. Host Security

The ASP must provide the following information upon request:

a. How and to what extent the hosts comprising the TWU application infrastructure have been hardened against attack. If the ASP or SaaS/IaaS/PaaS has hardening documentation, provide that as well.

b. A listing of current patches on hosts, including host Operating System (“OS”) patches, web servers, databases, and any other material application.

c. Information on how and when security patches will be applied.

d. Processes for monitoring the integrity and availability of hosts.

e. Information on their password policy for the TWU application infrastructure.

f. A list of possible authentication methods to the TWU application. TWU will not provide internal usernames/passwords for account generation.

g. Information on the account generation, maintenance and termination process for both system administration and user accounts.

5. Web Security

The ASP must provide the following information upon request:

a. The specific configuration files for any web servers and associated support functions (such as search engines or databases) that pertain to the TWU application.

b. Information pertaining to all programming languages used to develop the TWU application.

c. Information regarding any security and/or quality assurance testing performed on the web application.

d. Information regarding its code review process and vulnerability remediation process.

6. Cryptography

When protecting sensitive information, any symmetric, asymmetric, or hashing algorithm utilized by the TWU application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community. Connections between TWU Information Resources and an ASP or SaaS/IaaS/PaaS utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, TLS, SSH/SCP, PGP.

7. ITS shall define and document organizational oversight and user roles and responsibilities with regard to external system services.

E. Developer Configuration Management

1. Changes to the Information System, Information System Component, or Information System Service will be tracked as follows:

a. Authorized changes shall be tracked in the SDLC to ensure appropriate management and control of the changes, and to prevent unauthorized changes.

b. All application access-related changes to Information Resources shall be approved by the Data Owner through a change control process managed by the Service Request System.

c. Changes in Production environments must be reviewed and approved by the ITS Change Advisory Board prior to change implementation.

d. Authorized changes will also be tracked by Data Owners using tools appropriate to their assigned Information System.

2. All Users must report information security flaws using the Service Request System.

F. Developer Testing and Evaluation

The developer of the Information System, Information System Component, or Information System Service, at all post-design stages of the System Development Life Cycle, shall:

1. Develop and implement a plan for ongoing security and privacy control assessments;

2. Perform unit, integration, system, and regression testing/evaluation at regular intervals;

3. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

4. Implement a verifiable flaw remediation process; and

5. Correct flaws identified during testing and evaluation as appropriate.

G. Unsupported Information System Components

ITS shall:

1. Replace Information System Components when support for the components is no longer available from the developer, vendor, or manufacturer; or

2. Provide an in-house or external source for continued support of unsupported Information System Components.

II. Regulatory Compliance

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

1. SA-1, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-11, and SA-22

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

1 Tex. Admin. Code Ch. 202.

NIST Special Publication 800-53 (Rev. 5)

Texas Department of Information Resources Security Standards Catalog

DoD 5220.22-M Data Erasure Standard

Higher Education Community Vendor Assessment Toolkit

American Institute of CPAs, SOC for Service Organizations: Information for Service Organizations

ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT

HITRUST Certification Resources

Texas Risk and Authorization Management Program (TX-RAMP)

URP 01.320: University Policy Development and Implementation

URP 04.360: Purchase of Goods and Services

URP 04.570: Capital Planning

URP 04.735: Information Security Identification and Authentication

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

HECVAT Tools

Service Request System

TWU Procurement Contract Routing Request

Publication Date: 07/02/2021

Revised: 12/15/2021; 03/26/2025