Texas Woman's University
University Regulation and Procedure

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

POLICY STATEMENT

This University Regulation and Procedure ("URP") establishes the information security system and services acquisition regulations and procedures, to 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 Texas Woman's University's ("TWU") mission.

APPLICABILITY

This policy is applicable to TWU Students, Employees, 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 Resources. 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, 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. If an agency does not designate an IRM, the title defaults to the agency’s Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

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 Director of Technology Infrastructure.

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. “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.

12. “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.

13. “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.

14. “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. General Guidelines

A. This URP applies to all Information Resources owned, operated, or controlled by TWU. All Users are responsible for adhering to this policy.

B. The scope of these regulations, processes, and procedures, applicable to all controls and standards established to meet the requirements of this URP, shall incorporate: (1) TAC Title 1, Part 10, Chapter 202; (2) NIST Special Publication 800-53 (Rev. 5); (3) the Texas Security Control Standards Catalog, Version 1.3 (2/26/2016); and (4) other required information resources owned or operated by TWU.

C. The State of Texas has chosen to adopt a select number of the principles established in NIST SP 800-53 “System and Service Acquisition,” Control Family guidelines. The NIST SA controls have been assigned a number; however, because the State of Texas has not adopted every NIST SA control, there are gaps in the numbering sequence. The following subsections outline the SA standards that constitute TWU’s regulations and procedures.

II. SA-1 System and Services Acquisition

A. Regulations

1. TWU must develop, document, disseminate, review, and update system and services acquisition regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

2. TWU must designate an individual or entity to manage the development, documentation, and dissemination of the system and services acquisition regulations and procedures.

B. Procedures

1. IT Solutions (“ITS”) is responsible for managing the development, documentation, and dissemination of the system and services acquisition regulations and procedures.

2. ITS, in coordination with Data Owners, will establish a process for the effective implementation of security Controls for services acquisition that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. ITS is responsible for establishing a schedule to review and update the process.

III. SA-2 Allocation of Resources:

A. Regulations

TWU must:

1. Determine information security requirements for the Information System or Information System Service in mission/business process planning;

2. Determine, document, and allocate the resources required to protect the Information System or Information System Service as part of its capital planning and investment control process; and

3. Establish a discrete line item for information security in organizational programming and budgeting documentation.

B. Procedures

ITS shall follow the following schedule in determining information security requirements:

1. Beginning in the Summer and continuing into the Fall semesters, ITS will perform an annual review of Information Resources that culminates with the creation of an annual report. The annual review process includes feedback from colleagues across TWU, review of best practice, internal metrics, and time to reflect on future trends in technology. The annual review process is also used to: 1) identify opportunities for continuous improvement; 2) inform the next fiscal year financial plan, and 3) allocate the resources required to protect the information systems. In addition, ITS will:

    a. Review requests for resources submitted to the Service Desk,

    b. Conduct meetings with department leaders, meetings with faculty, involvement with student committees, and

    c. Review requests on behalf of the Cabinet through the Vice President for Finance and Administration.

2. Depending on the nature of the Information System requested, the acquisition may be reviewed by the ITS Information Security Manager and the TWU Information Security Officer (“ISO”) for additional recommendations regarding security resources.

3. Toward the end of the Fall semester, ITS will develop actionable goals for the following fiscal year based on the information obtained during the annual review. The goals will be evaluated by ITS and Data Owners for alignment to the TWU strategic plan. This

evaluation will consider future resource availability and need, as well as trends in enrollment, input from TWU leaders, and changes in the field of technology. If the goal includes the acquisition of products and/or services, Data Owners will gather more information from the requestors and vendors when appropriate.

4. Risk assessments will be conducted for all software 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. By the end of January of each fiscal year, ITS and Data Owners will prioritize the established goals based on what is required, highest priority, and affordable under the current budget. When new resources are needed, ITS and the Vice President for Finance and Administration will submit a proposal, including a budget justification, to the Provost to be presented for approval by Board of Regents during its February meeting.

6. During March, Data Owners will make necessary adjustments based on the strategic plan approved by the Board of Regents and submit to ITS for review.

7. In August, the Vice President for Finance and Administration approves the final financial plan and Data Owners enter the plan into the ITS budget manager system to be used in the upcoming fiscal year.

IV. SA-3 System Development Life Cycle (SDLC):

A. Regulation

TWU must:

1. Manage information systems using a System Development Life Cycle (SDLC) that incorporates information security considerations;

2. Define and document information security roles and responsibilities throughout the SDLC;

3. Identify individual having information security roles and responsibilities; and

4. Integrate the organizational information security risk management process into the SDLC process.

B. Procedure

1. ITS will establish a SDLC to manage information security systems.

2. The SDLC will:

a. Ensure the confidentiality, integrity, and availability throughout the information 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 roles and responsibilities;

d. Identify individuals with information security roles and responsibilities;

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

f. Integrate 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 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.

V. SA-4 Acquisition Process:

A. Regulation

TWU must include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for any information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and TWU mission/business needs:

1. Security functional requirements;

2. Security strength requirements;

3. Security assurance requirements;

4. Security-related documentation requirements;

5. Requirements for protecting security-related documentation;

6. Description of the information 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; and

8. Acceptance criteria

B. Procedure

ITS will ensure that security requirements and/or security specifications are addressed in acquisition contracts for any Information System, Information System Component, or Information System Service during the risk assessment process. Possible security requirements and specifications to be included in the contract may include:

1. Require the developer to provide a description of the functional properties of the Controls to be implemented;

2. Require the developer provide design and implementation information for the Controls that includes: security-relevant external

system interfaces; high-level design; low-level design; source code or hardware schematics;

3. Require the developer to demonstrate the use of a SDLC process that addresses systems security, privacy, software development methods, testing, evaluation, assessment, verification, validation methods, and quality control processes;

4. Require the developer to deliver the system, component, or service with specific security configurations implemented and use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade;

5. Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted;

6. Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance Partnership (“NIAP”) approved protection profile for a specific technology type, if such a profile exists;

7. Require a FIPS-validated or NSA-approved cryptographic module for commercially provided information technology products that rely on cryptographic functionality to enforce its security policy;

8. Require the developer to produce a plan for continuous monitoring of control effectiveness that is consistent with TWU policies, regulations and procedures;

9. Require the developer to identify the functions, ports, protocols, and services intended for TWU use;

10. Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (“PIV”) capability implemented within organizational systems;

11. Include privacy requirements in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function;

12. Include organizational data ownership requirements in the acquisition contract; or

13. Require all data to be removed from the developer's system and returned to the organization within a specified time frame.

VI. SA-5 Information System Documentation:

A. Regulation

TWU must:

1. Obtain or develop 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. Obtain or develop 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. Document 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; and

4. Distributes documentation to appropriate personnel.

B. Procedure

ITS is responsible for creating required documentation and ensuring distribution to appropriate individuals, consistent with the Regulation above.

VII. SA-9 External Information System Services:

A. Regulation

TWU must:

1. Require that providers of external information system services comply with TWU information security requirements;

2. Define and document oversight and User roles and responsibilities with regard to external information system services; and

3. Employ processes, methods, or techniques to monitor security control compliance by external service providers on an ongoing basis.

B. Procedure

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”) 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 will require that the ASP 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 must 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 ensure that the ASP is able to immediately disable all or part of the functionality of the application when a security issue is identified.

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 Information Security Manager and 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 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 must provide a signed statement to TWU certifying the data was destroyed.

2. Physical Security

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

b. The ASP must identify personnel who will have access to the environment hosting the application for TWU.

c. The ASP must disclose their background check procedures before they are selected as a provider by TWU.

3. Network Security

a. The network hosting the application must have, at a minimum, a firewall separating the hosted application from the internet and any DMZ networks. The firewall must be configured using the “least privilege” methodology.

b. Sensitive information transmitted over the ASP 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 has hardening documentation, provide that as well.

b. A listing of current patches on hosts, including host 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. Encryption methods utilized must be listed within URP: I.19.g Information Security Identification and Authentication. Connections between TWU Information Resources and an ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP.

VIII. SA-10 Developer Configuration Management:

A. Regulation

TWU requires internal and external developers of Information Systems, Information System Components, and Information System Services to:

1. Perform configuration management implemented while Information Systems are operational;

2. Document, manage, and control the integrity of changes to the Information Systems;

3. Implement only organization-approved changes to the Information System;

4. Document approved changes to the Information System, Information System Components, and Information System Services and the potential security impacts of such changes; and

5. Track security flaws and flaw resolution within the Information System and report findings to the appropriate personnel.

B. Procedure

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

    c. 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.

IX. 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 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

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

URP 04.735: Information Security Identification and Authentication

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

HECVAT Tools

Service Request System

Publication Date: 07/02/2021

Revised: 07/02/2021