Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security System Communications Protection**
Regulation and Procedure Number:	**URP: 04.770**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This document establishes the information system communications protection regulations and procedures. The purpose of these regulations and procedures are to manage Texas Woman's University's ("TWU") risks from vulnerable system configurations, denial of service, data communication and transfer through the establishment of an effective system communications protection program.

APPLICABILITY

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

DEFINITIONS

1. "Cryptographic Key" means a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.

2. "Denial of Service" is when an attacker attempts to prevent legitimate users from accessing information or services.

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. "Explicit Indication of Use" includes, for example, signals to local users when cameras and/or microphones are activated, or remote desktop notification that they user is logged in.

5. "Guests" mean any individual not affiliated with TWU.

6. “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.

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

8. “Information System Communications” are data transmissions and system-to-system communications, including analyzing the identity of communicators (e.g., over the Internet, within the organization, private networks, etc.).

9. “Name/Address Resolution Service” serves to translate a name address, like a computer name, in a network into an address that a machine or network understands.

10. “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.

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 this policy. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

II. Regulations and Procedures

The State of Texas has chosen to adopt the information security system communication principles established in NIST SP 800-53 “System and Communication Protection,” Control Family guidelines. The following subsections outline the system and service acquisition standards that constitute TWU’s regulations and procedures.

A. SC-1 System and Communications Protection:

1. Regulations

TWU must develop, document, disseminate Information System and Communications protection 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 Information System and Communications protection that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

B. SC-5 Denial of Service Protection:

1. Regulations

TWU Information Systems must have protections against or reduce the effects of denial of service attacks.

2. Procedures

ITS Information Security and ITS Network and Unified Communications employ various systems, architecture, and

techniques to protect against denial of service attacks (e.g., DMZ, firewall, intrusion detection and/or other prevention systems).

C. SC-7 Boundary Protection:

1. Regulations

TWU must

a. Monitor and control communications at the external boundary of the network system and at key internal boundaries within the network system;

b. Implements subnetworks for publicly accessible communication devices that are separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with University security architecture.

2. Procedures

a. ITS Information Security and ITS Network and Unified Communications install information systems on TWU's network into zones. There must be a firewall between any of the zones. The firewall should be the only device to allow traffic between zones. Types of zones defined are as follows:

i. Administrative;

ii. Core business;

iii. Wireless/dorms; and

iv. Internet accessible.

b. As new services are implemented within TWU, they must undergo an assessment as where they best fit on the network using the following checklist:

i. Define zone list;

ii. Define zone hardening policy; and

iii. New systems must be classified to fit in zones.

D. SC-8 Transmission Confidentiality and Integrity:

1. Regulations

TWU Information Systems must secure confidential information during transition.

2. Procedures

Users must ensure that confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted.

E. SC-12 Cryptographic Key Establishment and Management:

1. Regulations

TWU must establish and managed cryptographic keys when cryptography is required by an Information System.

2. Procedures

ITS Information Security generates and manages cryptographic keys when needed by an Information System owner.

F. SC-12 Cryptographic Protection:

1. Regulations

TWU must implement cryptographic keys in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

2. Procedures

a. ITS Information Security implements cryptographic keys in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

b. Confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control must be encrypted.)

c. Confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-state organization owned computing device. The minimum algorithm strength for protecting confidential information is 128-bit.

G. SC-15 Collaborative Computing Devices:

1. Regulations

TWU must prohibit remote activation of collaborative computing devices unless users authenticate using TWU defined VPN and the computing device provides an explicit indication of use to users physically present at the devices.

2. Procedures

Users may not remotely activate a computing device unless they:

a. Are physically present; or

b. Authenticate using TWU defined VPN and the computing device provides an explicit indication of use to users physically present at the devices.

c. Any TWU purchased network enabled collaboration device must be assessed prior to purchase and evaluated through the risk assessment process and determined what controls are necessary at that time. If devices cannot meet the requirements of the control it will be noted in the risk assessment with recommendations from ITS Information Security for reducing the risk.

H. SC-20 Secure Name/Address Resolution Service (Authoritative Source):

1. Regulations

TWU Information Systems, specifically DNS, must:

a. Provide additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

2. Procedures

ITS Network and Unified Communications manages TWU DNS Information Systems that meet the standards set forth in this control.

I. SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver):

1. Regulations

TWU Information Systems, specifically DNS, requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

2. Procedures

ITS Network and Unified Communications manages TWU DNS Information Systems that meet the standards set forth in this control.

J. SC-22 Architecture and Provisioning for Name/Address Resolution Service:

1. Regulations

TWU must operate Information Systems that collectively provide name/address resolution service that are fault-tolerant and implement internal/external role separation.

2. Procedures

ITS Network and Unified Communications maintains internal DNS at all locations and external DNS at more than one location.

K. SC-39 Process Isolation:

1. Regulations

TWU Information Systems must maintain a separate execution domain for each executing process.

2. Procedures

TWU uses modern operating systems that support process isolation.

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 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

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

None

Publication Date: 07/02/2021

Revised: 07/02/2021