Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**System and Communication Protection**
Regulation and Procedure Number:	**URP: 04.770**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

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

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 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. "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. “Confidential Data Classification or Confidential Data” applies to the data that is private, confidential by law or otherwise exempt from public disclosure (i.e. exemptions under the Texas Public Information Act, Social Security Numbers, personally identifiable Medical and Medical Payment Information subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 C.F.R. 160, Driver's License Numbers and other government-issued identification numbers, Education Records subject to the Family Educational Rights & Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), financial account numbers or credit or debit card number in combination with any required security code or Access code permitting Access to an individual’s financial account, and/or other University Data about an individual likely to expose the individual to identity theft).

6. “Information” means data as processed, stored, or transmitted by a computer.

7. “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.

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

9. “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.).

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

11. “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.

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. “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.

14. "User" means TWU Employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. Denial of Service Protection

1. TWU Information Systems shall have protections against or reduce the effects of denial of service attacks (internal and external).

2. TWU Information Security and ITS Platforms and Unified Communications employ various systems, architecture, and techniques to protect against denial of service attacks (e.g., DMZ, firewall, intrusion detection, or other prevention systems).

B. Boundary Protection

1. TWU ITS shall:

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

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

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

2. TWU Information Security and ITS Platforms 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. Isolated Network;

ii. Business Network;

iii. Wireless/Student Housing Network; and

iv. Internet accessible.

C. Transmission Confidentiality and Integrity

1. TWU Information Systems shall secure the confidentiality of information during transmission.

2. Users must ensure that Confidential Information that is transmitted over a public network (e.g., the Internet) must be encrypted. The minimum algorithm strength for protecting confidential Information is 128-bit.

D. Cryptographic Key Establishment and Management

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

2. TWU Information Security generates and manages cryptographic keys when needed by an Information System Owner.

E. Cryptographic Protection

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

2. TWU Information Security shall generate, distribute and manage cryptographic keys using automated mechanisms with supporting procedures where feasible.

a. When automated mechanisms are not feasible, manual key generation, distribution and management may be used.

3. Select Users have access to access and generate cryptographic keys.

4. Users assigned or generating cryptographic keys shall appropriately secure public and private keys.

5. TWU Information Security shall revoke cryptographic keys when necessary.

6. The minimum algorithm strength for protecting Confidential information is 128-bit; however, a business functional area may choose to implement additional protections, including stronger encryption algorithms or key lengths.

F. Collaborative Computing Devices and Applications

1. With some exceptions, TWU shall prohibit remote activation of collaborative computing devices (e.g. networked white boards, cameras, and microphones, etc.) and applications. TWU Information Security ensures a standard (see Information Security Standard – Web Conferencing) is in place to:

a. Prohibit remote activation of collaborative computing devices unless authorized; and

b. Provide an explicit indication of use to Users physically present at the collaborative computing device.

G. Secure Name/Address Resolution Service (Authoritative Source)

1. ITS Platforms and Unified Communications shall ensure that TWU Information Systems, specifically the Domain Name Service (“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.

H. Secure Name/Address Resolution Service (Recursive or Caching Resolver)

1. ITS Platforms & Unified Communications shall ensure that 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.

I. Architecture and Provisioning for Name/Address Resolution Service:

1. ITS Platforms & Unified Communications shall ensure that TWU Information Systems that collectively provide name/address resolution service are fault-tolerant and implement internal/external role separation.

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

J. Process Isolation

1. TWU Information Systems shall maintain a separate execution domain for each executing system process.

2. TWU ITS shall use modern operating systems that support process isolation.

II. Regulatory Compliance

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

1. SC-1, SC-5, SC-7, SC-8, SC-12, SC-13, SC-15, SC-20, SC-21, SC-22, and SC-39.

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

URP 01.320: University Policy Development and Implementation

URP 04.795: Data Access and Use Policy

Information Security Standard - Web Conferencing

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: 03/25/2022