Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Media Protection**
Regulation and Procedure Number:	**URP: 04.743**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

The Texas Woman's University ("TWU" or "University") Media Protection policy and procedures provides guidance regarding the protection of digital and non-digital information system media, the assurance that access to information on information system media is limited to authorized Users, and the requirements that information system media is sanitized or destroyed before disposal or release for reuse.

This University Regulation and Procedure ("URP") is applicable to all Media 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. "Data Classification System" means the separation of University Data into the following categories:

    a. "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, or other University Data about an individual likely to expose the individual to identity theft).

b. "Agency Sensitive Data Classification" or "Agency Sensitive Data" applies to less-sensitive business Information that is intended for use within TWU. Its unauthorized disclosure could adversely impact TWU or its students, strategic partners, or Employees.

c. "Public Data Classification" or "Public Data" applies to Information that has been approved by TWU management or the State of Texas for release to the public. There is no such thing as unauthorized disclosure of this Information and it may be disseminated without potential harm.

d. "Business Functional Data Classification" or "Business Functional Data" applies to data relating to items, components, or processes that are sufficient to enable physical and functional processing of operations. Examples of data are: meta data (i.e., data defining other data), size, configuration, department structures, characteristics, functional characteristics, and performance requirements.

2. "Data Custodian" means an individual designated by the Data Owner who assists with the ongoing operational tasks of managing Information assets.

3. "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.

4. "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.

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

7. "Media" means digital or non-digital storage devices or systems. Digital Media may include, but are not limited to systems, diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives and other portable mass storage devices, compact disks, and digital video disks. Media also applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, tablets, and smart phones). Non-digital Media may include but are not limited to paper records/documents or microfilm.

8. "Media Protection" means the protection of digital and non-digital information system Media, the assurance that access to information on information system Media is limited to authorized users, and requirements that information system Media is sanitized or destroyed before disposal or release for reuse.

9. "National Institute of Standards and Technology ("NIST")" means a non-regulatory agency of the United States Department of Commerce that works in cooperation with various industries to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology.

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, or a person who has been admitted or readmitted to TWU.

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:

    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.

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

REGULATION AND PROCEDURE

I. Security Standards

A. Media Access

1. Access to Media containing Confidential or Agency Sensitive Data shall be restricted to authorized personnel using physical access controls and safeguards (such as a locked cabinet or office). Data Owners are responsible for authorizing User access to their respective Media.

2. Users shall not share or distribute Media with non-authorized Users.

3. Users should label and handle media according to Data Classification (i.e. Confidential, Agency Sensitive). If labeled Media is found in public, the Media should be reported to the Information Security Officer.

B. Media Sanitization

1. TWU-owned Media must be sanitized prior to disposal, release of TWU control, or release for reuse. Sanitization may be accomplished via overwriting or modifying the Media to make data unreadable or indecipherable, or physically destroying the Media. Users may make a Media sanitization request using the Service Request System.

2. Users shall only dispose of Media in accordance with state requirements and applicable University records retention schedules and Data Classification.

3. Media containing Confidential Data or Agency Sensitive Data, shall be disposed of if no longer in use or completely cleared before it is reassigned to a different User or disposing of it when no longer used consistent with the Department of Defense ("DoD") 5220.22-M data erasure standard. The appropriate Data Custodian is responsible for ensuring compliance with this standard.

C. Media Sanitization: Review, Approve, Track, Document, and Verify

1. The Data Custodian is responsible for documenting and tracking their respective Media throughout its lifecycle.

2. The Data Custodian shall review, approve, track, document, and verify Media sanitization and disposal actions.

3. The Data Custodian shall keep a record (electronic or hard copy) documenting the completion of the sanitization or destruction process (may be referred to as a "Certificate of Destruction"). The record should include the following information, as applicable:

a. Date of sanitization or destruction;

b. Description of the item(s) and serial number(s), if available;

c. Inventory number(s);

d. The process and sanitization tools used to remove the data or method of destruction; and

e. The name and address of the organization the equipment was transferred to.

D. Media Use

1. Media containing Confidential and Agency Sensitive Data must be encrypted.

2. Confidential and Agency Sensitive Data may be stored on removable Media if the Media is encrypted. Data Owners are responsible for authorizing Data storage on removable Media and ensuring encryption.

3. All removable Media containing Confidential or Agency Sensitive Data, shall have a clearly designated owner, accountable for ensuring all applicable security controls are met.

4. The use of Media that has no identifiable owner is prohibited on TWU Information Resources.

5. Personally-owned Media should not be used to store or transmit TWU Confidential and Agency Sensitive Data.

II. Regulatory Compliance

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

1. MP-1, MP-2, MP-3, MP-6, MP-6(1) and MP-7.

III. Compliance

Employees that violate this policy are subject to corrective and disciplinary action, including and up to dismissal, in accordance with 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

Texas Government Code §441.187 Destruction of State Records

DoD 5220.22-M Data Erasure Standard

URP 01.320: University Policy Development and Implementation

URP 01.310: Records Retention

URP 04.795: Data Access and Use

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

Service Request System

Publication Date: 01/11/2022

Revised: 09/13/2023