Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Data Access and Use Policy**
Regulation and Procedure Number:	**URP: 04.795**
Policy Owner:	**Information Technology Solutions**

POLICY STATEMENT

This University Regulation and Procedure ("URP") provides a framework for managing Texas Woman's University ("TWU") data assets based on value and associated risks and for applying the appropriate levels of security Controls to protect information as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. 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 Employees, Students, University Affiliates, and Guests.

DEFINITIONS

1. "Access" means the physical or logical capability to view, interact with, or otherwise make use of Information Resources.

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. "Production System" means a production system is a system being used for current operations. A production system is different from a test or development system, which are not used for operational purposes.

4. "Data" means all information, regardless of size or storage media, including email messages, system logs, and software (commercial or locally developed).

5. “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, and/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, and/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.

6. “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.

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

For example, server and application administrators and software developers may be considered data custodians.

8. “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.

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

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

11. “Information Resources” is 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.

12. “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. The designated IRM at TWU is the Deputy CIO.

13. "Information Security Officer ("ISO")" is 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 and for administering the Information security program. The designated ISO at TWU is the Director of Enterprise Services and Information Security.

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

15. "Production Information" includes all electronic Information used within or in support of a mission critical business function.

16. "Security Standards" are documented Controls specified for specific technology components, which when implemented, reduce risk of compromise (i.e. document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, Access Controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures).

17. "Sensitive Information" means Information that could be subject to release under an open records request but should be controlled to protect third parties. This includes data that meets the definition of Personally Identifiable Information under the Texas Business and Commerce Code §521.002(a)(1) and §521.002(a)(2), such as Employee records and gross salary Information. Other examples include but are not limited to emails, voicemails, instant messages, internal communications, and departmental procedures that might reveal otherwise protected Information.

18. "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.

19. “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.

20. “University Data” means 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.

21. “User” means an individual or automated application or process that is authorized Access to the resource by the Data Owner, in accordance with the Data Owner’s procedures and rules.

REGULATION AND PROCEDURE

I. General Guidelines

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

II. User Responsibilities

A. All Data Users who contact or handle Information that is classified as either Confidential Data or Agency Sensitive Data are expected to familiarize themselves with this URP and to consistently use these same ideas in their daily TWU business activities. Although this Policy provides overall guidance, to achieve consistent Information protection, Data Users are

expected to apply and extend these concepts to fit the needs of day-to-day operations.

B. The Data Classification System shall be used to ensure that only those Users with a legitimate and demonstrable business need are able to Access Sensitive Information. The Data Classification System, when combined with this URP, will protect TWU information from unauthorized disclosure, use, modification and deletion.

III. Data Owner Responsibilities

Data Owners and his/her designated representative are responsible for the following:

A. Ensuring access to, and use of Data is in alignment with institutional goals and objectives;

B. Approving Access and formally assigning Data Custodians for an Information Resource;

C. Determining Information Resources asset values;

D. Specifying data Control requirements and conveying them to Data Users and Data Custodians;

E. Specifying appropriate Controls, based on a risk assessment, to protect the state's Information Resources from unauthorized modification, deletion, or disclosure. Controls shall extend to Information Resources and services outsourced by TWU;

F. Confirming that Controls are in place to ensure the confidentiality, integrity, and availability of data;

G. Assigning custody of Information Resources assets and provide appropriate authority to implement security Controls and procedures;

H. Reviewing Access lists based on documented risk management decisions;

I. Approving, justifying, documenting and holding oneself accountable for exceptions to security Controls. The Data Owner shall coordinate exceptions to security Controls with the Information Security Officer or Information Resource Manager; and

J. Classifying University Data as Confidential Data, Agency Sensitive Data, Public Data, or Business Functional Data in consultation with the Data Standards and Integrity Committee.

IV. Data Custodian Responsibilities

Data Custodians, including third party entities providing outsourced services relating to Information Resources, are responsible for:

A. Implementing Controls as specified by Data Owners;

B. Providing physical, technical, and procedural safeguards for Information Resources;

C. Assisting owners in evaluating the cost-effectiveness of Controls and monitoring; and

D. Implementing monitoring techniques and procedures for detecting, reporting and investigating incidents.

V. Data Owners

Type of Data	**Data Owner**
Academic Program Application Data	Program Director
External Constituent and Alumni Data	Vice President of Advancement
Applicant Data (Pre-admission)	Director, Admissions
Audit Data	Director of Internal Audits
Board of Regent Data	General Counsel
Budget Data	Director of Budget
Career Services	Director of Career Services

Type of Data	Data Owner
Employee Data	Director of Human Resources Professional Services
Electronic Protected Health Information (ePHI) / HIPAA Data	Director of Operations, Student Health Services
Facilities Data	Director of Physical Plant
General Ledger Data	Controller
Identification and Food Service Data	Director of Food Service and ID Systems
Institutional Research Data	Assistant Provost of Institutional Research and Data Management
Library Data	Dean of Libraries
Payroll Data	Director of Human Resources Employee Services
Public Safety Data	Director of Public Safety
Purchasing Data	Director of Procurement Services
Research Data	Primary Investigator
Student Academic Data (Post-admission)	Registrar
Student Disciplinary Data	Director, Civility and Community Standards
Student Financial Aid Data	Director of Financial Aid
Student Health Data	Director of Student Health Services

Type of Data	Data Owner
Student Housing Data	Director of University Housing
Technology Infrastructure and Security Data	Information Security Officer
Treasury Data	Controller

VI. Access Control

A. The proper Controls shall be in place to authenticate the identity of Users and to validate each User's authorization before allowing the User to Access Information Resources. Data used for authentication shall be protected from unauthorized Access. Controls shall be in place to ensure that only Users with the proper authorization and a legitimate and demonstrable business need are able to Access Information Resources. Remote Access shall be controlled through identification and authentication mechanisms.

B. Access to Sensitive Information will be provided only after documented authorization of the Data Owner has been obtained. Access requests will be presented to the Data Owner using an Access Request Form (for Affiliate Access) or a service request ticket. Custodians of the involved information will refer all requests for Access to the relevant Data Owners or their delegates. After receiving approval from the Data Owner, Data Custodians will grant the approved Access. Special needs for other Access privileges will be dealt with on a request-by-request basis. The list of individuals with Access to Confidential Data or Agency Sensitive Data must be reviewed periodically for accuracy by the relevant Data Owner.

C. All University Data on a Production System must have a designated owner. Data Owners are responsible for assigning appropriate classifications to University Data. Data Owners do not legally own the University Data entrusted to their care.

VII. Use of Data

A. University Data classified as Confidential Data must not be stored on a personally-owned computer, portable computer, personal digital assistant, or any other personally-owned single-user system.

B. Confidential Information stored in a public location that is directly accessible without compensating controls in place (e.g., File Transfer Protocol without access control) must be encrypted.

C. Confidential Information must be encrypted if copied to, or stored on, a TWU-owned portable computing device, or removable media.

D. If Agency Sensitive Data is going to be stored on a personally-owned computer, personal portable computer, personal digital assistant, or any other personally-owned single-user system, the system must conform to data Access Control safeguards approved by the Data Owner and the Data Custodian. When Users are not Accessing or otherwise actively using the system, they must log off the system, invoking a password protected screen saver or otherwise restricting Access to the Agency Sensitive Data.

E. If Agency Sensitive Data is to be transmitted over any external communication network (i.e. the internet or electronic mail systems), it must be sent in an approved encrypted form. All transmissions must use a Virtual Private Network ("VPN") or similar Access Controls as approved by the Data Owner and the Data Custodian. Departments transmitting Agency Sensitive Data will receive annual reviews to validate encryption protocols and procedures. Training on a secure transmission will be provided by IT Solutions ("ITS").

F. Before any Agency Sensitive Data may be transferred from one computer to another, the person making the transfer must ensure that Access Controls on the destination computer are commensurate with Access Controls on the originating computer. If comparable security cannot be provided with the destination system's Access Controls, then the information must not be transferred.

G. Storage media containing Sensitive Information, including 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 5220.22-M data erasure standard. The appropriate Data Custodian is responsible for ensuring compliance with this standard. Training on secure data storage and destruction will be provided by ITS.

VIII. Requesting User Information Collected

If users wish to review or correct any information held by TWU related to forms provided to TWU by the user, they are entitled upon request to ITS to receive and review the information and, as appropriate, update their incorrect information that is held by TWU. TWU complies with all applicable records retention laws and regulations.

VIV. Physical Security

TWU network equipment (routers, switches, etc.) and servers must be physically secured or locked in a location that denies Access to unauthorized personnel.

VV. Exception

Information owned by or under the control of the United States Government must comply with the federal classification authority and federal protection requirements.

VVI. 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

Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (1976)

Foreign Corrupt Practices Act of 1977, Pub. L. No. 95-213, 91 Stat. 1494 (1977) (codified as 15 U.S.C. §§78dd-1, et seq.)

Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474 100 Stat. 1213 (codified as amended in 18 U.S.C. §1030)

Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988) (codified as amended in scattered sections of 15 U.S.C. and 40 U.S.C.)

Family Education Rights and Privacy Act of 1974, 20 U.S.C.S. § 1232g (Law. Co-op. 2002)

Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999)

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002)

NIST Special Publication 800-128, 44 U.S.C. § 3502

Tex. Civ. Prac. & Rem. Ch. 134A

1 Tex. Admin. Code Ch. 202

Tex. Bus. & Com. Ch. 48, 521

Tex. Gov't Code Ch. 441, 552, 559, 2054

Tex. Penal Code Ch. 33, 33A

TWU Security Office: infosec@twu.edu

Payment Card Industry Data Security Standard

DoD 5220.22-M Data Erasure Standard

Department of Information Resources Security Standards Catalog

URP 01.320: University Policy Development and Implementation

URP 04.700: Computer & Software Acceptable Use Policy

URP 05.600: Staff Standards of Conduct and Disciplinary Process

URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes

URP 06.200: Student Code of Conduct

FORMS AND TOOLS

Affiliate Access Form

Publication Date: 07/02/2021

Revised: 09/07/2021