Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Computer & Software Acceptable Use Policy**
Regulation and Procedure Number:	**URP: 04.700**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

Texas Woman's University ("TWU") policies work to preserve the integrity of Information Resources, ensuring the contents of communications will not be tampered with, destroyed, stolen, and/or violated by misrepresentation. TWU encourages access to knowledge and to share that information, therefore contributing to TWU's mission of instruction, research and service.

TWU's Computer & Software Acceptable Use Policy applies equally to all individuals granted access privileges to any TWU Information Resources, and is established to ensure compliance with applicable statutes, regulations, and mandates regarding the management of Information Resources; establish prudent and acceptable practices regarding the use of Information Resources; and to educate individuals who may use Information Resources with respect to their responsibilities associated with such use. 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, University Affiliates, and Guests.

DEFINITIONS

1. "Artificial Intelligence ("AI") Systems" means systems capable of the following:

    a. Perceiving an environment through Data acquisition and processing and interpreting the derived information to take an action or actions or to imitate intelligent behavior given a specific goal; and

b. Learning and adapting behavior by analyzing how the environment is affected by prior actions.

2. "Automated Decision System" means an algorithm, including an algorithm incorporating machine learning or other artificial intelligence techniques, that uses data-based analytics to make or support governmental decisions, judgments, or conclusions.

3. "Automated Final Decision System" means an Automated Decision System that makes final decisions, judgments, or conclusions without human intervention.

4. "Automated Support Decision System" means an Automated Decision System that provides information to inform the final decision, judgment, or conclusion of a human decision maker.

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

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. “Faculty Member” means an individual who is employed by TWU as a member of the faculty and whose duties include teaching, research, service, and administration. Professional librarians and graduate assistant titles are excluded from the definition of faculty member.

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

11. "Information" means data as processed, stored, or transmitted by a computer.

12. “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.

13. “Information Resource Manager” 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.

14. “Information Security Officer” is responsible to the executive management for administering the information security function within the agency. The ISO is the agency’s internal and external point of contact for all information security matters. The designated ISO at TWU is the Director of Enterprise Services and Information Security.

15. “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.

16. “TWU Administration” means the organizational structure of TWU that is overseen by the Chancellor and President and includes employees responsible for the management and coordination of programs and activities for TWU consistent with the mission, goals, priorities and policies approved by the TWU Board of Regents.

17. “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.

18. “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.

19. “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. Procedures

A. Users may use only TWU Information Resources for which they are authorized. Users must not attempt to access any University Data for which they do not have authorization or explicit consent. Information Resources are intended primarily for activities related to accessing, sharing, and creating information, and collaborating with other members of this and other communities for scholarly and work-related communications. Secondarily, they are intended for use to enhance community service.

B. Users must report any weaknesses in TWU computer security, to include any incident of possible misuse or violation of this URP to IT Solutions ("ITS"). Users must not share their TWU account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or any other information device used for identification and authorization purposes (to include your TWU voicemail security code).

C. Users must respect the legal protection provided by copyright and licensing of programs, data, and intellectual property and must not make unauthorized copies of copyrighted software. (i.e., you shall not make copies of a licensed computer program to avoid paying additional license fees, to share with other Users, or to reproduce, in any form, protected works).

D. Users must only use standard and approved software included on the TWU standard software list. Any use of non-standard shareware or freeware software requires ITS approval.

E. Users must not purposely engage in activity that may: negatively impact the performance of Information Resources; deprive an authorized User access to an Information Resource; obtain extra resources beyond those allocated; circumvent TWU computer security measures.

F. Users must respect the privacy of other Users, and may not: intentionally seek information on, obtain copies of, or modify files, tapes, or passwords belonging to other Users; act on behalf of other Users, unless authorized to do so explicitly by those Users; or divulge sensitive personal data to which you have access concerning Students or Employees.

G. While using Information Resources, Users must respect the rights of other Users and must comply with policies, regulations and procedures, including policies prohibiting abuse, discrimination and harassment.

H. Users must not interfere or alter the integrity of Information Resources by:

1. Impersonating other individuals in communication;

2. Downloading, installing, or running security programs that reveal or exploit weaknesses in the security of a system. For example, Users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on Information Resources;

3. Destroying or altering data or programs belonging to other Users;

4. Using Information Resources that exceeds incidental use (as provided under this URP); or

5. Using Information Resources for illegal purposes, including not limited to violation of federal or state criminal laws.

I. Users must not intentionally access, create, store, or transmit material which TWU may deem offensive, indecent or obscene (other than in the course of academic activity or research where this aspect of the research has the explicit approval of the TWU official processes for dealing with academic ethical issues).

J. Access to the Internet from a TWU-owned, home-based computer must adhere to all the same policies that apply to use from within TWU facilities. Employees must not allow family members or other non-Employees to access TWU computer systems.

K. Users that remotely access TWU Information Resources from an off-campus location must ensure that Information Resources used at the remote location, in accordance with URP 04.710: Information Security Access Control:

1. Use secure network and access control mechanisms;

2. Secure the exchange of Information transferred between the remote location and TWU through use of the TWU Virtual Private Network (“VPN”) (for authorized Users);

3. Uphold current maintenance of Information Resources; and,

4. Prevent unauthorized viewing of confidential and Personally Identifiable Information (“PII”).

5. Users must also comply with all export control requirements for any information accessed while outside the United States.

L. Users must not otherwise engage in acts against the aims and purposes of TWU as specified in its governing documents or in policies, regulations and procedures.

M. Users must respect the intended usage of resources. Users shall only use those resources assigned to them by TWU for the purposes specified in the assignment and shall not access or use other such resources unless explicitly authorized to do so by executive-level authority.

N. Users must not use TWU resources assigned to them or others for personal profit-making or fundraising.

O. Users must respect the intended usage of systems for electronic exchange, and may not send spam, forged email/voice mail or chain mail that can interfere with the efficiency of the system. Also, User’s shall not access another User’s email/voice mail box or read/listen to another User’s electronic mail without that User’s explicit verbal or written permission.

P. Users must respect the integrity of the system or network, and shall not intentionally develop or use programs, transactions, data, or processes that harass other Users or infiltrate the system or damage or alter the software or data components of a system. Alterations to any system or network software or data component shall be made only under specific instructions from ITS.

Q. Users must adhere to all TWU policies, regulations, and procedures including, but not limited to, policies on proper use of Information Resources, information technology and networks; acquisition, use and disposal of TWU-owned property; use of telecommunications equipment; ethical and legal use of software; and ethical and legal use of administrative data.

R. Employees must complete and pass a Basic Information Security Awareness Course upon assignment to TWU and an Annual Refresher Course each year of employment.

S. ITS is not responsible for policing User activity. However, when made aware of violations, either through the normal course of duty or by a complaint, ITS will initiate an investigation. ITS may take action to preserve the state of files and other information relevant to an investigation, including suspension of a User's account privileges while an investigation is pending.

T. ITS acts in accordance with federal and state law, as well as TWU policy, regulation, and procedure governing privacy of User information by seeking permission to examine the content of User email and other private files. In instances where User permission cannot be obtained and the content of files or email may jeopardize the security of systems, safety of Users, or ability of TWU or its constituent parts to conduct necessary business, ITS must obtain authorization from executive level authority to examine the contents of a User's account.

II. Incidental Use

TWU resources are provided for the purpose of conducting TWU business. However, as a convenience to the TWU Users, incidental use of Information Resources is permitted. The following restrictions apply:

A. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to TWU approved Users. It does not extend to family members or other acquaintances.

B. Incidental use must not result in direct costs to TWU.

C. Users have no expectation of privacy regarding any University Data they create, send, receive, or store on TWU owned computers, servers, or other Information Resources owned by, or held on behalf, of TWU. TWU may access and monitor its Information Resources for any purpose consistent with TWU's duties and/or mission without notice.

D. Incidental use must not interfere with the normal performance of an Employee's work duties. Incidental use to conduct or promote the User's outside employment, including self-employment, is prohibited. Incidental use for purposes of political lobbying, or campaigning is prohibited.

E. No files or documents may be sent or received that may result in legal action or embarrassment to TWU.

F. Storage of personal email messages, voice messages, files and documents contained within TWU's Information Resources must be nominal.

G. All messages, files and documents including personal messages, files and documents located on TWU Information Resources are owned by TWU and may be subject to release in response to an open records request.

H. Incidental use must be consistent with federal and state law, and TWU policies, regulations and procedures.

III. Legal and Ethical Use of Software and Digital Material

A. TWU forbids, under any circumstances, the unauthorized reproduction of software or the use of illegally obtained software. Using TWU equipment to make illegal copies of software is prohibited. Employees and Students who violate this policy are subject to disciplinary action. Individuals who violate U.S. copyright law and software licensing agreements also may be subject to criminal or civil action by the owner of the copyright.

B. TWU, along with many other colleges and universities, supports the following statement from the EDUCOM Code, Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community, distributed by EDUCOM, a non-profit consortium of colleges and universities:

1. "Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy and right to determine the form, manner and terms of publication and distribution.

2. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, trade secret, and copyright violations, may be grounds for sanctions against members of the academic community."

C. TWU prohibits the use of its network for the unauthorized duplication, use, or distribution of copyrighted digital materials, regardless of the method

employed (e.g., web pages, peer-to-peer (P2P) file sharing, email, etc.). You must have fair use rights or authorization from the copyright holder for any material you use, make available, or share over the campus network.

D. Software programs are protected by Section 117 of the 1976 Copyright Act. Most TWU software is protected by federal copyright laws. Educational institutions are not exempt from these laws. Software is also protected by the license agreement between supplier and purchaser. Software provided by TWU can only be used on the computer equipment specified in the software license. It is against University policy to copy or reproduce any licensed software on University computing equipment, except as expressly permitted by the software license.

E. TWU will not install any software or hardware on a personal computer not owned by TWU. TWU will not provide technical assistance on non-university machines for computer problems and will not be responsible for repairing, replacing, or installing any hardware component or peripheral. TWU will not be responsible for any payment relating to consequential damages resulting from the installation or configuration of a network interface card and/or the configuration of any personal computer not owned by TWU for use on the TWU network.

IV. Internet Filtering

A. Filters are designed to restrict access to Web sites, newsgroups, and chat rooms by a variety of techniques. TWU utilizes content filtering to protect university systems.

1. Users are responsible for adhering to TWU's content filtering. Bypassing content filters is prohibited. Employees, University Contractors and Students who violate this policy are subject to disciplinary action.

2. ITS is responsible for configuring content filters for the TWU network. Any filtering decisions that address system performance, malicious activity, or threats to the information technology environment must be approved by the Change Advisory Board.

3. Other categorical filtering decisions that are of a topical/specific nature (i.e. Shopping, Nudity, Gambling, etc.) will be reviewed at minimum by ITS, the Vice President for Finance and

Administration, Human Resources, and Provost and will follow the change management process.

B. Employees that work remotely may not have all content filters and security controls applied to their computing environment without the use of TWU VPN. VPN connection to the TWU network is encouraged for all remote work.

V. Privacy Statement and Ownership of Electronic Files

A. The contents of communication across the TWU network are considered private to the fullest extent permitted by law. Electronic files created, sent, received, or stored on Information Resources that are owned, leased, administered, or otherwise under the custody and control of TWU are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code, Chapter 202 (Information Security Standards). In the normal course of doing their assigned work, some individuals, by virtue of their positions within TWU and their specific responsibilities, may have special access privileges to hardware and software and therefore, to the content that resides in those resources. TWU will strive to protect individual privacy by ensuring that the number of individuals with this level of access is strictly limited and that individuals placed in those positions are selected for their judgment and ethics, as well as their technical expertise. This Information may also be subject to the disclosure requirements under the Texas Public Information Act and the laws applicable to state records retention.

B. Ordinarily, access to a User's accounts and files require permission of the sender/recipient of the message or owner of the file (the person to whom the account ID is assigned). In the event of a TWU investigation for alleged misconduct, the contents of the account may be locked or copied to prevent destruction and loss of information and would require executive-level approval to view.

VI. Security

A. Users of TWU computing resources are expected to act responsibly to maintain the security of information stored on computing systems. Computer passwords, account names and other types of authorization assigned to a User must be safeguarded and not shared with others. Microcomputer Users must take the necessary steps to protect their systems from computer viruses and other destructive computer programs.

Each User should understand the level of file protection required by each computer system. Each department must determine and implement appropriate backup procedures, as necessary, to be followed to protect critical and sensitive information from loss.

B. All personnel are responsible for managing their use of Information Resources and are accountable for their actions relating to Information Resource security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

C. The use of Information Resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to: email, web browsing, and other electronic discussion tools. The use of these electronic communication tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of Information Resource utilization, the establishment of effective use, and reporting of performance to management.

D. Users are responsible for accessing, storing and securing University Data in the manner appropriate for their assignment, per TWU URP 04.795: Data Access and Use Policy. The type or classification of Information or the Information itself is the basis for determining whether the data must be kept confidential and secure. When the data classification is unknown, Users shall treat the University Data as confidential.

E. All computer software programs, applications, source code, object code, documentation, and data shall be guarded and protected as if it were state property.

F. Departments must provide adequate access controls in order to monitor systems to protect University Data from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled by each department’s Data Owner or designated Data Custodian.

G. All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The Information

Resource Manager reserves the right to remove any unlicensed software from any computer system.

H. The Information Resource Manager reserves the right to remove any non-business related software or files from any system, including games, instant messengers, pop email, music files, image files, freeware, and shareware.

VII. Academic Freedom Related to Electronic Communications

A. An important part of the identity of TWU is recognizing the need for personal expressions and insights by members of the campus community. The use of Information Resources infrastructure, both within TWU and beyond, provides a vehicle for those expressions and insights. The use of electronic communication requires all Users to act responsibly and professionally.

B. A Faculty Member should be free from institutional censorship or discipline, but each Faculty Member's position in the TWU community implies special obligations. The public may judge the profession and the institution by the Faculty Member's communications. The Faculty Member's obligations include: maintaining accuracy and currency of information at all times, exercising appropriate restraint, respecting the opinion of others, and stating clearly that they do not speak for TWU. These obligations exist in all communications, but are especially important with the global accessibility of electronic communications.

VIII. Risk Management

The TWU Administration adopted risk management guidelines in compliance with the Texas Administrative Code to identify and to set up technical and procedural mechanisms to make the information technology environment at TWU and its internal and external networks resistant to disruption and unauthorized access. Therefore, all technology-related acquisitions for TWU must undergo a risk assessment prior to use or purchase. The risk assessment will review network access along with security requirements, as directed by Texas Administrative Code, Chapter 202. The integrity of this resource is the responsibility of its Users who must guard against abuses that disrupt and/or threaten the long-term viability of the Information Resource systems at TWU and beyond. Access to the Information Resources is a privilege and must be treated as such by all Users. The use of the Information Resources constitutes acceptance of the terms and requirements of this URP, its inherent responsibilities, relevant laws, contractual obligations, and the highest standard of ethics.

IX. Communication Resources

A. Open communication within a diverse institution is critical to building a sense of community. Members of the community also strive for the most responsible use of the Institutional Resources. Therefore, limiting the number of purely personal communications is appropriate and reasonable. Users are encouraged to use communication resources such as electronic mail, audio/video and web conferencing systems, telecommunications, instant messaging, Short Message Service (SMS), facsimile transmission, social media, and other communications systems provided by TWU primarily for purposes related to accessing, sharing, creating Information, and collaborating with other members of this and other communities for scholarly and work-related communications. Secondarily, they are intended for use to enhance community service. Occasional and incidental social communications are not disallowed by this policy; however, each User should comply with specific policies of their individual units.

B. A supervisor concerned about an Employee's potential violation of this policy should consider the following:

1. Review whether or not standards and expectations in this area have been communicated to the Employee;

2. Pursue direct communication with the Employee regarding the issue; and

3. Proceed as one would handle any personnel-related disciplinary action.

X. Artificial Intelligence ("AI") Systems

A. All AI Systems used on TWU Information Resources with TWU Data are prohibited unless reviewed and approved in accordance with TWU URP 04.760: Risk Assessment and URP 04.765: Information Security for System and Services Acquisition.

1. The User shall submit a risk assessment to TWU Information Security. Information Security shall conduct a risk assessment of the AI System per URP 04.760 Risk Assessment. TWU Procurement will evaluate the acquisition in accordance with TWU policy and state regulations.

B. TWU Data classified as Confidential, Agency Sensitive, and Business Functional must not be used with public, open source AI Systems. Users interested in acquiring a licensed or private AI System to use with TWU Data must comply with Section X.A.

C. Public, open source AI Systems must not be used to generate TWU Data output that would be considered Confidential, Agency Sensitive, or Business Functional.

D. Click-through agreements used within AI Systems are considered contracts. TWU Users are prohibited from accepting click-through agreements without appropriate review and approval.

E. AI Systems must not be used for activities that may be considered a violation of state and federal regulations or TWU policies.

XI. Computer Lab Use

Access to Information Resources is for sharing information and for maintaining the security of the intellectual products of the academic community. Each User must accept responsibility to protect the rights of other Users. Any member of the TWU community who, without authorization, accesses, uses, destroys, alters, dismantles, or disfigures Information Resources, properties or facilities, threatens the atmosphere of increased access and sharing of information and the security within which members of the TWU community create intellectual products are subject to corrective and disciplinary action. Access to Information Resources is a privilege and must be treated as such by all Users. Members of the TWU community should strive for the most responsible use of the institution's resources. Users accept the responsibility to:

A. Respect the prohibition of using resources for any fraudulent and unlawful activities under applicable federal, state, or local laws, including the legal protection provided by copyright and licensing of programs and date;

B. Respect the privacy and rights of other Users; and

C. Respect the intended use of resources.

XII. TWU Web Sites

A. Only approved and authorized content managers maintained by the Office of Marketing and Communication shall update official TWU web pages.

B. Official TWU social media accounts shall be registered with the Office of Marketing and Communication. Content for each respective account shall be managed by a TWU Employee and must follow the Office of Marketing and Communication's published social media rules and guidelines.

C. TWU Employees that utilize digital curriculum vitae ("CV") web profiles to communicate their achievements in research, creative activities, scholarship, and teaching shall use the resource for professional purposes only and ensure that information is accurate and current.

D. It is encouraged that graphic and image use be evaluated for space allocation and accessibility. Any image of an individual used in a web page requires a signed release form on file at the Office of Marketing and Communication. If the individual is under 18 years of age, the release must be signed by a parent or guardian. Any protected work should not be used in a manner that violates copyright, patent protections, or license agreements. Any protected creative work should not be used as a graphic image without an appropriately signed release.

E. The same copyright and trademark laws of the United States that govern illegal copies of copyrighted material or the use of trademarks apply to the use of these materials on the TWU website. TWU is not responsible for any abuse of state and federal copyright or trademark laws that occur on User web pages or unofficial sites.

XIII. Information Collected, Stored Logs and Network Monitoring

A. TWU maintains log files of all access to its Web site and also monitors network traffic for the purpose of website management and security. This information is used to help diagnose problems with the servers and to carry out other administrative tasks. Log analysis tools are also used to create summary statistics to determine which information is of the most interest to Users, to identify system problem areas, or to help determine technical requirements. The following information is collected in these files:

1. Hostname: the hostname, site name, username, and IP address of the computer requesting access to the site.

2. User-Agent: the type of browser, its version, and the operating system of the computer requesting access.

3. Referrer: the web page the User came from.

4. System date: the date and time on the server at the time of access.

5. Full request: the exact request made by the User.

6. Status: the status code returned by the server.

7. Content length: the size, in bytes, of the file sent to the User.

8. Method: the request method used by the User.

9. Universal Resource Identifier (URI): the location of the information requested (aka URL).

10. Query String of the URI: anything after a question mark in a URI.

11. Protocol: the technical protocol and version used (e.g., http, ftp).

12. Cookies: a cookie is a small file containing information that is placed on a User's computer by a web server. Typically, these files are used to enhance the User's experience of the site, to help Users move between pages in a database, or to customize information for a User. TWU servers do not store personally identifiable information in cookies from pages intended for use by the general public. Information stored in cookies by TWU web servers is used for internal purposes only. It is not used in any way that would disclose personally identifiable information to outside parties unless TWU Administration is required to do so.

B. The above information is not used in any way that would reveal personally identifying information to outside parties unless TWU is legally required to do so. Web server logs are scheduled for regular destruction in accordance with the rules and regulations of the Texas State Library and Archives Commission.

XIV. Information Collected by Email and Forms

TWU collects the email addresses of individuals who communicate with us via email or who give us their email address. TWU collects information that is voluntarily provided by individuals who submit forms on our web site. If a member of the general public sends TWU an email message or fills out a web-based form

with a question or comment that contains personally identifying information, that information will only be used for the purposes for which the form is intended, to respond to the question, or comment and to analyze trends. The message or form may be redirected to another government agency or person who is better able to respond to the question or comment. TWU does not market such information. TWU does not use such information in any way that would reveal personally identifying information to outside parties unless legally required to do so.

XV. 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

Foreign Corrupt Practices Act of 1977

Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Digital Millennium Copyright Act of 1998

The State of Texas Information Act

Tex. Gov't Code § 441

Tex. Gov't Code, Ch. 2054

Tex. Adm. Code, Ch. 202

Tex. Adm. Code, Ch. 206

Tex. Admin. Code, Ch. 213

IRM Act, 2054.075(b)

Tex. Penal Code, Ch. 33 and 33A

DIR Practices for Protecting Information Resources Assets

DIR Standards Review and Recommendations Publications

Texas Department of Information Resources, Acceptable Use of the Internet, Guidelines for State Agencies and Institutions of Higher Education (Mar. 1, 2015)

Copyright Laws of the United States

EDUCAUSE

TWU Social Media Community Guidelines

TWU Standard Software

URP 01.320: University Policy Development and Implementation

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

URP 04.795: Data Access and Use Policy

URP 04.760 Risk Assessment

URP 04.710: Information Security Access Control

URP 04.765: Information Security for System and Services Acquisition

FORMS AND TOOLS

None

Publication Date: 07/02/2021

Revised: 09/07/2021; 11/07/2023