Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Technology Exceptions**
Regulation and Procedure Number:	**URP: 04.797**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

Texas Woman's University ("TWU" or "University") is committed to safeguarding its Information Resources and maintaining the security of data it collects or stores. All Users of TWU Information Resources are expected to adopt and adhere to information technology University Regulations and Procedures ("URP") and security Controls. However, TWU also recognizes that there may be urgent business needs or academic pursuits that require deviations from these policies, standards, and procedures. The purpose of this URP is to provide a process that documents an Information Resource owner's request for an exception to an information technology URP, security Control, standard or procedure, or an exception for personally-owned devices for telecommuting 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 Employees.

DEFINITIONS

1. "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.

2. "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.

3. "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 Information Resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

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 Security Officer ("ISO")" 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 Associate Director of Information Security.

7. "TWU Administration" means the organizational structure of TWU that is overseen by the Chancellor and President ("Chancellor") 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.

8. "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. Exceptions

The scope of these procedures is applicable to all Information Resources 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.

A. Exceptions to an information technology standard, procedure, URP, or required security Control may be granted by the Information Security Officer to address specific circumstances or business needs, relating to an individual program or department, only as authorized by applicable law and University policy.

B. The Information Security Officer may issue a single exception to address institution-wide risks or multiple situations.

C. Requests for exceptions may be submitted by any User within a TWU department or academic component. Documentation of approval by the User's supervisor, Data Owner, or TWU Administration may be required in the exception review process.

D. All exceptions must be documented.

E. All exceptions should be considered temporary solutions; therefore, all exception requests will expire. The maximum length of time that may be requested is one (1) year. It is the responsibility of the requestor to find a permanent solution before the exception request expires, or submit a new exception request with updated information.

F. Any User who wishes to be granted an exception from a policy (URP), standard, security Control, or procedure, must provide the following information relevant to the request:

1. Specific URP, standard, security Control, or procedure for which an exception is requested;

2. List of the systems, networks, or data for which the exception will apply. The list must include the fully qualified name of any servers (e.g., abc.twu.edu) and the category of data sensitivity (e.g., confidential data);

3. Business justification as to why this exception is being requested;

4. Details regarding the mitigating factors and compensating controls that will be used to offset the risk;

5. Length of time for which the exception is requested (e.g. three months, one year, etc.); and

6. Requestor's name, email address, and department or academic component and if applicable, technical person(s) name(s) and email address(es).

G. The TWU Information Security office will assess the level of risk associated with the proposed exception.

The level of risk will determine the additional approvals the User needs to obtain based on the following chart:

Resulting Risk from Exception	**Department Chair or Department Head (or designee) Approval Required**	**Vice President, Division Head, or Dean (or designee) Approval Required**	**Chancellor or TWU Administration designee Approval Required**
Low Risk	Yes	No	No
Medium Risk	Yes	Yes	No
High Risk	Yes	Yes	Yes

1. For example, an exception resulting in a “high risk” designation would require approvals from the following:

    a. Department Chair or Department Head or designee,

    b. The Vice President, Division Head, or Dean or designee, and

    c. The Chancellor or TWU Administration designee.

2. Note: University leaders, including academic deans, academic chairs, vice presidents, and TWU Administration Employees, may not approve their own exception requests. In such cases, either the supervisor of the requestor or a person in a similar position of authority, who is able to judge and accept the risk, business need, and appropriateness of the exception request for the unit, will be the designated authorizing official.

H. The Information Security Officer, or designee, will review the exception and provide the final decision. The Information Security Officer, or designee, may consult with other University stakeholders and senior administrators for input and clarification.

II. Requesting an Exception

Any User may initiate an exception request by using the Information Technology Solutions (“ITS”) Service Catalog Request an Exception for Information Technology URP, Security Control, Standard or Procedure Form, which guides Users through the policy exception request process:

A. After selecting the Service Catalog Request an Exception for Information Technology URP, Security Control, Standard or Procedure Form, the User enters the required information in the fields provided. Users may also upload supporting documentation.

B. Once the form is submitted, the request is assigned to TWU Information Security to review.

C. TWU Information Security will coordinate with ITS functional areas (if applicable) and work with the User to:

1. Assess the risks created by the exception,

2. Evaluate potential alternatives,

3. Provide recommendations, and

4. Determine the appropriate departmental and if applicable, Data Owner or TWU Administration approval(s), the User needs to obtain.

D. If applicable, the User will provide the appropriate approvals via the exception request.

E. The Information Security Officer, or designee, will review the exception and provide the final decision.

F. TWU Information Security will update the exception request with documented approval or denial of the request (along with request details) to the requestor or User for whom the exception was requested, copying the appropriate approvers.

1. If the exception is granted and approvals obtained, TWU Information Security will provide the User with additional assistance as needed, such as coordinating with the relevant Data Owner(s), Data Custodian(s) or other individual(s) who have a role in fulfilling the exception request. If the exception is granted, the ISO or their designee will set and document the expiration date of the exception. Exceptions will not be granted when feasible alternatives exist or risks outweigh the projected benefits.

2. If the exception is not granted, TWU Information Security will work with the User and the ISO to define a reasonable deadline for compliance.

3. If the exception is not granted, the User may appeal the decision to the Chief Information Officer ("CIO").

G. The User will be notified prior to expiration that the exception duration is ending. The User must then submit a new exception request or notify TWU Information Security that the exception is no longer needed.

III. Requesting an Exception for Personally-Owned Devices for Telecommuting

A. Per the Office of Human Resources' URP 05.620: Alternative Work Arrangements for Staff Employees, Employees are required to use University-owned and provided computers while telecommuting. Exceptions will be addressed on a case-by-case basis. If personally-owned equipment must be used, the personally-owned equipment must be enumerated, and rationale or justification documented as part of the alternative work agreement. Employees utilizing personally-owned equipment must adhere to the same mandated security requirements, and ensure their computer is up to date with patches.

B. Any Employee may initiate an exception request for personally-owned computers for telecommuting use by using the Request for Policy Exception - Use of Personally-Owned Computer for Telecommuting Form:

1. After selecting the Service Catalog Request for Policy Exception - Use of Personally-Owned Computer for Telecommuting Form, the Employee enters the required information in the fields provided. Employees may also upload supporting documentation.

2. The form must be completed by the Employee that owns the personally-owned device(s). The Employee's supervisor must also approve and verify the form for completeness and accuracy.

3. Once the form is submitted, the request is assigned to TWU IT Solutions for review.

4. The ISO, Information Resource Manager ("IRM") or their designee will update the exception request with documented approval or denial of the request (along with request details) to the requestor, copying the requestor's supervisor.

    a. If the exception is granted, the requestor may use the closed form with documented approval to support their request for alternative work arrangements with the Office of Human Resources.

    b. If the exception is denied, IT Solutions will work with the requestor to determine alternative solutions. If the requestor maintains that the personally-owned equipment originally submitted for exception is the only possible resource(s) to be used, an appeal may be made to the CIO.

IV. 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.

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. Adm. Code, Ch. 202

URP 04.700: Computer & Software Acceptable Use Policy

URP 04.795: Data Access and Use Policy

URP 05.620: Alternative Work Arrangements for Staff Employees

URP 05.600: Staff Standards of Conduct and Disciplinary Process

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

FORMS AND TOOLS

Request an Exception for Information Technology URP, Security Control, Standard of Procedure Form

Request for Policy Exception - Use of Personally-Owned Computer for Telecommuting Form

Publication Date: 08/25/2022

Revised: (MM/DD/YYYY)