Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Audit and Accountability**
Regulation and Procedure Number:	**URP: 04.720**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This document establishes the information security accountability, audit, and risk management regulations and procedures. This University Regulation and Procedure ("URP") helps Texas Woman's University ("TWU" or "University") implement security best practices with regard to managing risks from inadequate event logging and transaction monitoring.

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 Employees and University Affiliates.

DEFINITIONS

1. "Accountability" means the responsibility of either a person or a department to perform a specific function to verify the integrity and accuracy of organizational rules and processes.

2. "Events" means information or computer security-relevant information system actions that can be audited.

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. “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.

5. “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 Associate Director of Information Security.

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

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

8. “Time Stamp” means the current time of an event that is recorded by a computer.

9. “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.

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

REGULATION AND PROCEDURE

I. Security Standards

A. Event Logging

1. All TWU Information Resources must be capable of auditing the actions of Users deemed necessary by the Information Security Officer ("ISO").

2. TWU Information Security shall monitor the use of Information Systems, maintain security-related system logs, and retain logs in accordance with the University records retention schedule (*See* URP 01.310: Records Retention).

3. TWU Information Security shall coordinate the Event logging function with Information System Owners (or designees) requiring audit related information. This review will guide and inform the selection criteria for Events to be logged.

4. TWU logs the following types of Information System Events, which are deemed to be adequate to support after-the-fact investigations of incidents, and maintains ongoing logging of these Events, as they occur:

a. Diagnostic;

b. Administrative;

c. Transactional; and

d. Security.

5. IT Solutions (“ITS”) shall periodically review log Event types for effectiveness. Review and modification shall be coordinated with applicable Information System Owners, or designee(s).

B. Content of Audit Records

1. IT Solutions employs centralized audit logging systems that contain sufficient information to, at a minimum, establish what type of Event occurred, when (date and time) the Event occurred, where the Event occurred, the source of the Event, the outcome of the Event, and the identity of any User associated with the Event.

a. Information System Audit requirements:

i. Information System Owners shall be recorded by ITS.

ii. Information System data shall be classified in accordance with URP 04.795: Data Access and Use Policy.

iii. ITS managed monitoring systems are required for production, redundant, and failover servers.

a. Monitoring is optional for Development or Test servers.

iv. Information Systems must be configured to provide centralized logging managed by ITS.

C. Audit Log Storage Capacity

1. TWU Information Systems must allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.

2. ITS maintains capacity for one hundred and twenty (120) days’ worth of audit logs. Information System scripts will monitor available space and notify the appropriate individuals of high space utilization.

D. Response to Audit Logging Process Failures

1. TWU Information Systems must alert designated University officials in the event of an audit logging process failure. ITS utilizes

automated email alerts to inform the Associate Director of Information Security of failure. The Associate Director of Information Security then determines the source of the problem and coordinates with appropriate team members that are responsible for the failure.

2. TWU Information Systems must be configured to take appropriate actions during an audit log failure. In the event of a failure, systems are configured to either shut the system down, begin overwriting old logs, stop processing transactions, or other action deemed appropriate by the Information System Owner.

E. Audit Record Review, Analysis, and Reporting

1. TWU Information Systems Owners, or designees, shall periodically review and analyze Information System audit records for indications of inappropriate or unusual activity, and report findings to designated University officials.

2. When there is a change in risk to University operations, assets, individuals, or other organizations due to credible intelligence, the ISO will adjust the level of audit review, analysis, and reporting for an Information System.

3. Users shall utilize the incident reporting procedures as defined in URP 04.740: Information Security Incident Response for reporting inappropriate or unusual activity that has been discovered via the auditing process.

F. Time Stamps

1. TWU Information Systems must use standardized clocks to generate time stamps for audit records to facilitate logging and monitoring.

2. TWU Information Systems must be configured to a centralized Network Time Protocol (“NTP”) server that all servers and network devices are synced with as TWU’s authoritative time source. This centralized source can be mapped to Coordinated Universal Time (“UCT”). This aids in the monitoring of time stamps and logs.

G. Protection of Audit Information

1. TWU Information Systems must protect audit information and audit tools from unauthorized access, modification, and deletion.

2. All centralized audit logs are restricted to Users with administrative permissions as are the log collection servers that

report to it. Administrative permissions are controlled by TWU Information Security.

H. Audit Record Retention

1. TWU Information Systems shall retain audit records for one hundred and twenty (120) days to provide support for after-the-fact investigations of security incidents and to meet regulatory and University information retention requirements.

I. Audit Record Generation

1. ITS central audit systems shall provide audit record generation capability for the event types the system is capable of auditing.

2. TWU information audit systems must allow investigators to select which auditable Events are to be audited and the audit records must conform to the minimum standards defined in previous sections: Event Logging (AU-2) and Content of Audit Records (AU-3).

3. TWU ITS shall configure all Information Systems to generate audit records to all of the specifications set forth in previous procedures in this document.

II. Regulatory Compliance

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

1. AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-8, AU-9, AU-11, and AU-12.

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.

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 § 441.185

URP 01.320: University Policy Development and Implementation

URP 01.310: Records Retention

URP 04.795: Data Access and Use Policy

URP 04.740: Information Security Incident Response

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

URP 05.600: Staff Standards of Conduct and Disciplinary Process

FORMS AND TOOLS

None

Publication Date: 07/02/2021

Revised: 03/25/2022; 06/06/2024