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**

POLICY STATEMENT

This document establishes the information security audit and accountability regulations and procedures for managing risks from inadequate event logging and transaction monitoring. The information security audit and accountability program helps Texas Woman's University ("TWU") implement security best practices with regard to information security auditing and accountability.

APPLICABILITY

This policy is applicable to TWU Students, Employees, and Guests.

DEFINITIONS

1. "Audit 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. "Audit Events" means information or computer security-relevant information system actions 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. "Guests" means any individual not affiliated with TWU.

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, 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 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 Technology Infrastructure Director of Enterprise Services and Information Security.

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

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

9. "Time stamp" means the current time of an event that is recorded by a computer.

REGULATION AND PROCEDURE

I. Scope

The scope of these regulations and procedures are 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.

II. Regulation and Procedures

The State of Texas has chosen to adopt the Audit and Accountability principles established in NIST SP 800-53 "Audit and Accountability Control Family

guidelines". The following subsections outline the audit and accountability standards that constitute TWU's regulations and procedures.

A. AU-1 Audit and Accountability

1. Regulations

TWU must develop, adopt or adhere to a formal, documented audit and accountability for regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. Procedures

IT Solutions ("ITS") will maintain regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of TWU's information security audit and accountability program.

B. AU-2 Audit Events

1. Regulations

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

2. Procedures

TWU Information Resources will be reviewed during the risk assessment process to determine if Information Systems provide the necessary means whereby authorized personnel can audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information.

C. AU-3 Content of Audit Records

1. Regulations

a. TWU Information Systems must produce audit records 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 (success or failure) of the event, and the identity of any user associated with the event.

2. Procedures

a. IT Solutions employs centralized audit logging systems that contain the minimum required information for events and transactions.

b. Information System Audit requirements:

i. Information System owners have to be recorded by ITS Information Security.

ii. Information System data have to be classified by ITS Information Security as: 1) confidential (PIP); 2) agency sensitive (PI); and 3) public (PO).

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

a. Monitoring is optional for Dev/Test servers.

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

v. Production Information Systems must be physically located in one of TWU's controlled facilities.

vi. Information Systems that have update services are managed by ITS by default. Automatic updating can be configured on a case-by-case basis.

vii. When Information Systems allow, they must be joined to TWU's security group management system.

a. Exceptions can be made based on case-by-case basis by the ISO.

viii. When Information Systems allow, proper group policies must be applied.

ix. Information Systems must have endpoint security properly installed and configured.

x. Information Systems must have appropriate monitoring scripts installed, configured, and running to provide central notifications.

D. AU-4 Audit Storage Capacity

1. Regulations

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

2. Procedures

ITS maintains capacity for 90 days' worth of audit logs. Information System scripts will monitor available space and notify the appropriate individuals of high space utilization.

E. AU-5 Response to Audit Processing Failures

1. Regulations

a. TWU Information Systems must alert designated organizational officials in the event of an audit processing failure.

b. TWU Information Systems must be configured to take appropriate actions during an audit log failure.

2. Procedures

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

b. 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 system owner.

F. AU-6 Audit Review, Analysis, and Reporting

1. Regulations

a. TWU information asset records must be reviewed and analyzed periodically for indications of inappropriate or

unusual activity, and report findings to designated organizational officials.

b. TWU must adjust the level of audit review, analysis, and reporting within the information asset when there is a change in risk to organizational operations, organizational assets, individuals, or other organizations due to credible intelligence.

2. Procedures

a. On a monthly basis, the Information Security Manager will randomly select systems for review and analysis of inappropriate or unusual activity.

b. When necessary, the ISO will adjust the level of audit review, analysis, and reporting for an information asset.

c. ITS utilizes the following incident notification plan as the order for reporting inappropriate or unusual activity that has been discovered via the auditing process:

i. ITS Service Desk is notified.

ii. ITS Information Security is notified.

iii. ISO is notified.

iv. Vice President for Finance and Administration is notified.

G. AU-8 Time Stamps

1. Regulations

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

2. Procedures

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

H. AU-9 Protection of Audit Information

1. Regulations

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

2. Procedures

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 ITS Information Security.

I. AU-11 Audit Record Retention

1. Regulations

TWU Information Systems must retain audit records for a sufficient period of time to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

2. Procedures

All Information Systems must retain audit records for 90 days to provide support for after-the-fact investigations.

J. AU-12 Audit Generation

1. Regulations

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 AU-2 and AU-3.

2. Procedures

a. ITS central audit systems allow events to be reported and collected on the basis of event type.

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

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

Standards of Conduct Corrective Action Guidelines 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

URP 02.330: Faculty Standards of Conduct Corrective Action Guidelines

URP 05.600: Staff Standards of Conduct and Disciplinary Process

URP 06.200: Student Code of Conduct

FORMS AND TOOLS

None

Publication Date: 07/02/2021

Revised: 07/02/2021