UTHealth
The University of Texas
Health Science Center at Houston

17-202 Texas Administrative Code 202

We have completed our audit of compliance with Texas Administrative Code 202 requirements. This audit is required by Texas Administrative Code 202 and is part of our fiscal year (FY) 2017 audit plan. This audit was performed in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

The Texas Administrative Code is a compilation of all Texas state agency rules, with a total of 16 titles. Tile 1, Part 10, Chapter 202, Subchapter C (TAC 202) encompasses six sections and includes a Security Control Standards Catalog (Catalog), which was initiated by the Texas Department of Information Resources to assist state agencies and higher education institutions in implementing security controls. The Catalog contains a total of 282 control standards, 24 of which have a required implementation by February 2017.

OBJECTIVES

The objective of this audit was to determine compliance with selected requirements of TAC 202 Information Security Standards.

SCOPE PERIOD

The scope period was March 1, 2016 – February 28, 2017.

METHODOLOGY

The following procedures were performed:

- Verified actions are not performed by unauthenticated individuals and applications have defined authorizing officials. Obtained the FY2017 IT Risk Mitigation Plan and verified it is updated on a regular basis. Obtained the access control policy and determined a procedure for authorizing internal information resource connections exists. Reviewed system security and configuration documentation and confirmed Active Directory account lockout settings.
- Obtained and reviewed policies and procedures on peer-to-peer file sharing, data retention, and posting of information on publicly accessible information systems. Verified that maintenance records are current and updated according to vendor specifications and/or organizational requirements.
- Reviewed policies and procedures on acceptable usage and sanctions. Verified personnel acknowledge and agree to the acceptable usage policy.
- Verified incident policies and procedures exist, an incident response team is established, and personnel are trained on incident response and contingency responsibilities.

713.500.3160 phone 713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

AUDIT RESULTS

A&AS identified areas of improvement related to information security:

- One active employee maintains inappropriate access to the Archer risk assessment system.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None

We would like to thank the staff and management within the IT and IT Security departments who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

MAPPING TO FY 2017 RISK ASSESSMENT

Risk (Rating)	N/A

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned	Tammy Tran, CISA
End of Fieldwork Date	April 17, 2017
Issue Date	April 27, 2017

Copies to:
Audit Committee
Richard Miller
Kevin Granhold
Amar Yousif
Tammy Gardiner

Issue #1	Per the Security Control Standards Catalog, a supplement to Texas Administrative Code 202, control standard SA-5 requires the organization to effectively secure system security documentation and configuration settings. The Archer risk assessment system contains information on system security and configuration for systems across UTHealth, including Allscripts and GE Centricity Business Systems. A&AS reviewed the Archer access listing and noted 53 users, 1 (2%) of which is an active employee with inappropriate access. A&AS also noted four inactive UTHealth employees on the Archer access listing. General access to Archer is synced with active directory; as such, when an employee is terminated and network access is removed, access to Archer is automatically removed. For the four inactive UTHealth employees, A&AS verified both network and Archer access were properly removed. Additionally, A&AS noted one former UT System employee on the Archer access listing. UT System access to Archer is subject to UT System's internal controls and processes.
Recommendation #1	We recommend that Archer access be removed for the active employee with inappropriate access.
Rating	Medium
Management Response	We agree with the recommendation and have removed Archer access for the active employee with inappropriate access.
Responsible Party	Amar Yousif, Chief Information Security Officer
Implementation Date	Implemented as of April 27, 2017 (Verified by A&AS)