The University of Texas at Tyler

Administrative Privileges Audit

August 2018

THE UNIVERSITY OF TEXAS AT TYLER
OFFICE OF AUDIT AND CONSULTING SERVICES
3900 UNIVERSITY BOULEVARD
TYLER, TEXAS 75799

The University of Texas at Tyler
Administrative Privileges Audit
Fiscal Year 2018

BACKGROUND

Administrative privileges, also known as administrative rights, are often required to install or remove software programs, apply updates to software, and modify system settings on laptops and desktops. Extended use of these privileges could pose a risk to University data, the network, and other University systems, including desktops, laptops, and servers. The University of Texas at Tyler (UT Tyler) university-wide risk assessment identified administrative privileges as a critical risk; therefore, an audit of the process of granting and removing administrative privileges was included in the FY 2018 Annual Audit Plan and approved by the Institutional Audit Committee.

AUDIT OBJECTIVE

The objective of the audit was to determine if the UT Tyler Information Security Office is completing procedures to limit administrative privileges on campus desktop and laptop computers.

STANDARDS

The audit was conducted in accordance with guidelines set forth in *The Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing* and *Generally Accepted Government Auditing Standards*.

SCOPE AND METHODOLOGY

To accomplish the objective, the following procedures were completed.

- Gained an understanding of the current policies and procedures used by the Information Security Office to grant administrative privileges.
- Examined a sample of administrative privilege requests from employees and the responses from the Information Security Office.

RESULTS

According to The University of Texas System Audit Office, "*A Priority Finding is defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole. Non-Priority Findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable Qualitative, Operational Control, and Quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated.*

Finding Level Legend	
Priority	*A finding is defined as an issue that if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Tyler.*
High	*A finding that is considered to have a medium to high probability of adverse effects to UT Tyler as a whole or to a significant college or department.*
Medium	*A finding that is considered to have a low to medium probability of adverse effects to UT Tyler as a whole or to a college or department.*
Low	*A finding that is considered to have a minimal probability of adverse effects to UT Tyler as a whole or to a college or department.*

This audit resulted in **no** findings.

Employees who are assigned desktop computers must request administrative privileges from the Information Security Office and provide a business need for requesting the privileges. The Information Security Officer reviews the requests to determine if there is a valid reason to grant the privileges. Approved requests are emailed to the Campus Computing Services (CCS) so the privileges can be granted on the device. If the request is denied, the employee is referred to CCS for assistance in having the software or device installed. A sample of these requests and related responses was reviewed. The responses were appropriate based on the information the employee provided. Employees who are assigned laptop computers currently have administrative privileges.

A revised process is being developed to further control administrative privileges. The Information Security Office is collaborating with Information Technology Department to develop a link in conjunction with Service Now that will allow the user to request temporary administrative rights. UT Tyler will be utilizing "Make Me Admin", an application that allows standard user accounts to be elevated to administrator-level on a temporary basis (30 minutes at a time). The application will be installed on desktop and laptop computers and activated when administrative privileges are approved. When an employee needs administrative privileges on their desktop or laptop, after they have had their request for temporary administrative rights approved, they will be able to temporarily elevate their rights using "Make Me Admin". "Make Me Admin" will decrease the risk to UT Tyler's system and network by ensuring that user will not be operating desktops and laptops that are always using elevated privileges. The Information Security Office will also receive daily reports indicating what users have elevated their rights in the past 24 hours, and how many times their rights were elevated. This new process is planned to be completed in Fall 2019.

CONCLUSION

UT Tyler's Information Security Office has decreased the risks related to administrative privileges by limiting the number of employees' who have administrative privileges. The implementation of "Make Me Admin" will further decrease the risks. We commend the Information Security Office for their diligent work on mitigating this critical risk and appreciate their assistance during this project.