Personnel Security

Audit Report # 19-110
May 31, 2019

The University of Texas at El Paso

Office of Auditing and Consulting

"Committed to Service, Independence and Quality"

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

May 31, 2019

Dr. Diana Natalicio
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited scope audit of Personnel Security. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the departments in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by: the Information Security Office, Human Resources, Enterprise Computing, and Budget Departments during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Executive Vice President
Dr. Stephen Riter, Vice President for Resources and Planning
Ms. Sandy Vasquez, Associate Vice President, Human Resources
Mr. Gerard Cochrane, Chief Information Security Officer
Mr. Luis Hernandez, Assistant Vice President and Director, Enterprise Computing
Ms. Joanne Richardson, Assistant Vice President, Budget and Personnel
Ms. Mary Solis, Director and Chief Compliance and Ethics Officer

University of Texas System (UT System):
System Audit Office

External:
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office
Sunset Advisory Commission

Audit Committee Members:
Mr. Fernando Ortega
Dr. Gary Edens
Mr. Benjamin Gonzalez
Mr. Mark McGurk
Dr. Roberto Osegueda
Dr. John Wiebe

Auditors Assigned to the Audit:
Victoria Morrison

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of The University of Texas at El Paso (UTEP)'s compliance with security group "PS-Personnel Security" from the Texas Department of Information Resources, *Security Control Standards Catalog Version 1.3,* as required by Texas Administration Code Title 1, Part 10, Chapter 202, Subchapter C, RULE §202.76(c).

Personnel security includes ensuring (i) individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions and (ii) data and information systems are protected during and after personnel actions such as terminations and transfers; and employ formal sanctions for personnel failing to comply with security policies and procedures.

During the audit, we noted the following:

- PS-7 Third-Party Personnel Security: UTEP affiliates with possible access to confidential information resources do not have to sign the UTEP "*Acknowledgement of Policies*"; which requires personnel to acknowledge they will read the UTEP *"Information Resources Acceptable Use and Security Policy Agreement"*.

Control Number	Control Name	Results
PS-1	Personnel Security Policy and Procedures	No exceptions are noted
PS-2	Position Risk Designation	No exceptions are noted
PS-3	Personnel Screening	No exceptions are noted
PS-4	Personnel Termination	No exceptions are noted
PS-5	Personnel Transfer	No exceptions are noted
PS-6	Access Agreements	Audited in 2017. No exceptions were noted
PS-7	Third-Party Personnel Security	Exception noted, see above
PS-8	Personnel Sanctions	Audited in 2017. No exceptions were noted

BACKGROUND

Texas Administrative Code Title 1, Part 10, Chapter 202, (TAC 202) outlines mandatory information security controls to be implemented by all State agencies and institutions of higher education. The required TAC 202 information security controls are found in the Texas Department of Information Resources (DIR) *Security Control Standards Catalog Version 1.3*. Rule §202.76(c) further requires that a review for compliance with specified control standards "be performed at least biennially", based on business risk management decisions, by individual(s) independent of the information security program."

This audit is intended to meet the Rule §202.76(c) requirement for The University of Texas at El Paso (UTEP), as it relates to security group PS-Personnel Security, as well as verify compliance with University of Texas System Policy 165, (UTS 165) and UTEP Policies.

AUDIT OBJECTIVES

The objective of this audit was to determine UTEP's compliance with the DIR *Security Control Standards Catalog Version 1.3,* for the security control group PS-Personnel Security, as required by TAC 202 Rule §202.76(c).

SCOPE AND METHODOLOGY

The scope of the audit covers the period from January 1, 2018 to January 1, 2019, and is limited to the DIR security control group PS-Personnel Security. (Note: PS-6 Access Agreements and PS-8 Personnel Sanctions security controls were excluded as they were audited in 2017 with no exceptions noted).

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the authoritative guidelines of the *International Professional Practice Framework* issued by the Institute of Internal Auditors.

The criteria for the audit included:

- DIR *Security Control Standards Catalog Version 1.3*
- UT System Policy (UTS 165) Information Resources Use and Security Policy
- UTEP Information Resources Acceptable Use and Security Policy
- UTEP Handbook of Operating Procedures

Audit procedures included:

- interviewing and requesting information from key personnel
- reviewing applicable laws, regulations, policies and procedures
- verifying the existence of appropriate institutional policies and procedures
- running queries on PeopleSoft to extract data
- testing data using data analytics software
- limited testing, where appropriate

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority - 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.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

AUDIT RESULTS

A. Personnel Security Control Results

Control Number	Control Name	Results
PS-1	Personnel Security Policy and Procedures Existence of a written security policy	No exceptions are noted
PS-2	Position Risk Designation Acknowledgement of compliance with security policy	No exceptions are noted
PS-3	Personnel Screening Criminal background checks	No exceptions are noted
PS-4	Personnel Termination Access termination process	No exceptions are noted
PS-5	Personnel Transfer Access transfer process	No exceptions are noted
PS-6	Access Agreements Existence of access agreements	Audited in 2017. No exceptions were noted
PS-7	Third-Party Personnel Security Acknowledgement of compliance with security policy for non-university personnel	Exception noted, see B, below
PS-8	Personnel Sanctions Existence of written sanctions policies for non-compliance with security policy	Audited in 2017. No exceptions were noted

B. Affiliated personnel with possible access to confidential data are not required to sign an acknowledgement of UTEP Policies

Affiliated personnel are non-university personnel (e.g. guest faculty, contractors, or alumni) who a department has requested access as a sponsored account. Affiliated personnel are not required to sign the UTEP "*Acknowledgement of Policies*" as do all UTEP employees during the hiring process. This requires employees to acknowledge they will read the UTEP *"Information Resources Acceptable Use and Security Policy Agreement"* (AUP). The AUP contains details on what users need to comply with and explains expectations, confidentiality, and security of data. (See Appendix A: Criteria, *PS-7 Third-Party Personnel Security, AUP*).

When logging in to UTEP information resources, a general message is displayed stating the acceptance of UTEP policies. UTEP considers this an acknowledgement of UTEP policies for all users of UTEP's information resources. However, the AUP contains much more information that a new user needs to know. (See Appendix A: Criteria, *UTEP STANDARD 2: Acceptable Use of Information Resources*).

Recommendation:

Include a documented acknowledgment of UTEP policies in the processing of non-university personnel before granting access to UTEP's information resources.

Level: This finding is considered **MEDIUM** because non-university personnel should be held to the same standard as UTEP employees regarding access and security to UTEP's information resources.

Management Response:

The Information Security Office is exploring several options for delivering compliance training and recording the acceptance of the UTEP Acceptable Use Policy. These include leveraging Blackboard built-in features, or developing a customized application.

Responsible Party:

Gerard D. Cochrane Jr., Chief Information Security Officer

Implementation Date:

June 30, 2020

CONCLUSION

Based on the results of audit procedures performed, we believe that compliance with the DIR *Security Control Standards Catalog Version 1.3,* for the security control group PS-Personnel Security will be enhanced by implementing our recommendation.

We wish to thank the management and staff of the Information Security Office, Human Resources, Enterprise Computing, and Budget for their assistance and cooperation provided throughout the audit.

APPENDIX A: CRITERIA

Texas Department of Information Resource-*Security Control Standards Catalog Version 1.3*., *as required by* Texas Administration Code Title 1, Part 10, Chapter 202, Subchapter C RULE §202.76 Security Control Standards Catalog,

PS-7 Third-Party Personnel Security

"REQUIRED BY: Feb-16
CONTROL DESCRIPTION
The organization:

a. *Establishes personnel security requirements including security roles and responsibilities for third-party providers;*
b. ***Requires third-party providers to comply with personnel security policies and procedures established by the organization;***
c. *Documents personnel security requirements;*
d. *Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and*
e. *Monitors provider compliance.*

IMPLEMENTATION STATE
The state organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance."

UTEP STANDARD 2: Acceptable Use of Information Resources

OGC REVISED FINAL June 18, 2014

The University of Texas at El Paso

INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY AGREEMENT

All individuals granted access to or use of System Information Resources must be aware of and agree to abide by the following acceptable use requirements:

Definitions

- **University:** The University of Texas at El Paso (referred to as"UTEP" or "the University")
- **System**: The University of Texas System.
- **University Information Resources**: All computer and telecommunications equipment, software, data, and media, ownedor controlled by University or maintained on itsbehalf.
- **University Data:** All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paperrecords.
- **Confidential Data or Confidential Information:** All University Data that is required to be maintained as private or confidential by applicable law.
- **User:** Any individual granted access to University Information Resources.

General

- University Information Resources are provided for the purpose of conducting the business of University and/or System. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties to University or System (Incidental Use) as permitted by thispolicy.
- Users have no expectation of privacy regarding any University Data residing on University owned computers, servers, or otherinformation resources owned by, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission withoutnotice.
- Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personaldevice.
- All Users must comply with applicable University and System Information Resources Use and Security policies at alltimes.
- Users shall never use University Information Resources to deprive access to individuals otherwise entitled to access University Information, to circumvent University computer security measures; or, in any way that is contrary to the University's mission(s) or applicable law.
- Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of University and is approved in writing by the President or a specific designee. Viewing, access to, or storage or transmission of sexually explicit materials as Incidental Use is prohibited.
- Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of the University and do not express the opinion or position of

	University. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas at El Paso." ● Users should report misuse of University Information Resources or violations of this policy to their supervisors.
Confidentiality & Security of Data	● Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with University's Records Retention Policy and Records Management Guidelines. ● Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official University duties. ● Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on a centrally managed server, rather than a local hard drive or portable device. ● In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, the User must ensure the data is encrypted in accordance with University, System's and any other applicable requirements. ● The following University Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft. Email sent to and received from System and U. T. System institutions using University and/or System provided email accounts is automatically encrypted. The Office of Information Technology [or other applicable office] will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations. ● Users who store University Data using commercial cloud services must use services provided or sanctioned by University, rather than personally obtained cloud services. ● Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of University. ● All computers connecting to a University's network must run security software prescribed by the Information Security Officer as necessary to properly secure University Resources. ● Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.

Email	• Emails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements. • Users are to use University provided email accounts, rather than personal email accounts, for conducting University business. • The following email activities are prohibited when using a University provided email account: ○ Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work related purpose. ○ Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of University. ○ Sending or forwarding any email that is suspected by the User to contain computer viruses. ○ Any Incidental Use prohibited by this policy. ○ Any use prohibited by applicable University or System policy.
Incidental Use of Information Resources	• Incidental Use of University Information Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy. • Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University email accounts. • A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located. • Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited. • Incidental Use for purposes of political lobbying or campaigning is prohibited. • Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User's allocated mailbox space). • Files not related to System business may not be stored on network file servers.

Additional Requirements for Portable and Remote Computing	• All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised. • University Data created or stored on a User's personal computers, smart phones or other devices, or in data bases that are not part of University's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources • University issued mobile computing devices must be encrypted. • Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted. • University Data created and/or stored on personal computers, other devices and/or non-University data bases should be transferred to University Information Resources as soon as feasible. • Unattended portable computers, smart phones and other computing devices must be physically secured. • All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.
Password Management	• University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone. • Each User is responsible for all activities conducted using the User's password or other credentials.

User Acknowledgment

I acknowledge that I have received and read the Information Resources Acceptable Use Policy. I understand and agree that my use of University Information Resources is conditioned upon my agreement to comply with the Policy and that my failure to comply with this Policy may result in disciplinary action up to and including termination of my employment.

Signature: ______________________________ Date______________

Print Name: ______________________________