Texas Administrative Code 202
(Phase 2)

Audit Report # 14-08
September 16, 2015

Office of Auditing and Consulting Services

"Committed to Service, Independence and Quality"
September 16, 2015

Dr. Diana Natalicio
President, 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 the Texas Administrative Code 202, Subchapter C-Information Security Standards for Institutions of Higher Education. The main audit objective was to determine whether an information security policy exists and is enforced, and information resource roles and responsibilities are defined and adhered to.

We appreciate the cooperation and assistance provided by the management and staff of the Information Security Office, Information Resources and Planning Enterprise Computing, Human Resources and Technology Support.

Sincerely,

Lori N. Wertz, CPA
Chief Audit Executive
Report Distribution:

University of Texas at El Paso
   Mr. Richard Adauto III, Executive Vice President
   Dr. Stephen Riter, Vice President for Information Resources and Planning
   Mr. Gerard Cochrane, Jr, Chief Information Security Officer
   Mr. Luis Hernandez, Director Enterprise Computing
   Ms. Sandy Vasquez, Assistant Vice President for Compliance Services

University of Texas System
   Dr. Steven Leslie, Executive Vice Chancellor for Academic Affairs
   Mr. Alan Marks, Attorney, Office of Academic Affairs
   Mr. J. Michael Peppers, Chief Audit Executive
   Mr. Mark Salamasick, Executive Director – Audit Academic

External
   Governor’s Office of Budget
   Mr. Ed Osner, Legislative Budget Board
   Internal Audit Coordinator, State Auditor’s Office
   Sunset Advisory Commission

External Audit Committee Members
   Mr. David Lindau
   Mr. Steele Jones

Auditors Assigned to the Audit:
   Victoria Morrison (IT Auditor)
   Lorenzo Canales (Senior Internal Auditor)
   Narahay Buendia (Internal Auditor)
## Table of Contents

EXECUTIVE SUMMARY ................................................................. 1  
BACKGROUND .............................................................................. 2  
AUDIT OBJECTIVES........................................................................ 2  
SCOPE AND METHODOLOGY .......................................................... 3  
AUDIT RESULTS ............................................................................ 4  
   1. Account Management-Terminated Employee Access .................. 4  
   3. Encryption Policy .................................................................... 7  
   4. Account Management Policy .................................................. 9  
   5. User Security Practices- Security Awareness ............................ 10  
   7. Account Management – Process Map ...................................... 12  
CONCLUSION .................................................................................... 14  
APPENDIX A: TAC Moved Towards FISMA ................................. 15  
APPENDIX B: Cross Reference TAC 202 from Legacy to Current .... 16  
APPENDIX C: Terminated Employees Report ................................. 17  
APPENDIX D: Process: Grant Access New Employee ....................... 18  
APPENDIX E: Process: Grant/Remove Access Transfer Employee .... 20  
APPENDIX F: Process: Remove Access Terminated Employee ........ 22  
APPENDIX G: Glossary ................................................................. 24
EXECUTIVE SUMMARY

The Office of Auditing and Consulting (OACS) has completed a limited-scope audit of the Information Security Office to determine compliance with established guidelines and requirements specified in Texas Administrative Code Chapter 202 (TAC 202) Subchapter C: Security Standards for Institutions of Higher Education. Based on the results of audit procedures performed, the University is in general compliance with the TAC 202 Subchapter C, except as noted in this report.

During our audit we noted the following:

- scheduled monitoring of user accounts for terminated employees in the following systems: Banner (Student Information System), PeopleSoft Human Capital Management Suite, and Active Directory (Windows Operating System Security) was not performed effectively.

- there is not a complete inventory listing of computers on campus; therefore, it cannot assure that all “Public Access Devices” comply with the security program. Public Devices are computers which can be accessed by the public and do not require a UTEP account to login.

- The University “Information Security Policies”, found on Information Security Office (ISO) website, has not been updated since 2002. Therefore policies and/or procedures do not contain current guidelines or requirements.

- documentation for account set up procedures for new, transferred and terminated employees needs to be updated. OACS has documented the Process Flows and has provided the Process Maps Narrative (See APPENDIX D-F).

- The University has an updated “Security Awareness Program” for new employees and training is enforced yearly.

- The University is in compliance with non-disclosure agreements, which protect information from disclosure by employees, and ensures requirements are in place and well documented.

- The University Information Security Officer (ISO) is well informed of the processes for new, transferred and terminated employee access.
BACKGROUND

A limited review of compliance with the Texas Administrative Code 202 (TAC 202) was performed on the Information Security Office (ISO) to evaluate the information security program compliance with established guidelines and requirements as specified in Subchapter C: Security Standards for Institutions of Higher Education.

This report outlines the audit results for: Information Security Safeguards / User Security Practices.

Effective March 2015, TAC 202 was revised and moved towards Federal Information Security Management Act (FISMA) rules (See APPENDIX A). Therefore, the audited areas now fall under “Institution Information Security Program” (202.74) and/or “Security Control Standards Catalog” (202.76), (See APPENDIX B) which contain cross references between the old and new requirements for TAC 202.

AUDIT OBJECTIVES

The objective of this audit was to evaluate the information security program and determine compliance with established guidelines and requirements as specified in TAC 202 Subchapter C Security Standards for Institutions of Higher Education. The focal points were to review:

- encryption policy and encryption key standards,
- security awareness training for employees,
- user security practices, policies, non-disclosure agreements and public access devices,
- account management policy and procedures for new, transferred and terminated employees, and
- terminated employees’ access to information resources.
SCOPE AND METHODOLOGY

The audit scope was limited to information security policies and procedures in effect as of December 1, 2014. This audit is a subset of TAC 202.75 and 202.77.

Audit procedures included:

- interviewing 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,
- requesting data from account administrators (custodians),
- developing process flows as needed, and
- performing data analysis using IDEA Software.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors.
AUDIT RESULTS

The Office of Auditing and Consulting Services (OACS) tested seven procedures pertaining to TAC 202 rules and identified four findings. No exceptions were noted for the remaining three procedures.

1. Account Management-Terminated Employee Access

Requirements & Controls

TAC 202: A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities change.

UTSJ 65: Owners and Custodians must monitor access to records containing Confidential Data by the use of appropriate measures as determined by applicable policies, standards, procedures, and regulatory requirements. ...

Owners and Custodians must establish log capture and review processes based on risk and applicable policies, standards, procedures, and regulatory requirements.

UTEP Information Security Policies:

... System Administrators or other designated staff:
  Are responsible for removing the accounts of individuals that change roles within UTEP or are separated from their relationship with UTEP

... Must have a documented process for periodically reviewing existing accounts for validity
  Are subject to independent audit review
  Must provide a list of accounts for the systems they administer when requested by authorized UTEP management ...

Observations

- Periodic or scheduled review and monitoring of user accounts is not being performed by Enterprise Computing or the Information Security Office (ISO).

- There were terminated employees who still had access to information; however, none were found to have special privileges. See APPENDIX C: Terminated Employees Report for a review of terminated employees in Banner, Active Directory (Windows Operating System Security), and PeopleSoft.

- Policies for terminated employees with active accounts to UTEP resources are not clearly documented or are lacking for Banner, Active Directory, and PeopleSoft. There were verbal standards for exceptions and retention periods for students, faculty and staff within Enterprise Computing and ISO; however, they were not documented in the policies.
Recommendation:

- A scheduled periodic review and monitoring of user accounts should be performed by Account Administrators (Custodians) - Enterprise Computing as stated in the UTSI 65 and UTEP policies. The ISO should review monitoring performed by custodians or conduct his own monitoring.

- Policies and procedures should be updated to include exceptions for keeping an account active of a terminated employee (students, faculty and staff) in any Business Application or in Active Directory. In addition, the retention period to keep an account active in a Business Application or in Active Directory (Security system) should be clearly documented and communicated for terminated employees.

Management Response Enterprise Computing:

The account management process is automated for Active Directory (AD) and PeopleSoft (PS). UTEP receives a daily file feed from PS with employee data such as name, EMPLID, title and assignment. When an employee’s job assignment/appointment ends in PS, that information triggers action at the campus to begin disabling/deleting accounts and services. The employee’s account is then “marked” to be disabled 60 days from the last date of employment.

Within PS, when an employee’s job assignment/appointment ends, the system automatically assigns the “terminated” role. That role triggers a process that then removes all roles, except the employee self-service roles, in a batch process that runs overnight.

Banner access is managed internally to the application, so disabling the AD account will not remove access to Banner. To bridge that gap, the Banner security team receives a daily report on separation events so they can manually intervene. If an employee’s department changes, the team will lock the account. If the employee is “terminated” then the account is disabled. Periodic reviews are done by departments, specifically Financial Aid, Registrar and Student Business Services do periodic reviews of the access that users have to specific forms they own within Banner.

Will work with the Information Security Office to document and publish the Identity Management process to include timelines for the disabling/deleting of accounts for employees and students. Will have the document ready for review by the Vice President for Information Resources and Planning by 12/31/2015.

Will work with the Information Security Office to develop an account review process where account access is reviewed by divisions/departments/offices on a regular basis. Will have a plan developed and documented by 12/31/2015 so that the first review can happen during Q2 of 2016.

Responsible Party- Enterprise Computing:
Luis Hernandez, Director, Enterprise Computing
Implementation Date-Enterprise Computing:
February 29, 2016

Management Response ISO:
ISO will document and create a process that system administrators or Custodians of business systems and infrastructure systems can follow for monitoring accounts of terminated employees. The ISO will review on a yearly basis for compliance.

ISO will work with system administrators to clarify any exceptions or retention of accounts of terminated employees on a system-by-system basis.

Responsible Party - ISO:
Gerard Cochrane Jr., CISO

Implementation Date-ISO:
March 30, 2016


Requirements & Controls
TAC 202: devices designated for public access shall be configured to enforce security policies and procedures without the requirement for formal acknowledgement.

Observations:
- There is an incomplete inventory list of known Public Access Devices throughout the institution; therefore, not all Public Access Devices are in compliance with the University Security Policy.
- We found no policies or standards specific for Public Access Devices in the Information Security Office and UTEP Handbook of Operating Procedures.

Recommendations:
When public access to organizational information systems is allowed, security controls should be applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable for public access. Therefore, the device itself should be protected with software and boundary protection. This would include the following actions:
- Create policies or standards for Public Access Devices
• Complete an inventory of UTEP devices to identify all Public Access Devices and verify public access protection.

• Verify and certify that purchased devices for Public Use go through Technology Support in order to be in compliance with the University's security policy, and when possible, implement solutions to assist the department to be compliant with UTEP standards.

Management Response:

The ISO is currently in the process of updating the information security documentation to align with the 2015 TAC 202 and UTS 165 changes and will address Public Access Devices at that time.

The ISO will work with Inventory, Technology Support, Enterprise Computing, TIMs (Technology Information Managers) and department heads to verify that their inventory is complete and that all devices have Absolute Manage Software installed.

Responsible Party:

Gerard Cochrane Jr., CISO

Implementation Date:

August 31, 2016

3. Encryption Policy

Requirements & Controls

TAC 202: Security Policies, Encryption--Establishes encryption controls for institution of higher education-specified data classifications (e.g., confidential information), portable devices, removable media, transmission security, and encryption key standards and management.

Types of information that may be transmitted via wireless networks and devices with or without encryption. Institutions of higher education shall not allow access to confidential information, mission critical information or restricted personal information unless the cryptographic keys used are larger than 80-bits (See §3.3 Security of 802.11 Wireless LANs in the Wireless Security Guidelines).

UTS165: Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management shall be based on documented institution of higher education risk management decisions.

Observations:

The Encryption Policy found within the University Information Security Policies in the ISO policies website has not been updated since 2002 and may cause non-compliance with any
new federal, state and university requirements, including revisions to the requirements since the last policy update.

**Recommendation:**
The Information Security Officer should ensure that the University is in compliance with current encryption policies and requirements as promulgated by UT System Board of Regents and aligns with TAC 202 for an appropriate cryptographic key length.

**Management Response:**
ISO is currently in the process of updating the information security documentation to align with the 2015 TAC 202 and UTS 165 changes and will address encryption keys at that time.

**Responsible Party:**
Gerard Cochrane Jr., CISO

**Implementation Date:**
March 30, 2016
4. Account Management Policy

Requirements & Controls

TAC 202: Account Management—Establishes the rules for administration of user accounts.

UTS 165: Account Management. The U. T. System recognizes that proper management and use of computer accounts are basic requirements for protecting U. T. System Information Resources. All Entities shall adopt access management processes to ensure that access is administered properly. All offices that create access accounts for network and/or applications are required to manage the accounts in accordance with such access management processes and the requirements of the U. T. System Identity Management Federation Member Operating Practices (MOP). Access to a system may not be granted by another User without the permission of the Owner or the Owner’s delegate of that system.

UTEP Information Security Policies:
All accounts created must have an associated request and approval that is appropriate for the UTEP system or service. ...

... Accounts of individuals on extended leave (more than 30 days) will be disabled. All new user accounts that have not been accessed within 30 days of creation will be disabled.

Data Owners, System Owners, System Administrators and/or other authorized personnel:

• are responsible for removing the accounts of individuals that change roles within the University or are separated from their relationship with UTEP
• must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
• must have a documented process for periodically reviewing existing accounts for validity
• are subject to independent audit review
• must provide a list of accounts for the systems they administer when requested by the Information Security Office ...

Observations:
The Account Management Policy found within the University Information Security Policies posted on the ISO website has not been updated since 2002, and may cause non-compliance with any new federal, state and university requirements including revisions to the requirements since the last policy update.

Recommendation:
The Information Security Officer should update the IT Security Policy to ensure that the University is in compliance with current TAC 202 and UTS 165 Account Management policies and procedures and best practices.
Management Response:

ISO is currently in the process of updating the information security documentation to align with the 2015 TAC 202 and UTS 165 changes, and will address any changes to account management.

Responsible Party:

Gerard Cochrane Jr., CISO

Implementation Date:

March 30, 2016

5. User Security Practices- Security Awareness

Requirements & Controls:

TAC 202: State institutions of higher education are responsible for...
(2) Administering an ongoing information security awareness education program for all users; and
(3) Introducing information security awareness and informing new employees of information security policies and procedures during the onboarding process.

UTS 165:
Section 26 Security Training,

UTEP Information Security Policies: Security Training

Observations:

• An information security module is included in the annual compliance training that all UTEP employees need to complete, and is also covered at new employee orientations.

• The training modules are updated as needed. Additional training for specific topics, such as HIPAA, are available upon request by the departments.

• An annual email is sent as a reminder of the compliance training that needs to be completed by all employees.

• Consequences for non-compliant individuals can be found in UTEP's security policies, which were last revised on September 17, 2002. This policy is located on UTEP's Information Security website.

Recommendations:

No Exceptions were noted.

**Requirements & Controls**

*TAC 202*: Each institution of higher education head or his/her designated representative and information security officer shall establish a strategy for the use of written non-disclosure agreements to protect information from disclosure by employees and contractors prior to granting access.

*UTS165: Section 30 Vendor Access.*

... 30.1 Contracts. Vendor contracts must require that Vendors comply with all applicable U. T. System rules associated with this policy, practice standards, and agreements, and address all federal and State laws to which U. T. System must adhere to ensure that U. T. System remains in compliance with such law.

... Such measures must incorporate the following:

(a) Vendor shall represent, warrant, and certify it will:

i. hold all Sensitive Data in the strictest confidence;

ii. not release any Sensitive Data concerning an Entity student unless Vendor obtains Entity’s prior written approval and performs such a release in full compliance with all applicable privacy laws, including the Family Educational Rights and Privacy Act (FERPA);

iii. not otherwise use or disclose Sensitive Data except as required or permitted by law;

... A. written notice within one business day after Vendor’s discovery of such use or disclosure; and B. all information U. T. System requests concerning such unauthorized use or disclosure. ...

**UTEP Information Security Policies: Vendor Access > Policy**

- Vendors must comply with all applicable UTEP policies, practice standards and agreements, including, but not limited to:
  - Acceptable Use Policies
  - Auditing Policies
  - Privacy Policies
  - Non-Disclosure Agreement
  - Safety Policies
  - Security Policies
  - Software Licensing Policies
  - Non-Disclosure Agreement

**UTEP Handbook of Operating Procedures:**

A non-disclosure agreement (NDA) is in place on campus to protect information from employee and contractor disclosure. Data Privacy rules. Users of category 1 data and third party vendors are required for NDA ...
Observations

- Privacy and non-disclosure requirements are in place and well documented.
- The appropriate initial awareness and ongoing training with the required signature/acknowledgement procedures are in place.

Recommendations:

No Exceptions were noted.

7. Account Management – Process Map

Requirements & Controls

TAC 202: A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities change.

UTSJ 65: Owners and Custodians must establish log capture and review processes based on risk and applicable policies, standards, procedures, and regulatory requirements.

UTEP Information Security Policies: Account Management > Policy

All accounts created must have an associated request and approval that is appropriate for the UTEP system or service. ... Accounts of individuals on extended leave (more than 30 days) will be disabled. All new user accounts that have not been accessed within 30 days of creation will be disabled. Data Owners, System Owners, System Administrators and/or other authorized personnel:

- are responsible for removing the accounts of individuals that change roles within the University or are separated from their relationship with UTEP
- must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
- must have a documented process for periodically reviewing existing accounts for validity
- are subject to independent audit review
- must provide a list of accounts for the systems they administer
Observations

• The HR process for new hire, transferred and terminated employees is very well documented.

• IT has developed a semi-automated process for new hire, transferred and terminated employees.

• OACS documented the processes, by creating Process Maps for New Hire, Transfer and Terminated Employees. We have included the documented Process Flows in APPENDIX D – F.

• We found the ISO to be informed of the processes for new, transferred and terminated employee access.

Recommendations:

No Exceptions were noted.
CONCLUSION

Based on the results of audit procedures performed for the security modules covered in Phase 2, we believe that the University needs some improvement in order to be 100% compliant with Sections 202.75 and 202.77 of TAC 202; however, we believe that the University will be in compliance by implementing our recommendations.

We thank the Information Security Office, Information Resources and Planning Enterprise Computing, Human Resources and Technology Support for their assistance and cooperation during the audit.
APPENDIX A: TAC Moved Towards FISMA

Moving TAC toward FISMA

Legacy TAC 202
- Applicable Terms and Technologies for Information Security
- Institution of Higher Education
- State Agency
- Management and Staff Responsibilities
- Security Incidents
- Security Standards Policy
- Managing Security Risks
- Managing Physical Security
- Business Continuity Planning
- Information Resources Security Safeguards
- User Security Practices
- Removal of Data from Data Processing Equipment

Revised TAC 202
- Definitions
- Institution of Higher Education
- State Agency
- Responsibilities of the State CISO
- Responsibilities of the Agency Head
- Responsibilities of the Agency ISO
- Staff Responsibilities
- Security Reporting
- Agency Security Policy
- Control Catalog

FISMA
- Information Security
- Purposes
- Definitions
- Authority and functions of the Director
- Federal agency responsibilities
- Federal information security incident center
- National security systems
- Authorization of appropriations
- Effect on existing law

NIST SP 800-53
## APPENDIX B: Cross Reference TAC 202 from Legacy to Current

<table>
<thead>
<tr>
<th>Current TAC 202 (March 2015)</th>
<th>Previous Legacy TAC 202</th>
</tr>
</thead>
<tbody>
<tr>
<td>202.70 Responsibilities of the Institution Head</td>
<td>202.71 Management and Staff Responsibilities</td>
</tr>
<tr>
<td>202.71 Responsibilities of Information Security Officer</td>
<td>202.76 Security Incidents</td>
</tr>
<tr>
<td>202.72 Staff Responsibilities</td>
<td>202.70 Security Standards Policy</td>
</tr>
<tr>
<td>202.73 Security Reporting</td>
<td>202.72 Managing Security Risks</td>
</tr>
<tr>
<td>202.74 Institution Information Security Program</td>
<td>202.73 Managing Physical Security</td>
</tr>
<tr>
<td>202.76 Security Control Standards Catalog</td>
<td>202.75 Information Resources Security Safeguards</td>
</tr>
<tr>
<td>202.76</td>
<td>202.78 Removal of Data from Data Processing Equipment</td>
</tr>
</tbody>
</table>
APPENDIX C: Terminated Employees Report

The total number of terminated employees who were found to still be in the ACTIVE report for the systems: Banner, PeopleSoft and MS Windows Active Directory (Security Program). See APPENDIX G: Glossary for explanations of the terms covered in the Report.

Banner: 0

<table>
<thead>
<tr>
<th>TOTAL in Banner</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Active Employee - Rehired</td>
<td>2</td>
</tr>
<tr>
<td>Account Locked</td>
<td>1</td>
</tr>
</tbody>
</table>

PeopleSoft: 1

<table>
<thead>
<tr>
<th>TOTAL in PeopleSoft with Self-service Role</th>
<th>385</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retired Status</td>
<td>28</td>
</tr>
<tr>
<td>Current Active Employee - Rehired</td>
<td>7</td>
</tr>
<tr>
<td>&quot;Termination Role&quot; in employee’s security profile</td>
<td>349</td>
</tr>
<tr>
<td>Inactive with roles</td>
<td>1</td>
</tr>
</tbody>
</table>

Active Directory: 11

<table>
<thead>
<tr>
<th>TOTAL in Active Directory</th>
<th>377</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Student – (keep for one year)</td>
<td>300</td>
</tr>
<tr>
<td>NewEmailType='D' (set to be disabled 45 days after appointment ends)</td>
<td>62</td>
</tr>
<tr>
<td>Disabled during the testing period</td>
<td>13</td>
</tr>
<tr>
<td>Error-the record is stuck in HRReview and was dealt with manually</td>
<td>2</td>
</tr>
<tr>
<td>Still active after 45 days</td>
<td>9</td>
</tr>
</tbody>
</table>
# APPENDIX D: Process: Grant Access New Employee

## Scope of operation

<table>
<thead>
<tr>
<th><strong>New Employee/Affiliate</strong> Access Management</th>
</tr>
</thead>
</table>

## Description of operation

<table>
<thead>
<tr>
<th>Flow Chart Reference Page-1</th>
<th>Contents</th>
<th>Control No. Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Identify potential employee.</td>
<td></td>
</tr>
<tr>
<td>D.1</td>
<td>The hiring department contacts HRTC to identify required forms.</td>
<td></td>
</tr>
<tr>
<td>HR.1</td>
<td>Inform hiring department about any forms that need to be completed and actions that need to be taken.</td>
<td></td>
</tr>
<tr>
<td>D.2</td>
<td>Forms are accessed on UTEP’s website. Department fills out and signs off on HR forms.</td>
<td></td>
</tr>
<tr>
<td>D.3</td>
<td>Department filled and signed HR forms.</td>
<td></td>
</tr>
<tr>
<td>AE.1</td>
<td>Employee/Affiliate completes HR Forms</td>
<td></td>
</tr>
<tr>
<td>HR.2</td>
<td>Review forms for completeness. If there is any missing information or signatures from the department, forms will be sent back.</td>
<td></td>
</tr>
<tr>
<td>HR.3</td>
<td>Employee biographical and job record is created in Human Capital Management (HCM) system. HCM is a suite of PeopleSoft (PS) modules used to manage employee and human resource functions.</td>
<td>X</td>
</tr>
<tr>
<td>HR.4</td>
<td>For new affiliates, HR will email Enterprise Computing with the new affiliate information.</td>
<td></td>
</tr>
<tr>
<td>HR.5</td>
<td>Completed and reviewed HR Forms.</td>
<td></td>
</tr>
<tr>
<td>HR.6</td>
<td>Paper forms are scanned and saved in document manager. Paper forms are shredded.</td>
<td>X</td>
</tr>
<tr>
<td>EC.1</td>
<td>Enterprise Computing (EC) runs an interface nightly and every hour a web service to extract employee records from PS-HCM into the Person’s Database in the Identity Management System (IMS).</td>
<td></td>
</tr>
<tr>
<td>EC.2</td>
<td>EC Identity Management System (IMS) sends a daily report to the EC ISA(S), identifying any changes between the Person Database and the extracted PS data.</td>
<td></td>
</tr>
<tr>
<td>EC.3</td>
<td><strong>In Banner</strong> a search is conducted by EC to determine if an 80# or 88# already exist for the employee. Banner is an administrative software application developed specifically for higher education institutions that maintains student, alumni, financial and personnel data.</td>
<td></td>
</tr>
<tr>
<td>EC.4</td>
<td><strong>Decision Point: In Banner</strong>, does the new employee already has an 80# or 88# assigned?</td>
<td></td>
</tr>
<tr>
<td>EC.5</td>
<td>If no #80 or #88 ID exist for the new employee in Banner, an 80# is created.</td>
<td></td>
</tr>
<tr>
<td>EC.6</td>
<td><strong>Decision Point: In Active Directory</strong>, does the new employee with an 80# or 88# have an existing user name?</td>
<td></td>
</tr>
<tr>
<td>EC.7</td>
<td>If no user name has been assigned to the new employee, a user name is created in <strong>Persons Database</strong> (Identify Management System) and <strong>Active Directory</strong>.</td>
<td></td>
</tr>
<tr>
<td>EC.8</td>
<td>EC matches PeopleSoft Employee Number with existing user name in Persons Database.</td>
<td></td>
</tr>
<tr>
<td>EC.9</td>
<td>EC Provide new employee/affiliate credentials.</td>
<td></td>
</tr>
</tbody>
</table>

**Page-2**

| D.4 | New employee fills out “Access request form” selecting the roles needed for his position/department. BP logix form is then routed to department supervisor for approval. |
| D.5 | Access request form filled by new employee and approved by supervisor. |
| EC.10 | Institutional Security Administrator (ISA) reviews access request form and verifies there is no conflict between the roles requested. If there is a conflict access will be denied and form will route back to the department. |
| D.6 | Denied access request form is sent back to department requesting review and justification. |
| EC.11 | If no conflict exist between roles requested, ISA will grant the access to new roles in PeopleSoft. |
| EC.12 | Access request form with all necessary approvals to grant access. |
| End | New employee has access to the roles requested in PeopleSoft. |

**SYS.1** PeopleSoft Database
**SYS.2** Identity Management System-People Database
**SYS.3** Banner System
**SYS.4** Active Directory Database and Directory Services
**SYS.5** Document Manager
APPENDIX E: Process: Grant/Remove Access Transfer Employee

Scope of operation

| Transfer | Employee Access Management |

Description of operation

<table>
<thead>
<tr>
<th>Flow Chart Reference</th>
<th>Contents</th>
<th>Control No. Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Identify employee changing position or department.</td>
<td></td>
</tr>
<tr>
<td>HR.1</td>
<td>An employee’s job record is updated for an employee changing position or department in Human Capital Management (HCM) system. HCM is a suite of PeopleSoft (PS) modules used to manage employee and human resource functions.</td>
<td>X</td>
</tr>
<tr>
<td>EC.1</td>
<td>Enterprise Computing (EC) runs an interface nightly and every hour a web service to extract employee records from PS-HCM into the Person's Database in the Identity Management System (IMS).</td>
<td></td>
</tr>
<tr>
<td>EC.2</td>
<td>EC Identity Management System (IMS) sends a daily report to the EC ISA(S), identifying any changes between the Person Database and the extracted PS data.</td>
<td></td>
</tr>
<tr>
<td>EC.3</td>
<td>EC ISA(S), reviews the report for any changes made to employees’ records and removes roles in PeopleSoft.</td>
<td></td>
</tr>
<tr>
<td>EC.4</td>
<td>From the Data Warehouse, EC gets a report of employees that have a change in their job record and have a Banner account.</td>
<td></td>
</tr>
<tr>
<td>EC.5</td>
<td>Banner account gets locked</td>
<td></td>
</tr>
<tr>
<td>D.1</td>
<td>The transferee employee fills out “Access request form” selecting the roles needed for his position/department. BP logix form is then routed to department supervisor for approval.</td>
<td></td>
</tr>
<tr>
<td>D.2</td>
<td>Access request form filled by employee and approved by supervisor</td>
<td></td>
</tr>
<tr>
<td>EC.6</td>
<td>Institutional Security Administrator reviews access request form and verifies there is no conflict between the roles requested. If there is a conflict access will be denied and form will route back to the department.</td>
<td></td>
</tr>
<tr>
<td>D.3</td>
<td>Denied access request form is sent back to department requesting review and justification.</td>
<td></td>
</tr>
<tr>
<td>EC.7</td>
<td>If no conflict exist between accesses roles requested, ISA grants the access for requested roles in PeopleSoft.</td>
<td></td>
</tr>
<tr>
<td>EC.8</td>
<td>Access request form with necessary approvals to grant access. Access form is stored in Document Manager.</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>End</td>
<td>Transfer employee has the requested access for new position.</td>
<td></td>
</tr>
<tr>
<td>SYS.1</td>
<td>PeopleSoft Database</td>
<td></td>
</tr>
<tr>
<td>SYS.2</td>
<td>Identity Management</td>
<td></td>
</tr>
<tr>
<td>SYS.3</td>
<td>Banner System</td>
<td></td>
</tr>
<tr>
<td>SYS.4</td>
<td>Document Manager</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX F: Process: Remove Access Terminated Employee

Scope of operation

**Terminated Employee Access Management**

Description of operation

<table>
<thead>
<tr>
<th>Flow Chart Reference</th>
<th>Contents</th>
<th>Control No. Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Identify terminated employee</td>
<td></td>
</tr>
<tr>
<td>HR.1</td>
<td>Terminated employee job record is updated by changing the Action code, Reason code and Effective date, the system then updates the HR Status and Payroll Status in Human Capital Management (HCM) system. HCM is a suite of PeopleSoft (PS) modules used to manage employee and human resource functions.</td>
<td></td>
</tr>
<tr>
<td>EC.1</td>
<td>Enterprise Computing (EC) runs an interface nightly and every hour a web service to extract employee records from PS-HCM into the Person's Database in the Identity Management System (IMS).</td>
<td></td>
</tr>
<tr>
<td>EC.2</td>
<td>EC Identity Management System (IMS) sends a daily report to the EC ISA(S), identifying any changes between the Person Database and the extracted PS data.</td>
<td></td>
</tr>
<tr>
<td>EC.3</td>
<td>EC Identity Management System (IMS) identifies all terminated employees and flags them as 'ready for termination' in the Person’s Database.</td>
<td></td>
</tr>
<tr>
<td>EC.4</td>
<td>EC Identity Management System sends a notification to the ISA(s) that 21 days have passed for records flagged as ‘ready for termination’ and the IM system <strong>Disables</strong> account in <strong>Active Directory</strong> and Directory Services (<strong>LDP Sign on</strong>). In PeopleSoft the account roles get removed (exceptions apply).</td>
<td></td>
</tr>
<tr>
<td>EC.5</td>
<td>From the Data Warehouse, EC gets a report of employees that had a change in their job record and have a Banner account.</td>
<td></td>
</tr>
<tr>
<td>EC.6</td>
<td>In Banner, for employee with a change in their job record, EC locks their account.</td>
<td></td>
</tr>
<tr>
<td>End</td>
<td>Terminated employee no longer have edit access. There are instances where employees, such as retirees, keep self-service access role. Other case by case scenarios are addressed by EC</td>
<td></td>
</tr>
</tbody>
</table>
where certain level of access is retained by the former employee.

<table>
<thead>
<tr>
<th>SYS.1</th>
<th>PeopleSoft Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS.2</td>
<td>Identity Management System-People Database</td>
</tr>
<tr>
<td>SYS.3</td>
<td>Banner System</td>
</tr>
</tbody>
</table>

Note: Process maps for Appendices D-F are available upon request.
APPENDIX G: Glossary

TAC

*Texas Administrative Code*

TAC 202
Title 1 > Part 10 > Chapter 202, Subchapter C

FISMA

Federal Information Security Management Act

NIST SP 800-53


DIR

Texas Department of Information Resources Technology

DIR plays a leadership role in affecting Texas IT policy. Texas Government Code Chapter 2054, the Information Resources Management Act, describes information technology—or resources—as strategic assets that must be properly managed because of their value. The law affirms that sharing technologies is often the most prudent and efficient way to manage public information infrastructure to achieve the highest quality and most timely governmental services.

UTS 165

University of Texas System

UTS165 Information Resources Use and Security Policy

One of the policies for the UTEP’s Information Security Program, found in the Information Security Office website

Policies for the UTEP’s Information Security Program

UTEP policies, standards, and guidelines for the Information Security Program are located in the Information Security Office’s website

Termination Role

Once an employee is terminated, In the People Soft ERP business system, UT Share (Arlington TX) adds a “Termination Role” to the employee security profile. The new role will remove all other security roles and assign a self-service role. Note: accounts are never removed from People Soft.
"Current Active Employee-Rehired"  Means the user account was found to be in Active Account Report provided by the Account Administrator for Banner, PeopleSoft, and Active Directory. Then rehired during the testing period.

"Termination Role"  A role assigned to a terminated employee in PeopleSoft by UT Share in Arlington, TX. All roles are removed and this role is added and the self-service role is kept therefore they show in the Active Account Report provided by the Account Administrator for PeopleSoft.

"NewEmailType = 'D'"  The value set to determine that the Active Directory user account will be disabled 45 days after an appointment ends. Therefore during the testing period the user was active in the Active Account Report provided by the Account Administrator for Active Directory.

"Active Student"  The user account for a student in Active Directory that remains active for one year. Therefore during the testing period the user account was still active in the Active Account Report provided by the Account Administrator for Active Directory.

Active Directory  Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services. Windows Operating System Security for access management of users and devices.

Public Device  Is defined as any devices open to the public and therefore can be used without a UTEP account.