Departmental Change in Management Audit
Fiscal Year 2012

September 2013

The University of Texas at Austin
Office of Internal Audits
UTA 2.302
471-7117
The University of Texas at Austin
Internal Audit Committee

Mr. Frank W. Maresh, CPA, External Member, Chair
Mr. William C. Powers Jr., President
Dr. Steven W. Leslie, Executive Vice President and Provost
Mr. Kevin P. Hegarty, Vice President and Chief Financial Officer
Dr. Patricia L. Clubb, Vice President for University Operations
Ms. Patricia C. Ohlendorf, Vice President for Legal Affairs
Dr. Juan M. Sanchez, Vice President for Research
Dr. Gage E. Paine, Vice President for Student Affairs
Dr. Charles A. Roecke, Deputy to the President
Ms. Mary E. Knight, CPA, Associate Vice President
Mr. Paul Lieberman, Chief Compliance Officer and Director, University Compliance Services
Mr. Cameron D. Beasley, University Information Security Officer
Mr. William O’Hara, External Member
Mr. Tom Carter, External Member
Ms. Lynn Utter, External Member
Mr. Michael W. Vandervort, Director, Office of Internal Audits
Mr. J. Michael Peppers, Chief Audit Executive, The University of Texas System

The University of Texas at Austin
Office of Internal Audits

Director: Michael Vandervort, CPA
Assistant Directors: Angela McCarter, CIA, CRMA
                     *Chris Taylor, CIA, CISA
Auditor III: Ashley Foster, CPA
              *Brenda Guerrero
Auditor II: Cameosha Jones
Auditor I: Cynthia Martin-Hajmasy
           Miranda Pruett
           Derek Stuart
Sr. IT Auditor: *Tod Maxwell, CISA, CISSP
IT Auditor: *Brandon Morales, CISA, CGAP

* denotes project members

This report has been distributed to Internal Audit Committee members, the Legislative Budget Board, the State Auditor’s Office, the Sunset Advisory Commission, the Governor’s Office of Budget and Planning, and The University of Texas System Audit Office for distribution to the Audit, Compliance, and Management Review Committee of the Board of Regents.

Departmental Change in Management Audit
Project Number 779.12
September 11, 2013

President William C. Powers, Jr.
The University of Texas at Austin
Office of the President
P.O. Box T
Austin, Texas 78713

Dear President Powers,

We have completed seven additional audits of departmental units at the University which concludes the Departmental Change in Management Audit for fiscal year 2012. Our scope included 16 units selected based on a risk assessment and changes in departmental management as part of our Fiscal Year 2012 Audit Plan. Our audit process included surveying department heads by questionnaire, interviewing management and staff in each unit, reviewing electronic office structures, and transaction testing.

We completed and previously submitted reports on nine units. Due to the individual nature of each review, we have attached the following reports for your information:

0860-000 Department of Finance  
0840-000 Department of Accounting  
1400-000 Department of Electrical and Computer Engineering  
0100-000 Department of Anthropology  
0430-000 Department of Middle Eastern Studies  
3900-000 Tarlton Law Library (reissue)  
4035-000 University of Texas Elementary School (reissue)

For the 16 units, a total of 87 recommendations were made. 58 of those recommendations were related to Information Systems Security. The top five common findings between all of the units reviewed were also related to Information Systems Security. We have attached two lists with a more detailed overview of the recommendations that were made.

We appreciated the cooperation and assistance of all University personnel involved in this review and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA  
Director

cc: Internal Audit Committee Members
# FY12 Change in Management Audit

## Recommendations by Unit

<table>
<thead>
<tr>
<th>Unit</th>
<th>Unit Code</th>
<th>Recommendations</th>
<th>IT Rec.</th>
<th>Non-IT Rec.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dept of Elec &amp; Computer Engineering</td>
<td>1400-000</td>
<td>14</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>Dept of Middle Eastern Studies</td>
<td>0430-000</td>
<td>11</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>UT Elementary School</td>
<td>4035-000</td>
<td>8</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>UT Press</td>
<td>6130-000</td>
<td>7</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>Univ Development Office</td>
<td>5010-000</td>
<td>7</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Dept of Anthropology</td>
<td>0100-000</td>
<td>7</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Tarlton Law Library</td>
<td>3900-000</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Dept of Sociology</td>
<td>0680-000</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Dept of Finance</td>
<td>0860-000</td>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Dept of Accounting</td>
<td>0840-000</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>College of Natural Sciences (CNS)*</td>
<td>0083-000</td>
<td>4</td>
<td>0*</td>
<td>4</td>
</tr>
<tr>
<td>Texas Student Media</td>
<td>4620-000</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Dell Pediatric Research Institute (DPRI)</td>
<td>0055-000</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Petroleum Extension Services (PETEX)</td>
<td>3593-000</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Professional Development Center</td>
<td>3550-000</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ctr for Info Assurance &amp; Security (CIAS)*</td>
<td>2631-000</td>
<td>0</td>
<td>0*</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>87</strong></td>
<td><strong>58</strong></td>
<td><strong>29</strong></td>
</tr>
</tbody>
</table>

* IT Section was not audited.
<table>
<thead>
<tr>
<th>Recommendation Category</th>
<th>No. from all Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information System Security - Securing Unattended Devices</td>
<td>12</td>
</tr>
<tr>
<td>Information System Security - Administrative Access</td>
<td>7</td>
</tr>
<tr>
<td>Information System Security - Physical Access to Servers</td>
<td>6</td>
</tr>
<tr>
<td>Information System Security - Disaster Recovery Plan (DRP)</td>
<td>6</td>
</tr>
<tr>
<td>Information System Security - Compliance Training</td>
<td>6</td>
</tr>
<tr>
<td>Entertainment and Official Occasion Expenditures</td>
<td>5</td>
</tr>
<tr>
<td>Information System Security - Backup Recovery of Systems and Data</td>
<td>4</td>
</tr>
<tr>
<td>Information System Security - Position of Special Trust Forms (PoST)</td>
<td>4</td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling - Locked Bag</td>
<td>4</td>
</tr>
<tr>
<td>Purchasing Activities</td>
<td>3</td>
</tr>
<tr>
<td>Information System Security - Management of Sensitive Digital Data</td>
<td>2</td>
</tr>
<tr>
<td>Information System Security - Software Licensing</td>
<td>2</td>
</tr>
<tr>
<td>Information System Security - System Hardening</td>
<td>2</td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling - Document Transfer of Funds</td>
<td>2</td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling - Training</td>
<td>2</td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling - Pre-Numbered Receipts</td>
<td>2</td>
</tr>
<tr>
<td>General Departmental Information</td>
<td>2</td>
</tr>
<tr>
<td>Information System Security - Account Management</td>
<td>1</td>
</tr>
<tr>
<td>Information System Security - Passwords</td>
<td>1</td>
</tr>
<tr>
<td>Information System Security - Automatic Computer Updates</td>
<td>1</td>
</tr>
<tr>
<td>Information System Security - Portable Computing &amp; Remote Access</td>
<td>1</td>
</tr>
<tr>
<td>Information System Security - Support Staff</td>
<td>1</td>
</tr>
<tr>
<td>Information System Security - Virus Definitions</td>
<td>1</td>
</tr>
<tr>
<td>Information System Security - Operating System Upgrades</td>
<td>1</td>
</tr>
<tr>
<td>Information System Security - Firewalls</td>
<td>1</td>
</tr>
<tr>
<td>Authorization for Individual Services</td>
<td>1</td>
</tr>
<tr>
<td>Contracts</td>
<td>1</td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling - Weekly Deposits</td>
<td>1</td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling - Transporting Deposits</td>
<td>1</td>
</tr>
<tr>
<td>Petty Cash - Reconciliation and Reimbursement Vouchers</td>
<td>1</td>
</tr>
<tr>
<td>Account Reconciliation</td>
<td>1</td>
</tr>
<tr>
<td>Merchandise for Resale</td>
<td>1</td>
</tr>
<tr>
<td>Inventory</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>87</strong></td>
</tr>
</tbody>
</table>
MEMORANDUM

To:       Dr. Ahmed Tewfik, Department Chair
          Department of Electrical & Computer Engineering

From:     Mr. Michael Vandervort, CPA
          Director

Subject:  Final Report – Change in Management Audit, Fiscal Year 2012
          Unit #1400-000: Department of Electrical and Computer Engineering

Date:     September 6, 2013

We have completed our audit of your compliance with and awareness of certain policies and procedures of The University of Texas at Austin (UT Austin).

We reviewed internal controls in the following areas:

- Electronic Office Structure,
- General Departmental Information/Organization/Activities,
- Account Reconciliations,
- Endowed/Gift Administration,
- Cash and Cash Equivalent Handling,
- Petty Cash,
- Inventory,
- Controlled Items,
- Purchasing Activities,
- Procurement Cards,
- Travel Expenditures,
- Entertainment and Official Occasion Expenditures,
- Authorization for Individual Services,
- Contracts,
- Time Reporting, and
- Information Systems Security.

We performed the following procedures to complete this audit:

- Surveyed via a questionnaire to ascertain your reported strength in internal controls and compliance with UT Austin rules;
- Tested information systems security, entertainment and official occasion transactions, endowment transactions, and annual physical inventory completion;
- Reviewed your electronic office structure and employees’ appointment statuses; and
- Clarified follow-up issues with you and your staff.
This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and with *Government Auditing Standards*.

Based on the above procedures, the Department of Electrical and Computer Engineering (ECE) appears to have reasonable to strong controls in most areas. However, fourteen opportunities for improvement were noted. Twelve of the recommendations were related to Information Systems Security.

**Information Systems Security – Physical Access**
Non-IT staff may have access to the server room which is protected by a traditional lock and key. There are no plans to upgrade the server room at this time because the building is scheduled to be torn down. Without adequately securing the server room, there is an increased risk of unauthorized access to and/or loss of UT Austin information stored on the server.

According to Section 5.19.2.2 of UT Austin’s *Information Resources Use and Security Policy*, “all facilities supporting information resources must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and the systems housed in that facility.”

### Recommendation 1:
Management should ensure that at the current location, the server is accessible to IT staff only. In accordance with UT System’s recent virtualization and colocation initiative to increase security and decrease cost, the Internal Audit Committee suggests that all departments should make every effort to move servers to the University Data Center unless an exception is granted by the Information Security Office (ISO). If ECE has servers at the new location, management should ensure that the server is physically secured behind a locked door with a locking mechanism such as a Building Access Control System or Locknetics style device that logs access to the room and is only accessible to ECE IT employees.

**Management Response:** ECE is migrating web services to the UDC during summer 2013. File storage services (the ECE “filer”) is scheduled to be migrated to the UDC in fall 2013. Servers that remain within the ENS building are not used to store or access sensitive information and fall into one of two categories: (1) compute servers for specialized software used in teaching and research (2) license servers which provide software license provisioning for special-purpose software used in the department.

Management notes that the server room is locked and accessible only to IT personnel, and that upgrading the lock to an electronic lock does not appear to be an effective use of funds given that the building is slated for demolition.

**Implementation Date:** Migration of web services to the UDC to be completed by September 30, 2013. ECE filer to be migrated to the UDC by October 30, 2013.
**Information Systems Security – System Hardening**

Machines that are not centrally managed may not be updated on a regular basis. In addition, testing indicated that two of four computers did not have the automatic updates setting enabled and had pending updates of more than a month old. Without timely automatic updates on machines, there is an increased risk that information resources are more susceptible to unauthorized access, viruses, and malware.

According to Section 4.5.2 of UT Austin’s *Minimum Security Standards for Systems*, “operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures.”

**Recommendation 2:** Management should create a more centrally managed computing environment that ensures software updates are automatically applied to all UT Austin owned computers.

**Management Response:** Computers of administrative personnel are centrally managed by UT-ITS. Faculty, students, postdocs and other research personnel utilizing a UT Austin device will also be given the option to have their systems centrally managed. The remaining faculty, students, postdocs and other research personnel will be required to implement the *Electrical and Computer Engineering Security and Use Guidelines for Self-Managed Computers* (ECE-SUGSMC) for self-managed computers. The ECE-SUGSMC address practices for securing Windows, Mac and Linux computing devices. The effectiveness of these guidelines will be monitored and these guidelines will continue to be refined. All users of equipment that is not centrally managed will be required to complete an acknowledgement form per the ECE-SUGSMC guidelines. The acknowledgement forms will be collected annually and retained by ECE-IT. The acknowledgement form requires a statement from the primary user of the machine stating that user’s acceptance of the requirements that the system be appropriately hardened, and requiring the user to specify the mechanism (e.g., software configuration manager) that will be used to ensure that updates are regularly applied. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.

Management notes that there are several ways in which effective and practical centralized management is difficult to implement because of the unique needs of faculty, students, postdocs and other research personnel toward performing the mission of the ECE department. These individuals frequently work quite varied hours beyond the reasonable limits of UT IT support, assemble their own computer systems, install and/or develop their own research-specific software, and are frequently away from campus in locations where UT IT support may be unavailable at critical times.

**Implementation Date:** Acknowledgement forms to be collected by September 30, 2013.
Information Systems Security – Administrative Access

All faculty and student techs have administrative access to their machines. When users operate with administrative rights at all times, it is difficult to protect against unauthorized access to data, software installations, and system configuration changes to workstations.

According to Section 5.4.1 of UT Austin’s Information Resources Use and Security Policy, “individuals who use accounts with special privileges (for example System Administrators) must use these accounts only for their intended administrative purposes.”

Recommendation 3: Management should create a more centrally managed environment that ensures users do not operate workstations with administrative rights unless required for a specific business function. If determined necessary, a new user account with administrative rights should be created and used to perform administrative functions apart from their day-to-day activities.

Management Response: Computers of administrative personnel are centrally managed by UT-ITS. Faculty, students, postdocs and other research personnel utilizing a UT Austin device will also be given the option to have their systems centrally managed. The remaining faculty, students, postdocs and other research personnel will be required to implement the ECE-SUGSMC for self-managed computers. The ECE-SUGSMC address practices for securing Windows, Mac and Linux computing devices. The effectiveness of these guidelines will be monitored and these guidelines will be continued to be refined. All users for equipment that is not centrally managed will be required to complete an acknowledgement form per the ECE-SUGSMC guidelines. The acknowledgement forms will be collected annually and retained by ECE-IT. The ECE-SUGSMC requires that users create a standard (non-administrator) logon for the device and that this logon be the primary logon used for daily activity. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.

Management notes that there are several ways in which effective and practical centralized management is inconsistent with the needs of faculty, students, postdocs and other research personnel toward performing the mission of the ECE department. These individuals frequently work quite varied hours beyond the reasonable limits of UT IT support, develop their own computer systems, install and/or develop their own research-specific software, and are frequently away from campus in locations where UT IT support may be unavailable at critical times.

Implementation Date: September 30, 2013
Information Systems Security – System Hardening, Administrative Access

ECE IT staff does not know about all machines in the department because some are purchased without their knowledge. In addition, users have the ability to install their own computers and/or change configuration settings to those that may not meet UT Austin’s Minimum Security Standards for Systems. Therefore, ECE may have Category I Data stored on unsecured machines. Without ensuring that Category I Data is secure at all times, there is an increased risk of data being compromised.

According to Section 5.11.3 of UT Austin’s Information Resources Use and Security Policy, unless otherwise required by federal or state law or regulation, “Category I Digital Data must not be stored, processed, or transmitted on UT Austin or non-UT Austin owned computers or other electronic devices (e.g., laptop, hand-held device, Flash drives, or other Portable Computing Devices) unless:

- It is secured against unauthorized access in accordance with this policy,
- It will not compromise business or research efforts or privacy interests if lost or destroyed, and
- UT Austin has specific procedures in place that address this sub-section.”

**Recommendation 4:** Management should create a more centrally managed computing environment that ensures all Category I Data is identified, departmental computers are configured to follow the Minimum Security Standards for Systems, and that departmental configuration standards are documented.

**Management Response:** Computers of administrative personnel are centrally managed by UT-ITS. Faculty, students, postdocs and other research personnel utilizing a UT Austin device will also be given the option to have their systems centrally managed. The remaining faculty, students, postdocs and other research personnel will be required to implement the ECE-SUGSMC for self-managed computers. The ECE-SUGSMC address practices for securing data and computer systems that may contain sensitive data, including retention schedules, backup policies and encryption requirements. The guidelines cover securing data stored in the cloud. The effectiveness of these guidelines will be monitored and these guidelines will be continued to be refined. All users for equipment that is not centrally managed will be required to complete an acknowledgement form per the ECE-SUGSMC guidelines. The acknowledgement forms will be collected annually and retained by ECE-IT. The acknowledgment form requires a statement from the primary user of the machine stating whether the machine will be used to create and/or access potentially sensitive information, and the mechanisms in place to ensure that sensitive data is secure (e.g., encryption) regardless of where it is stored. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.
Management notes that there are several ways in which effective and practical centralized management is inconsistent with the needs of faculty, students, postdocs and other research personnel toward performing the mission of the ECE department. These individuals frequently work quite varied hours beyond the reasonable limits of UT IT support, develop their own computer systems, install and/or develop their own research-specific software, and are frequently away from campus in locations where UT IT support may be unavailable at critical times.

**Implementation Date:** September 30, 2013

**Information Systems Security – Management of Sensitive Digital Data**
The department does not follow or enforce UT Austin’s Records Retention Schedule for disposal of digital data containing Category I data. Without disposing digital data according to the records retention schedule, there may be increased risk of unauthorized access to the unit’s data.

According to Section 5.11.4.2 of UT Austin’s *Information Resources Use and Security Policy*, “the university shall discard electronic media (for example, disks, tapes, hard drives, etc.) containing Category I-Data is accordance with university’s records retention schedule.”

**Recommendation 5:** Management should ensure that data is discarded or deleted in accordance with UT Austin’s Records Retention Schedule.

**Management Response:** ECE has recently designated a permanent staff person as the records manager for all department information. This staff person has been trained in UT records policy. For records created by the ECE administrative office, this staff person will have direct oversight to ensure that records are retrained, managed and discarded in accordance with UT policy.

The responsibility to manage information consistent with UT Austin Records Retention Schedule is clearly identified in the ECE-SUGSMC. To assist faculty and staff to comply with these requirements, ECE actively encourages important records to be housed in secure, centralized locations (SharePoint, UT Box). Beginning in fall 2013, ECE will extend this practice to include short-term appointed instructional staff (e.g., Teaching Assistants and Adjunct Faculty). At the start of each appointment, TAs and Adjuncts will be required to complete an acknowledgement form stating that they are aware and will comply with University requirements for securing and retaining any category 1 data produced during their appointment and the use of such information during their appointment. At the end of each appointment period, a second acknowledgement form will be required stating that all category 1 information has been appropriately secured in a University owned location for retention, and that any such information has been removed from any personally-owned device (even if that device is encrypted).
Implementation Date: September 30, 2013

Information Systems Security – Portable Computing and Remote Access
Non-centrally managed laptops may not be encrypted. There is an increased risk of unauthorized access, modification, or disclosure of Category I Data on laptops without encryption.

According to Section 5.20 of UT Austin’s Information Resources Use and Security Policy, “All university-owned laptop computing devices must be encrypted, regardless of data classification, using products and/or methods approved by the UT Austin Chief Information Security Officer” and “All non-university-owned portable devices with a demonstrated business need to store Category-I university data must be encrypted using products and/or methods approved by the UT Austin Chief Information Security Officer.”

Recommendation 6: Management should identify all centrally managed and non-centrally managed laptops that may contain Category I data and ensure that they are encrypted using products and/or methods approved by the ISO.

Management Response: Management believes that all UT-owned laptops are encrypted and that ECE is in compliance with UT policy regarding encryption of portable devices. All university-owned laptops used by ECE personnel were encrypted during the 2012 calendar year. UT encryption policies mandating encryption of personally-owned devices that may be used to access sensitive data were communicated to all faculty and staff as part of the encryption rollout during 2012.

Beginning in fall 2013, ECE will additionally enforce information security guidelines on short-term appointed instructional staff (e.g., Teaching Assistants and Adjunct Faculty). At the start of each appointment, TAs and Adjuncts will be required to complete an acknowledgement form stating that they are aware and will comply with University requirements for securing and retaining any category 1 information produced during their appointment. The acknowledgement form requires the user to indicate what encryption method is being used on any personally-owned device(s). At the end of each appointment period, a second acknowledgement form will be required stating that all category 1 information has been appropriately secured in a University-owned location for retention, and that any such information has been removed from any personally-owned device (even if that device is encrypted).

Management restates that ECE is already in compliance with UT requirements that all UT-owned laptops are encrypted using an approved encryption method. This includes both centrally managed and non-centrally managed devices. Going forward, users of non-centrally managed devices will be additionally required to complete annually an acknowledgement form accepting the responsibilities of the ECE- SUGSMC and to indicate on that form the encryption method used for
each device. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.

**Implementation Date:** Acknowledgement forms to be instituted by September 30, 2013

**Information Systems Security – Software Licensing**
The department does not log or track software licenses on non-centrally managed machines. Without logging all software on all UT Austin owned devices, software may be installed on to computers without the proper license.

According to Section 5.24 of UT Austin’s *Information Resources Use and Security Policy*, “all software used on university computers will be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious violation subject to disciplinary action and any such use is without the consent of the university.”

**Recommendation 7:** Management should ensure that software on all UT Austin owned computers have a valid software license and are tracked. This information should be reviewed annual to ensure compliance with software license agreements.

**Management Response:** For specialized software licensed directly by ECE and used on centrally managed computers (e.g., teaching labs and computation servers used in support of the educational mission of the department), ECE maintains licensing records and actively runs licensing servers to ensure that the software usage complies with the terms of the license agreements. This software is tracked annually.

For standard software covered by site license or similar broad agreements with UT or UT System (e.g., Microsoft Office), ECE will distribute software only to UT-owned systems covered by the license terms. Faculty and staff seeking to install such software on personally owned devices must obtain that software from Campus Computers, which tracks licenses.

For other software, including a very large number of open-source and freely-distributed software packages, ECE does not track specific usage of the software. However, ECE reminds all users that software must be used in accordance with all appropriate licenses. Additionally, beginning fall of 2013, faculty, students, postdocs and other appointed research personnel as well as all short-term appointed instructional staff (Teaching Assistants and Adjuncts) will be required to complete an acknowledgement form per the ECE-SUGSMC guidelines. The acknowledgement form requires users to certify that all computing hardware and software is used in accordance with UT’s Acceptable Usage Policy, and that these requirements include both university owned and personally owned devices used for university
purposes. These forms will be collected annually and retained by ECE-IT. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.

**Implementation Date:** September 30, 2013

**Information Systems Security – Disaster Recovery Plan, Back up Recovery of Systems and Data**
The department does not have a documented disaster recovery plan (DRP). Without a documented DRP in place, ECE administrators may not be able to adequately recover critical systems and data in the event of a disaster.

According to Section 5.5.2 of UT Austin’s Information Resources Use and Security Policy, “each college, school, or unit responsible for a system(s) should maintain a [DRP]. The recovery plan includes the following:

- Procedures for recovering data and applications in the case an unexpected event occurs such as natural disaster, power or system disk failure, espionage, data entry error, human error, or other systems operations errors;
- Assignments of operational responsibility for backup of all systems connected to the respective network;
- Requirements for off-site storage needs;
- Physical and network access controls for on-site and off-site storage;
- Processes to ensure backups are viable and can be recovered (for example, routine testing of backup and recovery procedures.)”

**Recommendation 8:** Management should ensure that a comprehensive documented DRP exists within UT Austin’s Restarting Texas DRP application for all critical information resources and this it is tested at least annually. Additionally, the DRP should be kept up-to-date as staff and/or systems change.

**Management Response:** Computers of administrative personnel will be moved to Absolute Manage as overseen by UT-ITS so that we may centrally manage the infrastructure. Critical information stored on centrally managed devices are backed up securely by ITS. Faculty, students, postdocs and other research personnel utilizing a UT Austin device will also be given the option to have their systems centrally managed. The remaining faculty, students, postdocs and other research personnel will be required to implement the ECE-SUGSMC for self-managed computers. The ECE-SUGSMC address backup and disaster recovery, including use of UT Backup which has been purchased for UT faculty members. The effectiveness of these guidelines be monitored and these guidelines will continue to be refined. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.
ECE servers are being reviewed for possible migration to the UDC. Servers that provide mission-critical services are recognized as high-priority for relocation to the UDC. Web servers are already being migrated to the UDC. For servers that are not migrated, the ECE DRP will identify how any critical data will be backed up. The ECE DRP is currently being developed and will be completed in fall 2013 and updated, reviewed and tested annually thereafter.

**Implementation Date:** The ECE DRP is expected to be completed by October 31, 2013.

**Information Systems Security – Support Staff**
The ECE IT department has lost staff that have not been replaced. Also, within the last year the ECE IT department has taken over IT operations at the Microelectronics Research Center. According to the 2012 Information Security Office Risk Assessment, ECE has 2,340 computers with four staff members to support those computers in a non-centrally managed environment. Without an adequate number of employees supporting the IT environment, there is an increased risk to UT Austin information resources.

According to Information Technology Services (ITS), depending on the environment, one full time employee per 200 machines is optimal after going through a process of “standardizing” a site.

**Recommendation 9:** Management should add additional support for IT needs, either in the form of additional staff or through a contract with ITS. If additional support is added, they should have expertise in this area.

**Management Response:** Management acknowledges that the ECE IT team is smaller than is necessary to optimally support all of ECE’s computing and information management needs. However, ECE has no additional resources to invest in IT administration, and any additional investment would have to come from funds diverted from ECE’s educational responsibilities. Given that ECE’s educational budget is already stretched, management feels that any further diversion of resources would result in ECE failing to meet its educational responsibilities.

Management notes that ECE minimizes the impact of any staffing gap by leveraging the expertise of our faculty and, where appropriate, our students. Computing and networking technologies are core competences for many in the ECE community. Several ECE faculty are recognized international experts in these fields, and dozens of our students are hired into technical positions in the computing and information technology industries every year.

**Implementation Date:** Not applicable
Information Systems Security – Securing Unattended Devices
Testing indicated that two of four computers did not have the password protected screensaver setting enabled and another computer had the setting enabled to activate after 30 minutes of inactivity. Unauthorized access to unattended devices may result in harmful or fraudulent disclosure, modification, or deletion of sensitive electronic data. In addition, it may lead to the misuse of critical applications or email accounts.

According to Section 5.18.5 of UT Austin’s Information Resources Use and Security Policy, “unattended computing devices must be secured from unauthorized access. Logical security options include screen saver passwords and automatic session time-outs.”

As a best practice, password-protected screensavers should activate after 15 minutes of idle time.

**Recommendation 10:** Management should ensure that the password-protected screensaver settings are enabled to activate after 15 minutes of idle time.

**Management Response:** Computers of administrative personnel will be moved to Absolute Manage and placed on the Austin active directory as overseen by UT-ITS so that we may centrally manage the infrastructure. This move will allow us to use group policy to make sure that password protected screen-savers are used. Password required screensavers will lock after 15 minutes of inactivity. Faculty, students, postdocs and other research personnel utilizing a UT Austin device will also be given the option to have their systems centrally managed. The remaining faculty, students, postdocs and other research personnel will be required to implement the ECE-SUGSMC for self-managed computers. The ECE-SUGSMC address securing unattended computers and include the requirement that computers lock after 15 minutes of inactivity. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.

**Implementation Date:** September 30, 2013

Information Systems Security – Virus Definitions
Machines that are not centrally managed may not have virus definitions updated on a regular basis. In addition, testing indicated that one of four computers did not have current anti-virus definitions. Without timely automatic updates on machines, there is an increased risk that information resources are more susceptible to unauthorized access, viruses, and malware.

According to Section 4.3 of UT Austin’s Minimum Security Standards for Systems, “anti-virus software must be installed and enabled.” Additionally, “anti-virus and, if applicable, anti-spyware, software should be configured to update signatures daily.”
**Recommendation 11:** Management should create a more centrally managed computing environment that ensures machines are configured with anti-virus software installed and enabled, and that virus definitions are updated daily.

**Management Response:** UT policy requires that an active anti-virus software subscription be used on all UT owned devices and any personally-owned devices that are connected to UT networks or used to access UT data. To better ensure that ECE faculty, staff and students are abiding by these requirements, ECE will begin requiring an annual acknowledgement form from all users of self-managed devices. This form requires the user to agree to follow the requirements of the ECE-SUGSMC and requires that the type of anti-virus software in use be identified on the form. Self-administered machines will be subject to random audit by ECE IT staff. Each semester, ECE will randomly select at least 5% of all of the self-managed systems to audit for compliance with the ECE-SUGSMC.

In addition, ECE is working with the ISO and campus networking to select and deploy network scanning technology that will report systems on the ECE network that are not properly protected by anti-virus software.

**Implementation Date:** September 30, 2013

**Information Systems Security – Compliance Training**
Fifty two out of 316 employees had not completed TX Class CW 170 – IT Security Awareness. There is an increased risk of security incidents if employees are not properly trained regarding the use of department information resources.

According to Section 5.22 of UT Austin’s *Information Resources Use and Security Policy*, all employees are required to take security awareness General Compliance training within the first 30 days of employment and every two years thereafter.

**Recommendation 12:** Management should ensure that all employees complete TX Class CW – IT Security Awareness within the first 30 days of employment and every two years thereafter.

**Management Response:** Management notes that permanent staff and full-time faculty are generally up to date on this mandatory compliance training. ECE will continue to validate that each of the faculty and staff complete compliance training modules as necessary. Faculty and staff who are not in compliance are reported to the department chairman for appropriate action.

Management notes that most of the employees identified in this audit were part time employees, largely student employees. ECE believes that this issue can be rectified by (1) including a written reminder that this training is mandatory as part of the appointment process for new teaching
assistants and research assistants, and (2) verifying that all necessary compliance training modules have been completed before a student can be re-appointed.

**Implementation Date:** September 30, 2013

**Cash and Cash Equivalent Handling – Transporting Deposits**
A locked bag is not used to transport funds for deposit. When a locked bag is not used, there is an increased risk of loss of funds.

According to the Cash Handling section of The University of Texas System Policy 166, “All cash, physical checks and receipts should be transported in tamper proof bags.”

**Recommendation 13:** Management should ensure that a locked bag is used when transporting funds.

**Management Response:** We have purchased a locked bag and are currently using for deposits.

**Implementation Date:** Implemented (May 2013)

**Petty Cash – Reconciliation and Reimbursement Vouchers**
The department does not reconcile the petty cash fund monthly. Without a monthly reconciliation there is an increased risk of funds being unaccounted for.

The department does not prepare reimbursement vouchers at least monthly, when it is used, to replenish the petty cash fund. There is an increased risk of loss or misuse of funds when reimbursement vouchers are not prepared in a timely manner.

As a best practice, a monthly reconciliation of the petty cash fund should be completed and documented. The reconciliation should be conducted by the responsible person or someone besides the petty cash custodian(s). The petty cash fund should be replenished in a timely manner after it has been used.

**Recommendation 14:** Management should ensure that the petty cash fund is reconciled monthly and documented, even if there is no activity and that reimbursement vouchers are prepared in a timely manner. Management should consider using a procard for the purchases or closing the petty cash fund if the benefit does not outweigh the time to manage the fund.

**Management Response:** The account was closed in July 2013 as it was rarely used.

**Implementation Date:** Closed July 11, 2013
Attached you will find a Change in Management Report Card, which is based on our understanding of the controls in place in your unit at the time of our review. If fully implemented, the recommendations above would improve your overall evaluation.

We appreciate the assistance and cooperation of you and your staff in this audit and hope that the information presented herein is beneficial. If you have any questions, please contact Brenda Guerrero at 471-9256 or brenda.guerrero@austin.utexas.edu.

MV: bg

Attachment

cc: Dr. Gregory Fenves, Dean, Cockrell School of Engineering
    Dr. Steven Leslie, Executive Vice President and Provost
<table>
<thead>
<tr>
<th>Areas Reviewed</th>
<th>Reasonable to Strong Controls in Place</th>
<th>Opportunity for Improvements</th>
<th>Significant Deficiencies</th>
<th>Material Weaknesses</th>
<th>Not Applicable to the Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Office Structure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Departmental Information/Organization/Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Reconciliation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endowed/Gift Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outside Employment/Conflict of Interest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Registers/Cashiers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts Receivable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Petty Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Merchandise for Resale</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlled Items</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchasing Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement Cards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Travel Expenditures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment and Official Occasion Expenditures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization for Individual Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information System Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ A weakness that significantly impacts the UT Austin's operations or finances