COLLEGE OF FINE ARTS
AUDIT OF ALLEGATIONS REGARDING MISUSE OF COMPUTER EQUIPMENT

THE UNIVERSITY OF NEW MEXICO

Report 2007-32
November 9, 2007

Audit Staff

G. Christine Chavez, Audit Director
Yvonne Cox, Audit Manager
Lisa Wauneka, Information Systems Auditor

CONTENTS

ABBREVIATIONS

Associate Dean	Associate Dean for Student Affairs and Technology
CIO	Interim Chief Information Officer
CFA	College of Fine Arts
Continuing Ed	Division of Continuing Education and Community Services

College	College of Fine Arts
CSG	Computer Support Group
Internal Audit	Internal Audit Department
IT	Information Technology
UBP	University Business Policies and Procedures Manual
University	The University of New Mexico

EXECUTIVE SUMMARY

The Internal Audit Department (Internal Audit) received a complaint regarding computer misuse in the College of Fine Arts (CFA). The complainant alleged that the faculty and staff at the CFA were violating University policy regarding information technology (IT). The complainant stated when the policy violations were brought to management's attention; they did not act on the complaints. The complainant further alleged that a CFA employee was "making illegal copies of music" during work hours. We found some evidence which indicates that the allegations appear valid.

We found that the CFA is not complying with The University of New Mexico (University) policy regarding IT requirements. To comply with the policy, the CFA will need to develop and document their departmental information security practices, communicate them to the CFA staff and faculty, and have a process in place to address information security violations. To help the colleges and departments create written security practices for their operations, the University needs to develop specific standards and guidelines outlining the practices the colleges and departments should put in place.

During the audit we also found pornography stored on a UNM laptop. In addition, CFA processed an inaccurate tuition remission form to pay for consulting services.

INFORMATION TECHNOLOGY SECURITY

The Dean of the CFA should assure that the CFA develops information security practices as required by University policy. The Dean of the CFA responded they will develop policies for security practices.

ALLEGATIONS OF MUSIC COPYRIGHT VIOLATIONS

The Dean of the CFA should ensure that the CFA develops a structure for the Computer Support Group that provides management oversight. The Dean of the CFA responded they will create a new IT structure in the CFA.

USING TUITION REMISSION TO PAY FOR CONSULTING

The Dean of the CFA should ensure that the Division of Continuing Education and Community Services is paid for their consulting services. The Dean of the CFA and the Dean of the Division of Continuing Education and Community Services should work with the Deputy Provost and the Human Resources Department, as appropriate, to determine if disciplinary action is appropriate for those involved in processing the inaccurate *Tuition Remission Form*. The Deans of the CFA and Continuing Ed responded they are working with the appropriate offices regarding possible disciplinary action.

UNIVERSITY INFORMATION TECHNOLOGY

The Interim Chief Information Officer (CIO) should complete the hiring process for the information security officer, develop specific standards and guidelines outlining the departmental security practices, and develop a process for investigating security violations. The CIO responded that he will complete the hiring process for the Director of Information Assurance. This Director will conduct a review of UNM IT security policies and will institute a review of security practices in departmental IT support groups. The policy review will include a recommendation on the best place to address the issue of reporting and investigating violations of UNM IT policies.

PORNOGRAPHY ON UNIVERSITY EQUIPMENT

The Human Resources Department should address, in University policy, the allowability of pornography on University computer equipment. The Interim Vice President for Human Resources responded she will work with University Counsel to draft a proposed policy.

INTRODUCTION

BACKGROUND

The CFA, founded in 1936, is recognized as a cultural resource contributing to the quality of life in New Mexico. It has 115 regular faculty and staff and 1,300 students seeking degrees in the arts. It offers bachelor's degrees, master's degrees, and terminal degrees in selected areas. Per the CFA, its annual budget is $8,500,000.

In the CFA, the Computer Support Group (CSG) is responsible for designing new technologies, providing desktop support for about 350 computers, and maintaining two file servers and one web server. The CSG has three employees: a Senior LAN Administrator, a System Analyst 3, and a System Analyst 2. The Senior LAN Administrator and the System Analyst 3 report to the Associate Dean for Student Affairs and Technology (Associate Dean) in the CFA. The System Analyst 2 reports to the Senior LAN Administrator.

Internal Audit received a complaint regarding misuse of computer equipment in the CFA. The allegation is that the CFA:

- does not have security policies and does not enforce basic IT security;
- did not investigate or resolve the complainant's security violation allegations;
- had computers containing viruses and non-university software on University equipment resulting in compromised computers and servers;
- had software and music loaded on computers in violation of copyright laws;
- has an employee using University equipment to copy music checked out from the library; and
- IT staff, at the direction of management, performed activities that may have violated copyright laws or University policies.

PURPOSE

The purpose of the audit is to determine whether there was support for the allegations regarding misuse of computer equipment, especially with regard to the employee who was allegedly copying music. We also looked into other information regarding computer misuse that came to our attention during the review.

SCOPE

The review of the IT computer misuse was limited to interviews with the CFA employees, a review of visible files on computers in the office of the CSG employee who was allegedly copying music, and a limited review of some of the CFA personnel's University e-mail.

The review of the computers in the office of the employee who was allegedly copying music was limited to visible music files and software programs open on the computer. Internal Audit did not perform a forensic computer analysis, attempt to recover deleted files, or attempt to determine if the computers were compromised.

Internal Audit completed the fieldwork in August 2007.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

INFORMATION TECHNOLOGY SECURITY

Security Practices

When Internal Audit first received the complaint in February 2007, we met with the Dean and Associate Dean to discuss the misuse of computer equipment. The Dean and the Associate Dean acknowledged that the CFA does not have documented computer security practices. This lack of documented policies was confirmed by a May 3, 2007, follow-up memo from the Associate Dean to the Internal Audit Director. In that memo, the Associate Dean states “We plan to create drafts of our policies during the summer so that they will be ready for our approvals process in the early fall which begins with our IT Policy Committee, made up of members of our faculty and staff.”

The CFA administration has been working on their practices and structure for several years. However, we found evidence of only one approved practice on computer purchases. There was an additional practice in draft but we did not find evidence that this practice was approved. Neither of these practices discuss appropriate use of University IT resources as required by Section 1. "Computer Security Controls and Guidelines" Policy 2520, University Business Policies and Procedures Manual (UBP):

> …all departments operating University owned computers, including those operated by faculty, staff, and students, must develop departmental security practices which comply with the security practices listed below. In addition, departments must have environment-specific management practices for business functions such as maintenance, capacity planning, software licensing and copyright protection, training, documentation, power, and records management for computing systems under their control. …Departments must document and periodically review established practices.

Information Technology Security Complaint

We found evidence that, on at least two occasions, the Associate Dean received complaints of security violations from the CSG staff. The staff appropriately reported security violations to the department head per policy but we did not find evidence that the CFA investigated the complaints to detect and correct non-compliance in accordance with Section 2.3. "Computer Security Controls and Guidelines" Policy 2520, UBP.

At the time of the audit, the policy assigned the responsibility for detecting and correcting non-compliance with University computer policies to department heads or designees and directed employees to report non-compliance to the department heads. The policy did not tell employees what to do if the complaints are un-resolved by the department heads. The university-wide policy issues are discussed later in this report.

In this case, the complainant came to Internal Audit. Internal Audit performed a minimal computer investigation but does not have the tools or the manpower necessary to perform a complex computer investigation. We found the following evidence documenting complaints to the CFA regarding non-compliance with University computer policies and the CFA resolution to the complaints.

- The complainant documented concerns about the CFA staff and faculty's understanding of Federal Copyright infringements in the complainant's 2005 Performance Review. We found no evidence the CFA acted on this complaint. The Associate Dean told us that she was not informed of this complaint as she did not see the performance reviews for staff who did not report directly to her. In this case, the CSG staff member reported to another CSG staff member.
- In November 2006, the Associate Dean directed an employee to contact Information Technology Services (ITS) to ask for guidance regarding copyrighted material on the CFA workstations. The reason the CSG employee wrote to ITS was because a CFA employee wanted 10 gigabytes of personal music files moved to a new University computer; a CSG employee moved the personal music. In the e-mail written to ITS, the CSG employee states, "We [*are*] having some issues in regards to users having tons of copyrighted files on their workstations. These files are personally owned or illegal materials on their hard drives (MP3s, movies, etc.)…The last time we encountered this the user had 10 GBs of MP3s the user wanted moved." The indication from this CSG employee is that the 10 gigabytes of music was not an isolated incident. We noted that the Associate Dean received this e-mail which included the original e-mail. The Associate Dean told us that she met with the CSG employee who authored the e-mail. She concluded that, "…the IT support staff stated they had no actual evidence of whether videos and other materials were legally acquired or pirated; they simply were there." The Associate Dean saw this as a stopping point.
- The complainant told his supervisor about software copyright violations but the supervisor stated that the CSG did not have the authority within the CFA to police potential violations. We confirmed this in an interview with the complainant's supervisor.
- The CSG documented security violations in the CFA IT work order database. Internal Audit reviewed the work order database for calendar year 2005. We found 52 work orders related to viruses (58% of all incidents), copyright infringements, shared accounts, shared passwords, and non-university software programs. The Associate Dean told us that she did not review or analyze the work order database so she was unaware of the security violations. We did not find evidence that the CFA developed written practices to address these risks.

The Associate Dean and the CSG staff indicated that they had unwritten practices. If the practices are not written it is difficult to enforce them and, when challenged, employees do not have a written document to support their actions.

Furthermore, the lack of documented security practices in the CFA may result in the following:

- increased risk to the University of fines and penalties for violations of federal regulations including copyright violations;
- insecure systems resulting in lost or stolen sensitive data which may damage the University's reputation;
- inefficient use of both computer users' and analysts' time in responding to incidents and repairing the damage caused by lack of security practices; and
- unreliability of the CFA network and computers.

It appears that the Associate Dean knew that the CSG staff had concerns about security. However, we did not find evidence that CFA developed, documented, or adapted computer security practices in response to their concerns.

Recommendation 1

The CFA needs to develop and document their security practices in accordance with "Computer Security Controls and Guidelines" Policy 2520, UBP. The security practices should address incidents where software and files for non-university use are identified. For these incidents, the policies should have steps to investigate and remove software and files which violate copyrights, compromise the computer security of the CFA or are incompatible with the CFA computer environment.

Response from the Dean of the College of Fine Arts

The Dean of the College of Fine Arts agrees with this recommendation.

*The CFA Associate Dean for Student Affairs and Technology, working with the CFA IT Policy Committee and in consultation with UNM ITS, will expedite and complete the process of developing comprehensive security practice policies for the College in accordance with Policy 2520, UBP. Draft policies of security practices will be submitted by **July 1, 2008**, for review and approval to the Office of the Director of Information Assurance in ITS, the CFA Dean's Policy Council, and the Dean of Fine Arts.*

ALLEGATIONS OF MUSIC COPYRIGHT VIOLATIONS

Internal Audit reviewed a CSG employee’s University computers to determine whether there was evidence of music copyright violations on the computers. As is standard in this type of situation, Internal Audit visited the CSG's area unannounced. Internal Audit performed a limited review of the employee's University computers. The computers were a Macintosh computer, a personal computer (PC), and a laptop computer. Internal Audit took the laptop for further review.

Internal Audit Department Unrestricted Access to Records

During the visit, the employee did not comply with the requests from the Internal Audit staff not to touch and not to delete files from the employee’s computers. Instead, the employee removed a CD from the PC and placed the CD into a stack of CD’s on the desk, deleted a file from the employees Macintosh and tried to delete additional files. The Internal Audit staff had to request that the employee sit out of reach of the computers.

Section 3. "Dishonest or Fraudulent Activities" Policy 7205, UBP states, "The Internal Audit Department's investigators are to have full and unrestricted access to all necessary records and personnel. All University furniture and contents, including desks, are open to inspection when there is a reasonable suspicion of a dishonest or fraudulent activity which makes such inspection appropriate; there is no assumption of privacy."

The employee’s actions compromised evidence in an Internal Audit investigation. It is unknown what was contained in the files the employee deleted. The employee stated that the employee felt Internal Audit should not view the files.

The employee may be subject to disciplinary action because of the employee's behavior during the visit.

Copyright Violations

Internal Audit found the employee may have violated copyright laws by copying music checked out from the public library.

- Eighty-two songs from CDs checked out from the public library were saved on the PC. The employee removed a CD from the PC and placed the CD into a stack of CDs on the desk. A software program used only for copying CDs was open on the PC. The software had completed copying a CD checked out from a public library. The CD was found in the stack of CDs on the desk.
- Other music was found on both the PC and the Macintosh but Internal Audit could not determine if the employee owned the music.
- One movie, rented from a movie rental store, was found saved on the Macintosh.

- Multiple e-mails from the employee discuss the employee burning music CDs for friends. The employee stated that “burning” discussed in the e-mail means purchasing the music on iTunes.
- Four e-mails dated from June 2006 through December 2006 show the employee checked out from 33 to 180 music CDs or LPs from the library at a time. The employee stated that the employee liked to listen to music.

In an interview with Internal Audit after the surprise visit, the employee stated that the computer had been hacked and every CD the employee listened to in the past few days was copied to the employee’s computer.

Copying music is a violation of copyright laws and University policy. Section 2.1. "Acceptable Computer Use" Policy 2500, UBP states, "Users shall respect all copyrights including software copyrights. Users shall not reproduce copyrighted work without the owner's permission." Violating copyright laws is listed as an example of misuse of computing services in Section 2.2. "Acceptable Computer Use" Policy 2500, UBP.

Federal regulations allow copyright owners to collect either actual damages and profits or statutory damages from the infringer of the copyright. Statutory damages are "not less than $750 or more than $30,000 as the court considers just…" Section 504. United States Copyright Office, *Circular 92: Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code (2003).*

The employee appears to have copied 82 songs and 1 movie. The infringer's statutory damages for 83 violations range from a minimum of $62,250 to a high of $2,400,000. The court may also award attorney's fees per Section 505. United States Copyright Office, *Circular 92: Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code (2003).*

The CFA Administration should have provided more oversight of the activities of the CSG. The CFA should have documented and enforced security practices.

Pornography

Internal Audit confiscated a laptop from the CSG employee’s office. The laptop contained 6 pornographic movies and 530 pornographic pictures. Fifteen percent of the file dates were on workdays during working hours. Internal Audit found the following evidence, which makes it appear that the pornography belonged to the employee.

- The pornography was under a file directory name similar to the directory names found on both the employee’s Macintosh and PC.
- The Senior LAN Administrator told us that file structures are unique to each employee in the department; there is no standard file structure in the department.

- The System Properties state the system is registered to the employee.
- The employee stated that Internal Audit needed the CSG Administrator password to log onto the PC. The administrator password is known only to the CSG and CSG contractors. To access the laptop, Internal Audit used the administrator password shared with a contractor through e-mail.

The employee told us that the pornography was not the employee's. The employee stated the laptop is a CSG computer loaned out to users. The laptop had basic software on it and was stored in an open area accessible to all of the CSG.

The University has not specifically defined whether pornography is allowable on University-owned computer equipment. The University has listed examples of misuse of computing services in Section 2.2. "Acceptable Computer Use" Policy 2500, UBP but pornography is not included in the examples. The University does allow incidental personal use of computing services per Section 2.3. "Acceptable Computer Use" Policy 2500, UBP. The University does not have policies addressing the allowability of viewing and saving pornography using University equipment. This university-wide issue is addressed later in this report.

The employee may have been engaged in questionable activities using University equipment during working hours. The CSG performs a critical function for the CFA. The questionable activities may have taken a significant amount of time away from the employee's work duties. The Associate Dean is working with the Department of Human Resources on potential disciplinary action for the employee.

Recommendation 2

The CFA Dean should ensure that the CFA develops a structure for the CSG that provides more oversight into the activities of the CSG.

Response from the Dean of the College of Fine Arts

The Dean of the College of Fine Arts agrees with this recommendation.

*This recommendation is consistent with the charge, given by the Dean of Fine Arts to the CFA Associate Dean for Student Affairs and Technology in her letter of appointment dated April 5, 2006, to review the structure and operations of the College Computer Support Group. The Associate Dean will work with UNM Human Resources, UNM ITS, the CFA IT Policy Committee, and the CFA Dean's Policy Council to establish a more effective, transparent, and responsible CFA IT support structure with clear lines of reporting authority and management supervision that coordinates CFA IT support with UNM ITS. This new structure will be in place and staffed by **July 1, 2008**.*

Recommendation 3

The CFA Dean should continue to work with Human Resources on potential disciplinary action for the employee's actions during the Internal Audit visit, the apparent copying of music files and the apparent storing of pornography on the University's equipment.

Response from the Dean of the College of Fine Arts

The Dean of the College of Fine Arts agrees with this recommendation.

[redacted].

USING TUITION REMISSION TO PAY FOR CONSULTING

The same CSG employee described above used a tuition remission to pay $1,000 to the Division of Continuing Education and Community Services (Continuing Ed) for consulting services. The CFA needed computer support for their CFAHELP website. The expertise for this website is in Continuing Ed's IT Department. In fiscal year 2006, the CFA and Continuing Ed processed two tuition remission forms for $500 each to pay for the consultation. Both forms were signed by the Associate Dean and the CSG employee. It appears that at least two employees in Continuing Ed worked with the CFA to process these transactions: the Computer Services Manager, and the Program Manager for the Custom Training and Outreach Group.

The tuition remission program is an employee benefit for employee development. It is funded through a small assessment to all University salary accounts. Section 1. "Tuition Remission Program" Policy 3700, UBP states "The Tuition Remission Program is a voluntary opportunity provided by the University for employees to select specific areas for furthering their professional skills. The Tuition Remission Program is designed to help with the cost of education opportunities offered by the University."

When we spoke with the CFA staff, they indicated they saw tuition remission as a way to increase resources available to the CSG.

The CFA and Continuing Ed misused the tuition remission resources. In addition, the CFA signed documents that misrepresented the true nature of the transaction. In effect, they used funds earmarked for employee benefits for their operating expenses.

After Internal Audit brought it to their attention, Continuing Ed reversed the two payments so that the tuition remission is no longer paying for the consultation. Therefore, the CFA still owes Continuing Ed for the consultation. We also addressed this issue in a recent audit report to Continuing Ed.

Recommendation 4

The Dean should instruct the CFA faculty and staff not to process transactions if the document misrepresents the transaction.

Response from the Dean of the College of Fine Arts

The Dean of the College of Fine Arts agrees with this recommendation.

*Three actions will be taken: 1. the Dean of Fine Arts will issue instructions to department chairs, directors, and senior CFA administrators in the Dean's Policy Council; 2. the College Administrator will issue instructions to department administrators and program coordinators in the College; 3. all transactions by CFA administrative units will be submitted for review to the Office of the Dean, even when the Dean of Fine Arts is not required to approve the transaction. These actions will be completed by **November 2, 2007**.*

Recommendation 5

The Dean of the CFA should assure that Continuing Ed is properly paid for the consulting services.

Response from the Dean of the College of Fine Arts

The Dean of the College of Fine Arts agrees with this recommendation.

*The Dean has instructed the College of Fine Arts Administrator to make the appropriate transaction to pay Continuing Education properly for its consulting services. This action will be completed by **November 2, 2007**.*

Recommendation 6

The Dean of CFA should:

- work with Human Resources to determine whether he should discipline the CSG employee for the employee's role in processing documents that misrepresented the transactions, and
- work with the Deputy Provost to determine whether he should discipline the Associate Dean for her role in processing documents that misrepresented the transactions.

Response from the Dean of the College of Fine Arts

The Dean of the College of Fine Arts agrees with this recommendation.

The CSG employee is [redacted] [redacted] [redacted]*; UNM Human Resources is aware of these additional Internal Audit findings and, pending further investigation by HR, would work with the Dean of Fine Arts to undertake further disciplinary action if necessary by* ***July 1, 2008****.*

The Dean of Fine Arts will work with the Deputy Provost to determine whether the Associate Dean for Student Affairs and Technology should be disciplined for her role in processing the documents. This action will be taken by ***November 2, 2007****.*

Recommendation 7

The Dean of Continuing Ed should work with Human Resources to determine whether she should discipline the Program Manager and the Computer Services Manager for their roles in processing the documents that resulted in using tuition remission to pay for consulting.

Response from the Dean of the Division of Continuing Education and Community Services

The Dean of Continuing Education concurs with the recommendation and is currently working with Human Resources and the Associate Dean of Operations to provide appropriate disciplinary action to the Program Manager and the Computer Services Manager. We hope to have this process completed by December 31, 2007.

UNIVERSITY-WIDE INFORMATION TECHNOLOGY

University Security Departmental Standards and Guidelines

The University has not developed departmental standards or guidelines to help the departments develop and enforce security practices. Departments are required to develop security practices in accordance with "Computer Security Controls and Guidelines" Policy 2520, UBP.

The University has not developed the infrastructure to provide university-wide computer standards and guidelines. The Interim Chief Information Officer (CIO) is in the process of hiring an information security officer to oversee the development of computer policies, standards and guidelines.

Without university-wide standards and guidelines, information security may not be adequate or effective enough to assure management that systems are functioning properly. The University may not be in compliance with relevant laws, regulations, and contractual agreements with IT-related provisions.

Recommendation 8

The CIO should:

- Complete the hiring process for the information security officer position, and
- Ensure guidelines and standards are developed to help the departments develop and enforce security practices.

Response from the Interim Chief Information Officer

The Interim CIO agrees with the recommendation.

We are in the final steps of hiring a Director of Information Assurance (grade 17) within the Office of the CIO. The position has been created and advertised, 14 applications were received by the August 30 closing date, and the search committee has identified a pool of five semi-finalists. I expect to identify the final candidate by mid-November and hope to have this person on staff by January 1, 2008, I will have this position staffed by ***July 1, 2008****.*

Once the Director for Information Assurance is on-board, I expect that this person will conduct a thorough review of UNM IT Policies and develop templates for standards and guidelines that can be adopted by departments. The Director of Information Assurance will also institute a review of security practices in departmental IT support groups. A plan for this review will be in place by ***November 1, 2008****.*

University Information Technology Security Investigations

The University has not developed a university-wide information security investigation process. The following policies address information security reporting but do not include all the elements of a comprehensive information security investigation process.

- A new UBP policy 2560, "Information Technology (IT) Governance, dated August 1, 2007, states that violations of IT policies and standards should be reported to the CIO.
- Section 2.3. "Computer Security Controls and Guidelines" Policy 2520, UBP assigns the responsibility of detecting and correcting non-compliance with University computer policies to department heads or designees and directs employees to report non-compliance to the department heads.

The new policy UBP 2560 conflicts with UBP Policy 2520 on where to report misconduct. UBP Policy 2560 states violations should be reported to the CIO while UBP Policy 2520 states non-compliance should be reported to the department heads or designees.

Policy 2520 UBP does not state what to do with non-compliance complaints which are unresolved by the departments, are too complex for the departments to investigate or involve university-wide security issue. Policy 2560 does not address the investigation process at the CIO level.

Responsibility for developing a process for information security investigations should be assigned to the information security officer. The information security officer is responsible for developing security policies and processes for information security investigations.

Without an information security investigation process, the University may not adequately investigate and correct non-compliance. Non-compliance may:

- interfere with the University's ability to ensure information system and data availability, reliability, and integrity, and
- result in the University being non-compliant with relevant laws, regulations, and contractual agreements with IT-related provisions.

Recommendation 9

The CIO should revise University policy to include a comprehensive process to report, investigate, and resolve non-compliance of information security at the departmental, college, and university-wide levels. The policy should define the roles and responsibilities at each level including the responsibilities assigned to the UNM Police. The IT UBP policies 2560 and 2520 should also be revised to be consistent on where violations of University IT policies should be reported and should be revised for overall consistency.

The process should be documented in University policy and include the following at the departmental, college and university-wide level:

- where to report violations,
- who investigates violations,
- who ensures violations are corrected, and
- who enforces disciplinary action.

Response from the Interim Chief Information Officer

The Interim CIO agrees that the procedures for reporting and the subsequent investigation and discipline associated with violations of UNM IT policy are not well defined in the current IT policies.

Once the hiring of a new Director of Information Assurance is completed, the CIO will initiate a review of all policy related to Information Technology (the 25xx policies). This review of policies will result in a prioritized plan for the modification of existing policies and the development of new policies. The review will also include a recommendation for the best place to address the issue of reporting and investigating violations of UNM IT policies. The review of policies will be completed by September of 2008.

PORNOGRAPHY ON UNIVERSITY EQUIPMENT

The University has not specifically defined when or if pornography is allowable on University computer equipment.

The University has a policy that lists employee behaviors that are "proper cause for disciplinary action. Per Section 2.3. "Performance Management" Policy 3215, UBP, "Post-probationary employees may be suspended or discharged only for proper cause." Pornography is not listed as an example of proper cause per Section 5 of the above referenced policy.

Management and employees may not be aware of what constitutes proper cause in regards to pornography, because the University does not have policies addressing the allowability of viewing and saving pornography using University equipment.

Recommendation 10

Human Resources should address the allowability of pornography on University computer equipment in University policy.

Response from the Interim Vice President for Human Resources

The Department of Human Resources concurs with this recommendation. As there are legal issues associated with this, we will work with University Counsel to draft a proposed policy. We anticipate a June 2008 completion date.

CONCLUSION

We found some evidence which indicates the complainant's allegations regarding misuse of computer equipment are valid. CFA is not complying with the University's policies regarding IT management. To comply with the policy, the CFA will need to develop and document their departmental information security practices, communicate them to the CFA staff and faculty, and have a process in place to address information security violations. To help the colleges and departments create written security practices for their operations, the University needs to develop specific standards and guidelines outlining the practices the colleges and departments should put in place.

APPROVALS

G. Christine Chavez

G. Christine Chavez, CPA
Director, Internal Audit Department

Approved for Publication

Chair, Audit Committee