STATE OF NORTH CAROLINA

SPECIAL REVIEW

NORTH CAROLINA CENTRAL UNIVERSITY

INFORMATION TECHNOLOGY SERVICES DEPARTMENT

DURHAM, NORTH CAROLINA

JUNE 2008

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

SPECIAL REVIEW

NORTH CAROLINA CENTRAL UNIVERSITY
INFORMATION TECHNOLOGY SERVICES DEPARTMENT

DURHAM, NORTH CAROLINA

JUNE 2008

STATE OF NORTH CAROLINA
Office of the State Auditor

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet
http://www.ncauditor.net

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Dr. Charlie Nelms, Chancellor, North Carolina Central University
Mr. Jim W. Phillips, Jr., Chair, Board of Governors, The University of North Carolina
Mr. Erskine Bowles, President, The University of North Carolina
Mr. Cressie H. Thigpen, Jr., Chair, Board of Trustees, North Carolina Central University
Members of the North Carolina General Assembly

Ladies and Gentlemen:

Pursuant to North Carolina General Statute § 147-64.6(c)(16), we have completed our special review of North Carolina Central University. The results of our review, along with recommendations for corrective action, are contained in this report.

Copies of this report have been provided to the Governor, the Attorney General, and other appropriate officials in accordance with North Carolina General Statute § 147-64.6(c)(12) which requires the State Auditor to provide written notice of apparent instances of violations of penal statutes or apparent instances of malfeasance, misfeasance, or nonfeasance by an officer or employee.

Respectfully submitted,

Leslie W. Merritt, Jr.

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

June 17, 2008

TABLE OF CONTENTS

PAGE

INTRODUCTION

The Office of the State Auditor was contacted by the University of North Carolina General Administration after they became aware of allegations regarding potential inappropriate use of the North Carolina Central University (University) computer networks. Allegedly, employees within the University's Information Technology Services Department misused the University's networks and computers by downloading copyrighted and pornographic materials. In addition, these employees allegedly circumvented purchasing procedures to acquire items for personal use.

Our special review of these allegations included the following procedures:

- Interviews with current and former employees of North Carolina Central University.
- Examination of relevant documents and records of the University including purchase orders, invoices, fixed asset inventories, personnel files, and financial statements.
- Review of policies and procedures and federal and State regulations including the North Carolina General Statutes and North Carolina Administrative Code.
- Forensic analysis of computer data storage devices and network drives.

This report presents the results of our special review. The review was conducted pursuant to North Carolina General Statute §147-64.6(c)(16) rather than a financial statement audit or review. The Office of the State Auditor also performs a financial statement audit of the University on an annual basis. In addition, the Office of the State Auditor conducts a periodic general controls review of information systems at the University.

[This Page Left Blank Intentionally]

BACKGROUND

North Carolina Central University (University) was established in 1910. Currently, the University enrollment approaches 9,000 students. The University is one of 16 constituent institutions in the University of North Carolina system. The University offers both undergraduate and graduate programs of study. A Board of Trustees oversees its operations at the institutional level. The University's Chancellor and other senior administrators manage the day-to-day operations.

The University provides computer services, Internet resources and telephone services to its students, faculty, staff, and administrators. The Information Technology Services (ITS) Department organizes and administers these efforts. These responsibilities provide academic and research support and assistance for the students and faculty while also providing an internal framework for administrative functions of the University.

The ITS Department is led by a Chief Information Officer (CIO). The CIO reports directly to the Chancellor and is responsible for all technology initiatives on campus. The ITS Department was organized into several functional areas with managers overseeing each section.

[This Page Left Blank Intentionally]

1. UNIVERSITY INFORMATION TECHNOLOGY SERVICES EMPLOYEES MISUSED THE UNIVERSITY NETWORK AND COMPUTERS BY DOWNLOADING MOVIES, MUSIC, GAMES, SOFTWARE, AND PORNOGRAPHY.

Data Base Administrator

Our review of computers and disk drives assigned to and under the control of the Data Base Administrator in the University's Information Technology Services (ITS) Department indicated inappropriate use of University networks and computers. We found numerous files of inappropriate material including "ripped"[1] versions of films, music, software, and video games. In addition, our analysis discovered pornographic materials.

During our interview, the Data Base Administrator admitted inappropriate use of University-issued computers by downloading files from various internet sites. He said that it was strictly for personal use and that he never sold or distributed any of the material except to a few friends.

The Data Base Administrator said he used the University networks because the larger bandwidth provided faster downloads. Using the University network, he would download the items to a University computer, transfer them to a personally-owned external hard drive, and then transfer to his personal computer at home.

During our review, we discovered two volumes[2] present on the University network server under the control of the Data Base Administrator. These volumes contained a number of files containing movies, music and pictures, some of which were pornographic. Also, various types of application software were in the volumes. The Data Base Administrator indicated that these volumes were where he would store data on a temporary basis until he transferred it to his external hard drive.

The Data Base Administrator could not quantify the exact number of movies he had downloaded because he did not keep count. He estimated that he had downloaded approximately 100.

When asked, the Data Base Administrator acknowledged that downloading copyrighted material was illegal. He also said that he downloaded pornographic material on a "semi-regular" basis but knew of no university policy prohibiting that. However, he said that he knew that the State had a policy prohibiting that activity.

The Data Base Administrator said that he learned about the downloading method from a former University ITS employee, who is now employed at another university, who had the reputation while at the University as the "movie guy."

[1] A "ripped" file is one in which encryption that prevents duplication has been removed by a software program.

[2] A "volume" is a fixed amount of storage on a disk or tape, often used interchangeably with "drive."

Information Technology Manager

We also reviewed the computers and disk drives assigned to and under the control of the Information Technology (IT) Manager. This review also indicated inappropriate use of University networks and computers. We found numerous files of inappropriate material including movies, music, software, and video games. In addition, some pornographic images were present on the IT Manager's computer.

In addition, we found decrypting software called AnyDVD[3] on the IT Manager's computer. When we questioned the IT Manager as to why this type of software was needed, he said that he made movies for the Chancellor of events such as inauguration and graduation using a digital camera. After further prodding, the IT Manager admitted that the software was not needed as he had indicated but was used to override copy protection on retail DVD's and to produce "ripped" copies of movies.

We asked the IT Manager if he had knowledge of the Data Base Administrator downloading movies using the University's equipment. He said that he once spoke to the Data Base Administrator about it and told him not to do it. The IT Manager said that he believed that the Data Base Administrator had stopped.

We discussed with the IT Manager the meaning of an e-mail we located on his computer stating that the Data Base Administrator was making downloaded movies available to him. The IT Manager stated that he had only accepted two or three of these type movies one time when he had to spend an evening working and he wanted a movie to watch while there. However, the Data Base Administrator said that he had provided the IT Manager with movies on approximately 20 occasions.

We asked the IT Manager why there were pornographic images on his assigned University laptop computer. The IT Manager answered that if there were any such images it was because he gets items sent to him by individuals who were "spammed" and he has to open the attachment to verify its content. We asked if he visited any pornographic sites while at work and he indicated that he did not. We then asked why we were able to locate 68 hits to a site called "Nudetube.com" originating under his user name. He denied any knowledge of that without giving a plausible explanation.

The Data Base Administrator and IT Manager are responsible for accessing and maintaining various computer networks for the University, including all campus network servers dedicated to specific departments. Their duties include network security and informing other users about inappropriate use. As such, they have an even higher responsibility to protect the University network from unauthorized use.

[3] AnyDVD is a driver allowing decryption of DVD's, as well as targeted removal of copy preventions. AnyDVD is also able to remove copy-prevention from audio CD's.

RECOMMENDATION

The University should take strong disciplinary action against the Data Base Administrator and IT Manager. In addition, the University should review all items for which they had access to determine the extent of their inappropriate use. Further, this review should seek to determine whether the University's computer system and network security were harmed.

2. UNIVERSITY INFORMATION TECHNOLOGY SERVICES EMPLOYEES DISTRIBUTED COPYRIGHTED MATERIALS.

The Data Base Administrator told us he downloaded movies, music, games, and software for personal use. In addition, he admitted that he provided copies of these items to friends and business associates. Further, he acknowledged using software programs to break encryption files used to protect copyrights.

The Data Base Administrator said he had given copies of movies and music to individuals within the Information Technology Services Department at NC Central University. He denied selling any of these materials, instead claiming they were given as free copies. The Data Base Administrator acknowledged that it was "illegal" to obtain and distribute these items.

Federal copyright laws contained in Title 17 of the United States Code prohibit infringement of copyrights and distribution of copyrighted materials. Violators of these copyright laws may be subject to both civil and criminal penalties.

Note: This finding will be referred to the U.S. Attorney's Office, Middle District, the District Attorney for North Carolina Judicial District 14, and the North Carolina State Bureau of Investigation.

RECOMMENDATION

The University should take strong disciplinary action against the Data Base Administrator. The University's copyright administrators should work in conjunction with law enforcement personnel to determine whether federal copyright laws were violated. Further, the University should perform periodic forensic reviews of its data networks to determine whether unauthorized copyrighted materials are being accessed and distributed.

3. THE INFORMATION TECHNOLOGY MANAGER WAS GRANTED UNAUTHORIZED ACCESS TO ANOTHER UNIVERSITY'S SERVER IN ORDER TO DOWNLOAD MUSIC FILES.

While reviewing e-mail messages located on the IT Manager's computer, we located an e-mail dated February 6, 2008 indicating that an employee at North Carolina State University (NC State) "set up a share" that allowed the IT Manager access to the NC State computer network. In a February 20, 2008 e-mail, the NC State employee told the IT Manager “the vendor came in yesterday to install the app on the server you were using and I had to drop the share.” In response, the IT Manager asked the NC State employee to “setup another share” and the NC State employee agreed.

The IT Manager told us that he was vacationing in Atlanta during that time and wanted to download some karaoke files to entertain his children. He said the NC State employee who previously worked at NC Central agreed to grant access to the IT Manager. He said that this access was granted “only that one time.”

The IT manager, whose responsibility at NC Central is to oversee network security, admitted that is was wrong for the NC State employee to grant him access to the NC State network. The IT Manager also said that he had never given similar access to the NC State employee to the NC Central network.

North Carolina General Statute § 14-454.1 outlines unlawful access to government computers as follows:

> *“Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any government computer for any purpose other than those set forth in subsection (a) of this section is guilty of a Class H felony.”*

Note: This finding will be referred to the U.S. Attorney’s Office, Middle District, the District Attorney for North Carolina Judicial District 14, and the North Carolina State Bureau of Investigation.

RECOMMENDATION

The University should take strong disciplinary action against the IT Manager. In addition, the University should provide additional training to all Information Technology Services Department employees that stress the need to ensure network security.

4. THERE EXISTS A LACK OF ADEQUATE CONTROLS OVER ASSETS.

During the course of our review, we became aware that the Information Technology Services Department lacks an adequate system of controls over the purchase and accountability of their assets.

The procedures in place are that any item purchased with a price of greater than $1,000 is tagged by the Fixed Asset Office and that office is required to log where the item is assigned. However, according to the Chief Information Officer (CIO), tracking inventory “is a gap for us.”

The CIO said that an annual inventory is required to be conducted and that the ITS Department receives a list of missing items in order to locate them. The CIO said that they have been able to locate most items in the past. He said that a transfer asset form is required to be completed when an asset is transferred to another user.

Because there were allegations raised as to questionable purchases being made, a complete inventory audit was performed and provided to the Fixed Asset Office. During that audit, equipment costing less than $1,000 was discovered that had been purchased and never authorized. For example, a digital camera and Global Positioning System (GPS) device was located that the CIO indicated that he had not approved. The CIO stated that four large screen HDTV monitors were purchased for the ITS department by his predecessor. These monitors are supposedly used by the managers to "monitor trouble tickets." However, when we reviewed the asset lists that were produced by the Fixed Asset Office, we did not see any TV monitors.

Both the CIO and IT manager said that the CIO signs off on all purchases of small items as well as large items. However, during our interview with the IT Manager, he indicated that he had purchased a camera and GPS device when a vendor contacted him stating that they had "extra money" on a purchase order and asked what was to be done with the money. The IT manager said that he ordered the camera and GPS device with that money. The IT Manager also said that the HDTV monitors had been purchased using "end of the year money."

The IT Manager said that he used the camera to take pictures around campus, broadcast football games, and record the Chancellor's inauguration, all of which are broadcast over the campus networks. The IT manager said that he ordered the GPS device "because he likes toys." The IT manager said that he only used the GPS device once on a trip to Asheville (or Asheboro) in December 2007.

During our interviews with other employees, we learned that there have been a number of smaller equipment purchases made such as Ipods and Blackberry devices with no tracking system in place to determine their current use. Also, we were told that some Macintosh laptop computers were purchased and that Ipod devices were included with the purchase. Four employees of the ITS department received those Ipod devices with no records being kept of their receipt.

During our review, we observed a significant amount of unused equipment present in the server room. These items included Blade servers, switches, laptops and monitors. We were unable to determine the exact purpose or need of this equipment.

RECOMMENDATION

University management should implement policies and procedures to ensure that all equipment purchases are properly approved and tracked as to where the equipment is being used. ITS personnel should work with the Fixed Asset Office to implement procedures to ensure that equipment is properly accounted for.

5. EMPLOYEES ARE NOT REQUIRED TO COMPLETE SECONDARY EMPLOYMENT FORMS.

During the course of our review, we discovered that the IT Manager was part-owner of a business providing network services. The IT Manager said that the business was no longer active but they were continuing to file tax returns in hopes of reviving the business in the future.

We reviewed the personnel file for the IT Manager and there was no indication that a secondary employment disclosure was completed by the IT Manager. During our questioning of the IT Manager, he indicated that he had not completed a secondary employment form related to his secondary business. Also, when we interviewed the CIO, he said that he was unaware of the IT Manager's secondary employment.

The North Carolina State Personnel Manual states:

> *"The employment responsibilities to the State are primary for any employee working full-time; any other employment in which that person chooses to engage is secondary. An employee shall have approval from the agency head before engaging in any secondary employment. The purpose of this approval procedure is to determine that the secondary employment does not have an adverse effect on the primary employment and does not create a conflict of interest."*
>
> *It is the responsibility of the employee:*
>
> - *To complete a Secondary Employment Form for all employment that is not covered by Dual Employment, and*
> - *To update the form annually, as well as to document changes as they occur."*

According to the University Human Resource officials, the University follows the State Personnel policy related to secondary employment and the policy has always been in place but "only in the past couple of years" has the Human Resource division attempted to encourage compliance. The official said that it is the responsibility of each employee to submit and update a secondary employment form and for each department to keep employees informed of the need to do so.

RECOMMENDATION

University management should ensure that all employees have completed a secondary employment form in accordance with State Personnel policies and should annually remind employees of the need to complete the form if there have been any changes.

6. UNIVERSITY OFFICIALS DID NOT PROPERLY VERIFY DEGREES, PRIOR EMPLOYMENT, AND CREDENTIALS WHEN HIRING AND PROMOTING EMPLOYEES.

During our review, we noted that the Data Base Administrator indicated on his initial employment application for the position of Computer Consulting II, that he had obtained a degree in computer science with 108 semester hours of credit from an out of state university. However, during the verification of reference and education process, it was confirmed that the Data Base Administrator had completed only 52 semester hours and did not obtain a degree as he had indicated on his employment application.

During our interview with the Data Base Administrator, he confirmed that he had not completed the degree requirements and was still attending the school online.

Training and Experience requirements for the position stated that: "Graduation from a two-year college or technical school with a degree in data processing and eighteen months of experience in data processing; or graduation from a four-year college or university and eighteen months of experience in data processing; or equivalent combination of training and experience," were required for the position.

We reviewed the personnel file of the Data Base Administrator and noted that no action appeared to have been taken with regard to the discrepancy. Human Resource officials indicated that the Data Base Administrator's employment qualifications were based upon a combination of work experience as well as educational achievement. Also, according to University Human Resource officials, subsequent promotions that the Data Base Administrator received were done so under the new "Career Banding" initiative that emphasizes job skills and experience rather than educational attainment.

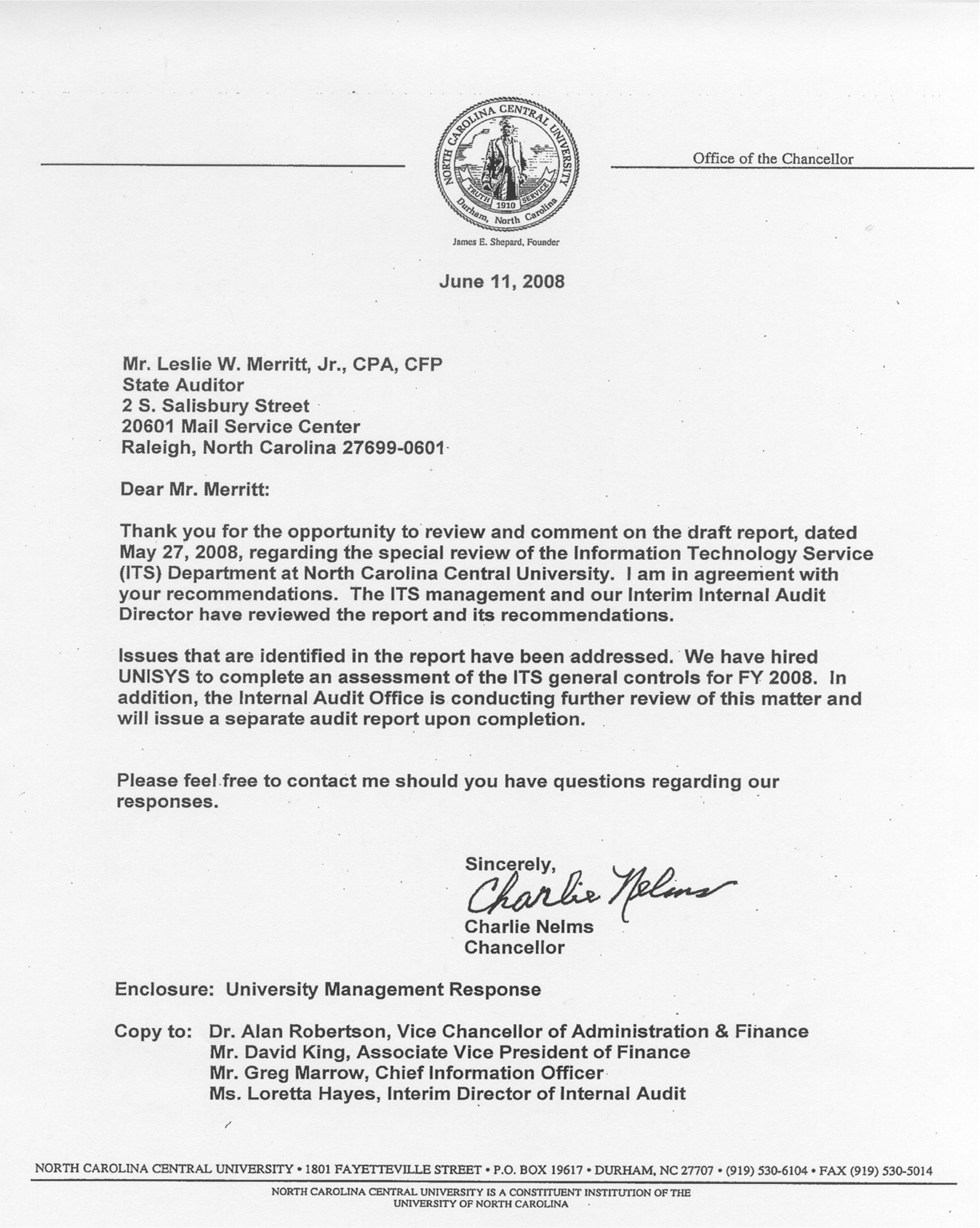
However, we believe that the inclusion of incorrect or false information on an employment application should have raised concerns about the applicant. We saw no evidence that the issue was ever addressed.

RECOMMENDATION

University management should ensure that any discrepancies that are discovered related to a new employee's employment history and educational achievements are noted and addressed. Any actions taken related to the discrepancies (up to and including rescinding the employment offer) should be noted in the employee's personnel file for review in future promotions and/or hiring decisions.

[This Page Left Blank Intentionally]

RESPONSE FROM NORTH CAROLINA CENTRAL UNIVERSITY



Office of the Chancellor

James E. Shepard, Founder

June 11, 2008

Mr. Leslie W. Merritt, Jr., CPA, CFP
State Auditor
2 S. Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Dear Mr. Merritt:

Thank you for the opportunity to review and comment on the draft report, dated May 27, 2008, regarding the special review of the Information Technology Service (ITS) Department at North Carolina Central University. I am in agreement with your recommendations. The ITS management and our Interim Internal Audit Director have reviewed the report and its recommendations.

Issues that are identified in the report have been addressed. We have hired UNISYS to complete an assessment of the ITS general controls for FY 2008. In addition, the Internal Audit Office is conducting further review of this matter and will issue a separate audit report upon completion.

Please feel free to contact me should you have questions regarding our responses.

Sincerely,

Charlie Nelms

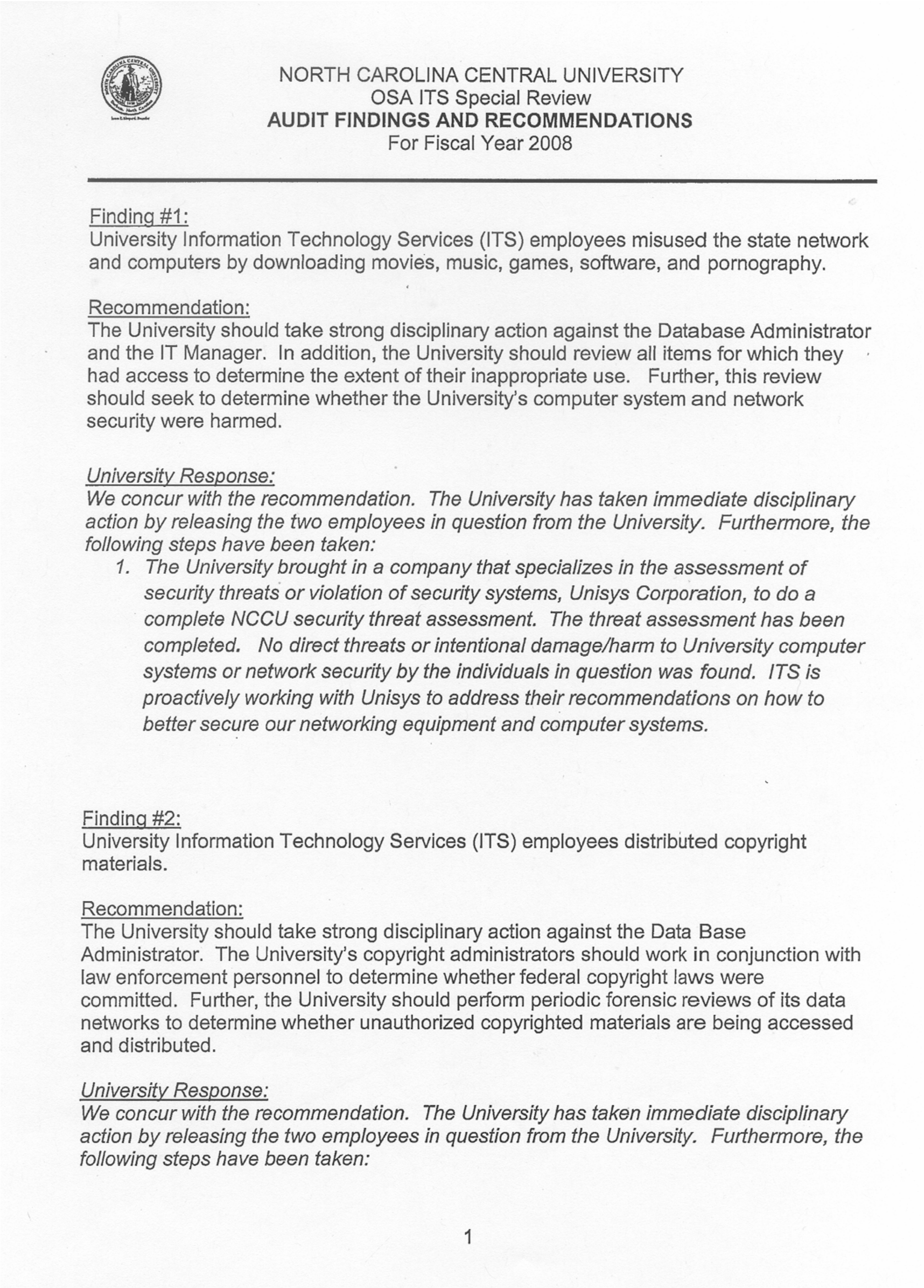
Charlie Nelms
Chancellor

Enclosure: University Management Response

Copy to: Dr. Alan Robertson, Vice Chancellor of Administration & Finance
Mr. David King, Associate Vice President of Finance
Mr. Greg Marrow, Chief Information Officer
Ms. Loretta Hayes, Interim Director of Internal Audit

NORTH CAROLINA CENTRAL UNIVERSITY • 1801 FAYETTEVILLE STREET • P.O. BOX 19617 • DURHAM, NC 27707 • (919) 530-6104 • FAX (919) 530-5014

NORTH CAROLINA CENTRAL UNIVERSITY IS A CONSTITUENT INSTITUTION OF THE
UNIVERSITY OF NORTH CAROLINA



NORTH CAROLINA CENTRAL UNIVERSITY
OSA ITS Special Review
AUDIT FINDINGS AND RECOMMENDATIONS
For Fiscal Year 2008

Finding #1:
University Information Technology Services (ITS) employees misused the state network and computers by downloading movies, music, games, software, and pornography.

Recommendation:
The University should take strong disciplinary action against the Database Administrator and the IT Manager. In addition, the University should review all items for which they had access to determine the extent of their inappropriate use. Further, this review should seek to determine whether the University's computer system and network security were harmed.

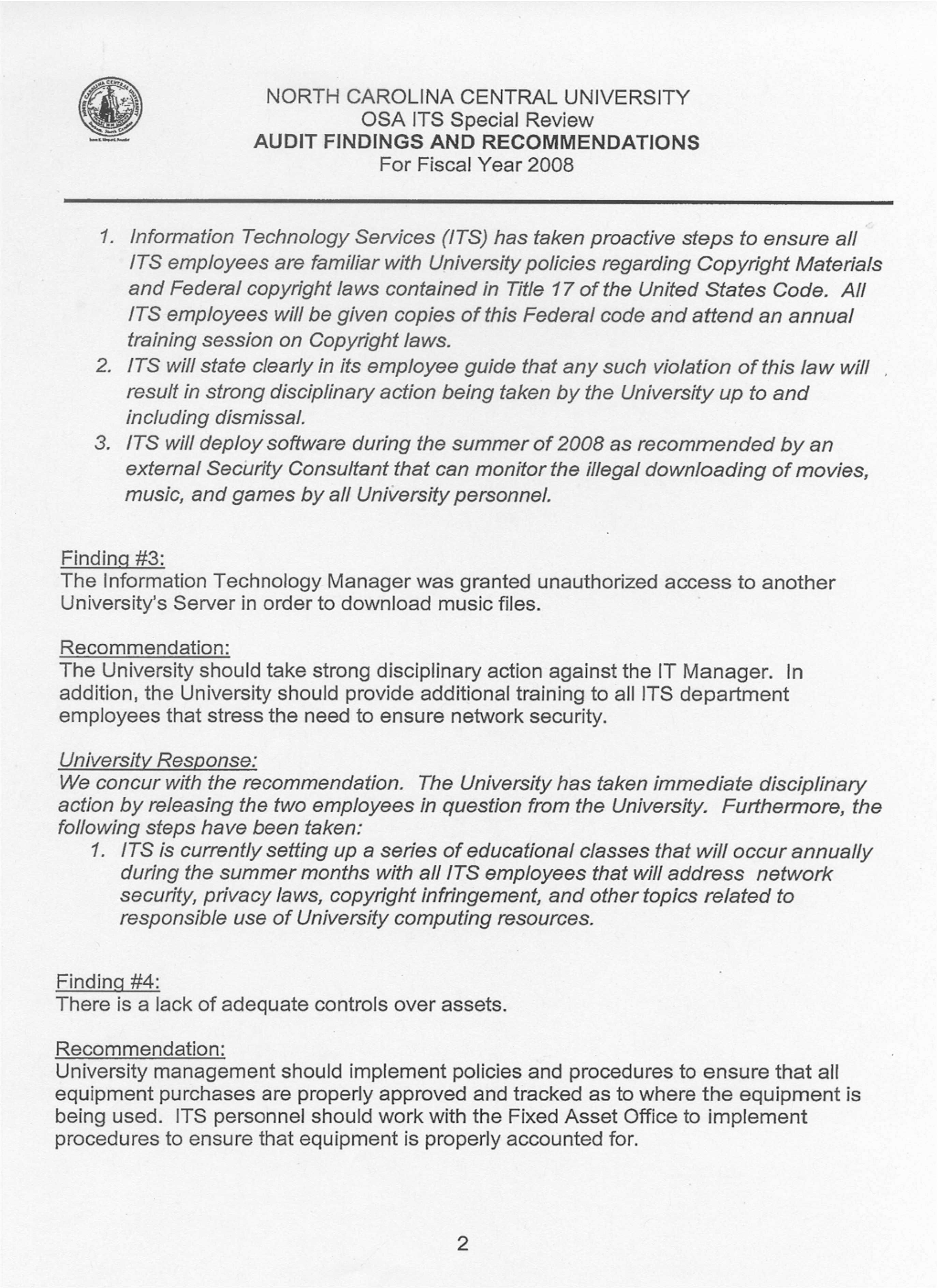
University Response:
We concur with the recommendation. The University has taken immediate disciplinary action by releasing the two employees in question from the University. Furthermore, the following steps have been taken:

1. *The University brought in a company that specializes in the assessment of security threats or violation of security systems, Unisys Corporation, to do a complete NCCU security threat assessment. The threat assessment has been completed. No direct threats or intentional damage/harm to University computer systems or network security by the individuals in question was found. ITS is proactively working with Unisys to address their recommendations on how to better secure our networking equipment and computer systems.*

Finding #2:
University Information Technology Services (ITS) employees distributed copyright materials.

Recommendation:
The University should take strong disciplinary action against the Data Base Administrator. The University's copyright administrators should work in conjunction with law enforcement personnel to determine whether federal copyright laws were committed. Further, the University should perform periodic forensic reviews of its data networks to determine whether unauthorized copyrighted materials are being accessed and distributed.

University Response:
We concur with the recommendation. The University has taken immediate disciplinary action by releasing the two employees in question from the University. Furthermore, the following steps have been taken:



1. *Information Technology Services (ITS) has taken proactive steps to ensure all ITS employees are familiar with University policies regarding Copyright Materials and Federal copyright laws contained in Title 17 of the United States Code. All ITS employees will be given copies of this Federal code and attend an annual training session on Copyright laws.*
2. *ITS will state clearly in its employee guide that any such violation of this law will result in strong disciplinary action being taken by the University up to and including dismissal.*
3. *ITS will deploy software during the summer of 2008 as recommended by an external Security Consultant that can monitor the illegal downloading of movies, music, and games by all University personnel.*

Finding #3:
The Information Technology Manager was granted unauthorized access to another University's Server in order to download music files.

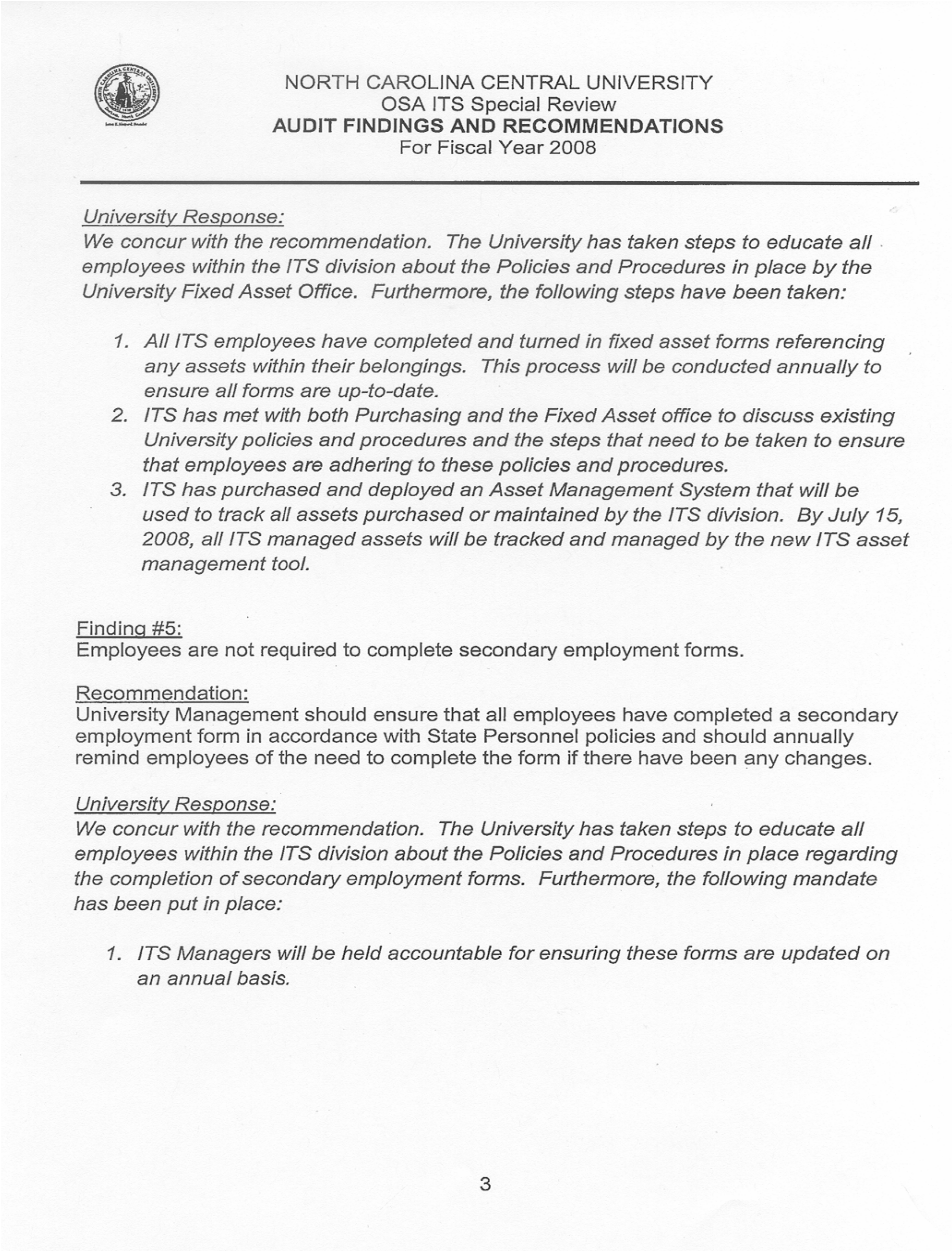
Recommendation:
The University should take strong disciplinary action against the IT Manager. In addition, the University should provide additional training to all ITS department employees that stress the need to ensure network security.

University Response:
We concur with the recommendation. The University has taken immediate disciplinary action by releasing the two employees in question from the University. Furthermore, the following steps have been taken:

1. *ITS is currently setting up a series of educational classes that will occur annually during the summer months with all ITS employees that will address network security, privacy laws, copyright infringement, and other topics related to responsible use of University computing resources.*

Finding #4:
There is a lack of adequate controls over assets.

Recommendation:
University management should implement policies and procedures to ensure that all equipment purchases are properly approved and tracked as to where the equipment is being used. ITS personnel should work with the Fixed Asset Office to implement procedures to ensure that equipment is properly accounted for.



University Response:
We concur with the recommendation. The University has taken steps to educate all employees within the ITS division about the Policies and Procedures in place by the University Fixed Asset Office. Furthermore, the following steps have been taken:

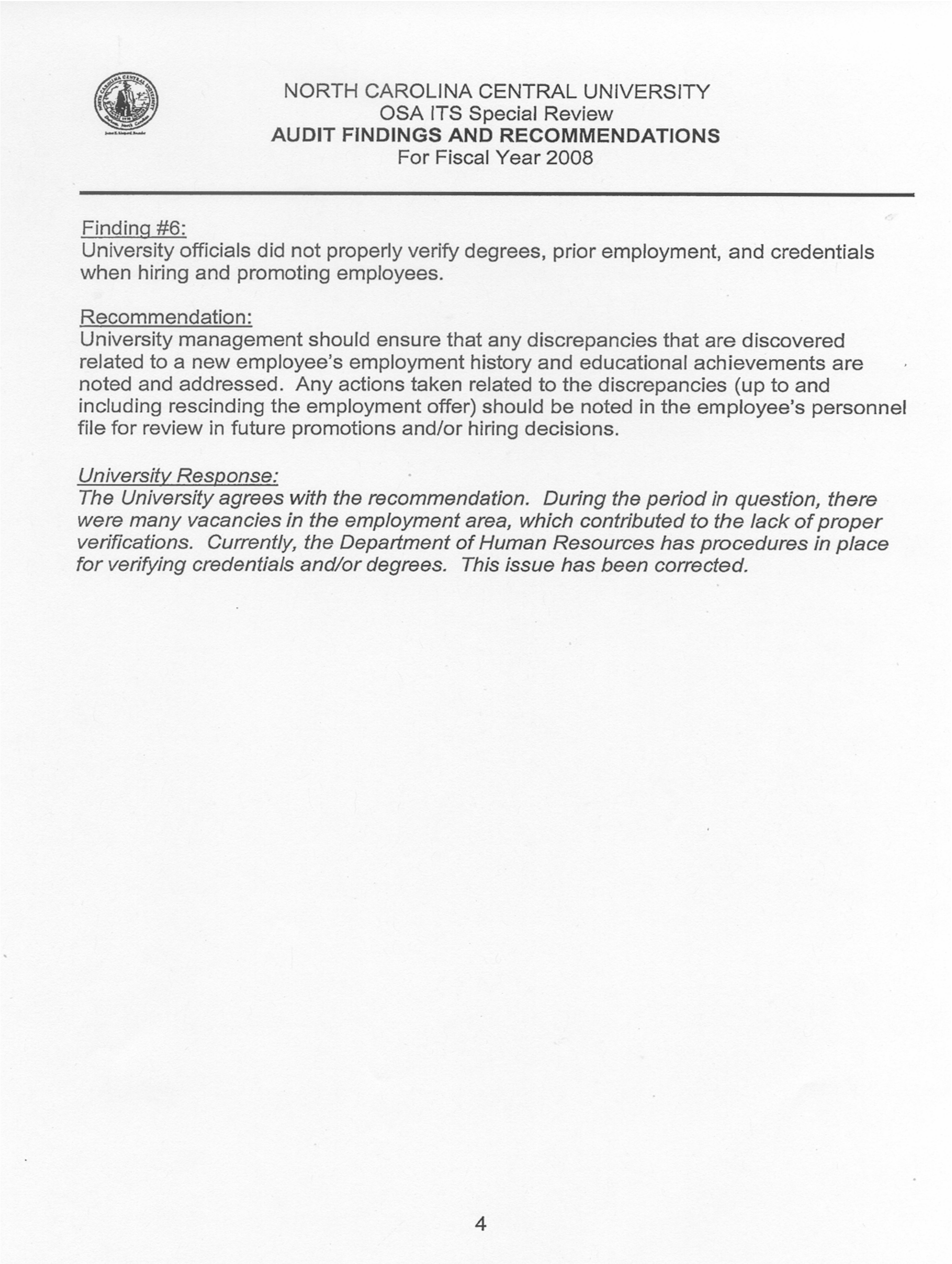
1. *All ITS employees have completed and turned in fixed asset forms referencing any assets within their belongings. This process will be conducted annually to ensure all forms are up-to-date.*
2. *ITS has met with both Purchasing and the Fixed Asset office to discuss existing University policies and procedures and the steps that need to be taken to ensure that employees are adhering to these policies and procedures.*
3. *ITS has purchased and deployed an Asset Management System that will be used to track all assets purchased or maintained by the ITS division. By July 15, 2008, all ITS managed assets will be tracked and managed by the new ITS asset management tool.*

Finding #5:
Employees are not required to complete secondary employment forms.

Recommendation:
University Management should ensure that all employees have completed a secondary employment form in accordance with State Personnel policies and should annually remind employees of the need to complete the form if there have been any changes.

University Response:
We concur with the recommendation. The University has taken steps to educate all employees within the ITS division about the Policies and Procedures in place regarding the completion of secondary employment forms. Furthermore, the following mandate has been put in place:

1. *ITS Managers will be held accountable for ensuring these forms are updated on an annual basis.*



Finding #6:
University officials did not properly verify degrees, prior employment, and credentials when hiring and promoting employees.

Recommendation:
University management should ensure that any discrepancies that are discovered related to a new employee's employment history and educational achievements are noted and addressed. Any actions taken related to the discrepancies (up to and including rescinding the employment offer) should be noted in the employee's personnel file for review in future promotions and/or hiring decisions.

University Response:
The University agrees with the recommendation. During the period in question, there were many vacancies in the employment area, which contributed to the lack of proper verifications. Currently, the Department of Human Resources has procedures in place for verifying credentials and/or degrees. This issue has been corrected.

[This Page Left Blank Intentionally]

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Internet:	http://www.ncauditor.net
Telephone:	919/807-7500
Facsimile:	919/807-7647