STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE UNIVERSITY OF NORTH CAROLINA AT GREENSBORO

GREENSBORO, NORTH CAROLINA

DECEMBER 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE UNIVERSITY OF NORTH CAROLINA AT GREENSBORO

GREENSBORO, NORTH CAROLINA

DECEMBER 2004

STATE OF NORTH CAROLINA
Office of the State Auditor

Ralph Campbell, Jr.
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
Members of the North Carolina General Assembly
The Board of Directors of The University of North Carolina at Greensboro
Dr. Patricia A. Sullivan, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of The University of North Carolina at Greensboro (UNCG). This audit was conducted from October 11, 2004 through November 4, 2004. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate IS general controls at UNCG. The scope of our IS general controls audit included general security, access controls, program maintenance, system development, systems software, physical security, operations procedures, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary and audit results which detail the areas where UNCG has performed satisfactorily relevant to our audit scope, where improvements should be made, and where further study is necessary.

We wish to express our sincere appreciation to the staff of The University of North Carolina at Greensboro for the exceptional courtesy, cooperation and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Ralph Campbell, Jr.

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the University of North Carolina at Greensboro (UNCG) from October 11, 2004 through November 4, 2004. The primary objective of this audit was to evaluate the IS general controls in place during that period. Based on our objective, we report the following conclusions.

General security involves the establishment of a reasonable security program that addresses the general security of information resources. Our audit did not identify any significant weaknesses in general security.

The **access control** environment consists of access control software and information security policies and procedures. We noted several weaknesses in access controls. Due to the sensitive nature of the conditions found in these weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of the North Carolina General Statute 147-64.6(c)(18).

Program maintenance primarily involves enhancements or changes needed to existing systems. We found that modified programs did not receive user approval prior to placement into the production environment. See Audit Finding 1, *Program Changes Without Documented Client Approval* for further information.

Systems software is the collection of programs that drive the computer. The selection of systems software should be properly approved and the software should be maintained by the computer center**.** Our audit did not identify any significant weaknesses in systems software.

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the agency in significant ways. Consequently, the agency should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. There were currently no systems were under development during the period of our audit.

Physical security primarily involves the inspection of the agency's computer center for the controls that should reasonably secure the operations of the computer center from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. Our audit did not identify any significant weaknesses in physical security.

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. The computer operations area did not have an updated operations manual to ensure that operations remain effective. See Finding 2, *The Operations Procedures Manual is Incomplete* for further information.

A complete **disaster recovery** plan that is tested periodically is necessary to enable UNCG to recover from an extended business interruption due to the destruction of the computer center or other university assets. Our audit did not identify any significant weaknesses in disaster recovery.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. IS general control audits are examinations of controls which effect the overall organization and operation of the IS function. This IS audit was designed to ascertain the effectiveness of general controls at the University of North Carolina at Greensboro.

SCOPE

General controls govern the operation and management of computer processing activities. The scope of our IS general controls audit was to review general security issues, access controls, program maintenance, systems software, system development, physical security, operations procedures, and disaster recovery which directly affect the University of North Carolina at Greensboro's computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, toured the computer facility, tested on-line system controls, reviewed appropriate technical literature, reviewed computer generated reports, and used security evaluation software in our audit of information systems. We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

The University of North Carolina at Greensboro (UNCG) was established by legislative enactment on February 18, 1891. The institution opened on October 5, 1892 with a student body of 223 and a faculty of 15. In 1962, the Board of Trustees recommended that the Greensboro campus become coeducational at all levels of instruction in the fall of 1964. Subsequently, by act of the General Assembly in the spring of 1963, the name of the institution was changed to the University of North Carolina at Greensboro. UNCG offers men and women over 150 graduate and undergraduate programs and provides opportunities to apply classroom learning to real life situations through internships.

The Information Technology Department

The Vice Chancellor for Information Technology and Planning reports directly to the Chancellor of UNCG. Information Technology (IT) is a department comprised of four areas under the division of Information Technology and Planning:

- IT-Management Information Systems
- IT-Networks
- IT-Services
- IT-Systems

IT is a service organization whose mission is to plan and provide UNCG with the best computing and technology support possible within the context of institutional priorities and available resources. IT is responsible for university-wide administrative and academic computing as well as campus networking for data and video.

[This Page Left Blank Intentionally]

CURRENT AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where UNCG has performed satisfactorily and where recommendations have been made for improvement.

GENERAL SECURITY ISSUES

General security issues involve the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. The University of North Carolina at Greensboro has established a reasonable security program that addresses the general security of information resources.

ACCESS CONTROLS

The most important information security safeguard that UNCG has is its access controls. The access controls environment consists of access control software and information security policies and procedures. An individual or a group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. During our audit, we noted network architecture controls that strengthen the control environment at the university. However, we also found several weaknesses in access controls. Due to the sensitive nature of the conditions found in the weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

PROGRAM MAINTENANCE

Program maintenance consists of making changes to existing application systems. Programmers should follow program change procedures to ensure that changes are authorized, made according to specifications, properly tested, and thoroughly documented. Application programmers should be restricted to a test environment to ensure that all changes to production resources are tested and approved before moving the changes into production. Changes to application system production programs should be logged and monitored by management.

AUDIT FINDING 1: PROGRAM CHANGES WITHOUT DOCUMENTED CLIENT APPROVAL

UNCG programmers made various changes to critical programs at the request of the Registrar, Human Resources, and Financial divisions. These changes were to ensure correct posting of student payments, calculations in payroll rates, and retirement contribution rates. We could not find evidence of these clients' approval or acceptance of these program changes

Per UNCG policy, a client who requests a change in a file or program must test and document in writing their approval of the program changes. Those approvals must be kept in a permanent file. Since these changes affected calculations in payroll rates, retirement contribution rates, and posting of student payments, client approval is needed to ensure that these program changes are working as intended.

*Recommendation***:** UNCG should ensure that all programmers are aware of university policies regarding obtaining the client's approval in writing for all program changes. In addition, the programmers' supervisors should perform periodic reviews of the permanent files to ensure programmers are retaining written client approval documentation as required by UNCG's policy.

Auditee's Response: A plan with a timetable has been initiated for corrective action.

SYSTEMS SOFTWARE

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. Systems software changes should be properly documented and approved. Our audit did not identify any significant weaknesses in systems software.

SYSTEMS DEVELOPMENT

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the agency in significant ways. Consequently, the agency should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. There were no systems were under development during the period of our audit.

PHYSICAL SECURITY

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes. Physical security controls ensure that the computer service center is reasonably secure from

foreseeable and preventable threats to its physical continuity. Our audit did not identify any significant weaknesses in physical security.

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment.

AUDIT FINDING 2: THE OPERATIONS PROCEDURES MANUAL IS INCOMPLETE

The Operations procedures manual does not contain the necessary components to provide for an orderly and planned execution of job processes.

To ensure that operations are effective, the manual should contain at least the following components:

- Description of processing in narratives and flowcharts.
- Identify required computer inputs and outputs.
- Data entry instructions, if needed.
- Job control language specifications.
- Scheduling requirements.
- Error message listings.
- Restart and recovery instructions.
- Procedures that require operators to record all exception processing.
- Procedures for re-running jobs to ensure the correct input files are used and that subsequent jobs in the sequence are re-run if appropriate.

In addition, the following policies should be defined in the operations procedures manual:

- All production jobs are run by authorized personnel and requested by authorized users.
- Regular production jobs (weekly, monthly) are at least authorized once, when the application is placed into production and that special jobs must have a special request form.
- All production jobs are accounted for through a review of scheduled jobs.
- Exception-processing requests are obtained in writing or electronically approved from application owners to run jobs or programs in another sequence.
- Operators obtain written or electronic approval from owners when scheduling jobs.
- Operators review the exception-processing request log to determine the appropriateness of procedures performed.
- All re-execution of jobs are properly authorized and logged for IS management review.

Without the aforementioned components in the operations procedure manual, operators may not have received proper guidance on handling the operations of the main computer center. Consequently, the scheduling of jobs, processes, and tasks may be handled in an inefficient manner.

Recommendation: UNCG should include the aforementioned components in their operations procedures manual to ensure that the continuous scheduling of jobs, processes, and tasks is organized into the most efficient sequence, maximizing throughput and utilization to meet the operations objectives.

Auditee's Response: A plan with a timetable has been initiated for corrective action.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many university services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center. Our audit did not identify any significant weaknesses in physical security disaster recovery.

DISTRIBUTION OF AUDIT REPORT

In accordance with General Statutes 147-64.5 and 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Powell	State Controller, President
Ms. Molly Corbett Broad	The University of North Carolina, Chancellor
Dr. Patricia A. Sullivan	The University of North Carolina at Greensboro

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore
Senator Marc Basnight, Co-Chair
Senator Charles W. Albertson
Senator Daniel G. Clodfelter
Senator Walter H. Dalton
Senator Charlie S. Dannelly
Senator James Forrester
Senator Linda Garrou
Senator Fletcher L. Hartsell, Jr.
Senator David W. Hoyle
Senator Ellie Kinnaird
Senator Jeanne H. Lucas
Senator Anthony E. Rand
Senator Eric M. Reeves
Senator Robert A. Rucho
Senator R. C. Soles, Jr.
Senator Scott Thomas

Speaker of the House
Representative James B. Black, Co-Chair
Representative Richard T. Morgan, Co-Chair
Representative Martha B. Alexander
Representative Rex L. Baker
Representative Bobby H. Barbee, Sr.
Representative Harold J. Brubaker
Representative Debbie A. Clary
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, III
Representative W. Pete Cunningham
Representative W. Robert Grady
Representative Joe Hackney
Representative Julia C. Howard
Representative Joe L. Kiser
Representative Edd Nye
Representative William C. Owens, Jr.
Representative Wilma M. Sherrill
Representative Thomas E. Wright

Other Legislative Officials

Mr. James D. Johnson	Director, Fiscal Research Division

January 12, 2005

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