STATE OF
NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

APPALACHIAN STATE UNIVERSITY

BOONE, NORTH CAROLINA

AUGUST 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

APPALACHIAN STATE UNIVERSITY

BOONE, NORTH CAROLINA

AUGUST 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 Appalachian State University
Dr. Harvey R. Durham, Interim Chancellor
Dr. Kenneth E. Peacock, Chancellor Elect

Ladies and Gentlemen:

We have completed our information systems (IS) audit of Appalachian State University (ASU). This audit was conducted from April 19, 2004 through May 14, 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 ASU. The scope of our IS general controls audit included general security, access controls, program maintenance, systems software, systems development, 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 ASU 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 Appalachian State University 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

PAGE

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at Appalachian State University (ASU) from April 19, 2004 through May 14, 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. We did not identify any significant weaknesses in general security during our audit.

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 North Carolina G.S. 147-64.6(c)(18).

Program maintenance primarily involves enhancements or changes needed to existing systems. We did not identify any significant weaknesses in program maintenance during our audit.

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**.** We did not identify any significant weaknesses in program maintenance during our audit.

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. Our audit did not identify any significant weaknesses in systems development.

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. We did not note any significant weaknesses in physical security during our audit.

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. We did not note any significant weaknesses in operations procedures during our audit.

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

[This Page Left Blank Intentionally]

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 Appalachian State University.

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, systems development, physical security, operations procedures, and disaster recovery which directly affect ASU'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 application controls. 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.[1]

[1] In 1992 the State created the Information Resource Management Commission to provide statewide coordination of information technology resources planning. The IRMC provides state enterprise IT leadership including increased emphasis and oversight for strategic information technology planning and management; policy development; technical architecture; and project certification. Pursuant to North Carolina General Statute 147-33.78 numerous state officials serve on the IRMC including four members of the Council of State who are appointed by the Governor. The State Auditor had been appointed a member of the IRMC and elected as chair of the IRMC by its members until March 31, 2004.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

Appalachian State University (ASU) is located in the heart of the Blue Ridge Mountains, in Boone, North Carolina. The University was founded in 1899 as Watauga Academy. Over the years, the University evolved into a state teachers' college and then was transformed into a multipurpose regional university. In 1971, ASU became a part of The University of North Carolina.

Information Technology Services (ITS)

ITS is under the leadership of the Chief Information Officer (CIO). The CIO reports to the Senior Associate Vice Chancellor for Academic Affairs. ITS is responsible for all central computing, and is responsible for both academic and administrative networking for the campus.

ITS is comprised of five divisions dedicated to providing networking services, application development and technical support for the benefit of departments, faculty, staff, and students across campus. The five divisions are as follows:

Academic Computing Services
Applications and Web Services
Network Support Services
Systems and Operations
Instructional Computing Services

[This Page Left Blank Intentionally]

CURRENT AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where ASU 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.

ITS and the Internal Audit Department work closely together to determine and manage ASU's level of risk in the area of general security, as well as in other areas. ASU has performed a risk assessment and incorporated the results into the university's security program. We did not identify any significant weaknesses in general security during our audit.

ACCESS CONTROLS

The most important information security safeguard that ASU 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.

We noted network architecture controls that strengthen the control environment at the university. However we noted several weaknesses in access controls that if corrected would further enhance network security. 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.

ASU has written policies and procedures for programmers to follow when they make program changes. After program changes are made, the changes are tested and documented. Our audit did not identify any significant weaknesses in program maintenance.

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.

A complete record of each server and the latest upgrades/changes is maintained by Computer Operations. We did not note any significant weaknesses during our review of 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.

ASU no longer performs any significant in-house systems development. New application systems are purchased from software vendors and the purchases are guided by procedures and standards for the procurement of software products. Our audit did not identify any significant weaknesses in systems development.

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. ASU's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity.

The computer service center is protected from fire by both halon gas and dry water sprinkler systems. It is protected from environmental hazards such as water, heat, and humidity by water alarms in the sub flooring and air conditioning and humidity control systems. The main computer room is protected from electrical power fluctuations and outages by redundant circuits. In addition, ASU has the capability for fail over power distribution from the power company. 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.

ASU uses automated job scheduling software that automatically assigns priorities to jobs based on their parameters. The Production Control Unit reviews the scheduled jobs against a printout of the jobs that were run to ensure there are no exceptions. Computer Operators do not have access to the job scheduler or to the tape library. We did not note any significant weakness in the operations procedures of the computer center during our review.

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.

ASU has a comprehensive disaster recovery plan. ITS in cooperation with the Internal Audit Department tests the disaster recovery plan on a regular basis. ASU has mirrored systems located in a separate building on campus to provide services in the event of a disaster. We did not note any significant weakness in disaster recovery planning during our review.

[This Page Left Blank Intentionally]

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 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
Ms. Molly Corbett Broad	President The University of North Carolina
Dr. Harvey R. Durham	Interim Chancellor Appalachian State University
Dr. Kenneth E. Peacock	Chancellor Elect Appalachian State University

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman
Senator Charlie Albertson
Senator Kever M. Clark
Senator Daniel G. Clodfelter
Senator Walter H. Dalton
Senator James Forrester
Senator Linda Garrou
Senator Wilbur P. Gulley
Senator Kay R. Hagan
Senator David W. Hoyle
Senator Ellie Kinnaird
Senator Jeanne H. Lucas
Senator William N. Martin
Senator Stephen M. Metcalf
Senator Eric M. Reeves
Senator Larry Shaw
Senator R. C. Soles, Jr.
Senator David F. Weinstein

Representative James B. Black, Co-Chairman
Representative Richard T. Morgan, Co-Chairman
Representative Martha B. Alexander
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, III
Representative W. Pete Cunningham
Representative Beverly M. Earle
Representative Stanley H. Fox
Representative R. Phillip Haire
Representative Dewey L. Hill
Representative Maggie Jeffus
Representative Edd Nye
Representative William C. Owens, Jr.
Representative Drew P. Saunders
Representative Wilma M. Sherrill
Representative Joe P. Tolson
Representative Thomas E. Wright
Representative Douglas Y. Yongue

DISTRIBUTION OF AUDIT REPORT (CONCLUDED)

Other Legislative Officials

Senator Anthony E. Rand	Majority Leader of the N. C. Senate
Senator Patrick J. Ballantine	Minority Leader of the N. C. Senate
Representative N. Leo Daughtry	N. C. House of Representatives
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

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

Telephone:	919/807-7500
Facsimile:	919/807-7647
E-Mail:	reports@ncauditor.net

A complete listing of other reports issued by the Office of the North Carolina State Auditor is available for viewing and ordering on our Internet Home Page. To access our information simply enter our URL into the appropriate field in your browser: http://www.osa.state.nc.us