# STATE OF
# NORTH CAROLINA

## AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

## AT

## NORTH CAROLINA STATE UNIVERSITY

## RALEIGH, NORTH CAROLINA

OCTOBER 2002

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

# AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

# AT

# NORTH CAROLINA STATE UNIVERSITY

RALEIGH, NORTH CAROLINA

OCTOBER 2002

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.osa.state.nc.us

## AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of North Carolina State University
Dr. Mary Anne Fox, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of North Carolina State University. 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 North Carolina State University. The scope of our IS general controls audit included general security, access controls, program maintenance, systems software, systems development, physical security, operations procedures, help desk, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary that highlights the areas where North Carolina State University has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at North Carolina State University for the 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 system (IS) audit at North Carolina State University from May 28, 2002 through October 15, 2002. 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 found that all users accessing the University's intranet could view operations staff production job output logs via the web using a web browser, such as Internet Explorer. See Audit Finding 1, *Information Leakage* for further information.

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the North Carolina State University critical operating systems. We 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 G.S. 147-64.6(c)(18). We also found that the firewall violation reports are not reviewed for irregular or unauthorized activity. We considered this weakness to be non-sensitive, but critical. See Audit Finding 2, *Monitoring of Violation Reports* for further information.

**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 systems software during our audit.

**Systems development** includes the creation of new application systems or significant changes to existing systems. We did not identify any significant weaknesses in systems development during our audit.

**Physical security** primarily involves the inspection of the university'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 identify 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 identify any significant weaknesses in operations procedures during our audit.

The **help desk** function ensures that any problem experienced by a computer system user is appropriately resolved. We did not identify any significant weaknesses in the help desk operations during our audit.

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

# 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. This IS audit was designed to ascertain the effectiveness of general controls at North Carolina 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, helpdesk, and disaster recovery which directly affect North Carolina State University 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 has been appointed a member of the IRMC and elected as chair of the IRMC by its members.

[ This Page Left Blank Intentionally ]

## BACKGROUND INFORMATION

North Carolina State University was founded on March 7, 1887 as a land-grant university. Located in Raleigh, it has emerged as a national leader in science, engineering and technology while keeping its roots deep in the North Carolina community through comprehensive extension outreach.

North Carolina State University offers more than 5,200 degrees in over 100 fields of study. Fifty-five research centers, institutes and laboratories support more than 400 faculty, 900 graduate students and 200 undergraduates. The University is made up of the colleges of Agriculture and Life Sciences; Design, Education, and Psychology; Engineering; Natural Resources; Humanities and Social Sciences; Management; Physical and Mathematical Sciences; Textile; and Veterinary Medicine.

The Administrative Computing Services (ACS) provides computer processing for the University. Under the direction of the Associate Vice Chancellor of Resource Management and Information Systems, ACS is responsible for providing general computing support to the administration of the University. The specific responsibilities include database administration, systems support, security administration, network management, application development, and data processing.

[ This Page Left Blank Intentionally ]

# AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where North Carolina State University 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. North Carolina State University has established a reasonable security program that addresses the general security of information resources. However, we identified one significant weakness in general security during our audit.

### *AUDIT FINDING 1: INFORMATION LEAKAGE*

The University has provided information to users of the University intranet that could allow them to view or access information that they are not authorized to access. Using available information from the Intranet, we were able to view financial production job logs via a common web browser, such as Internet Explorer. Providing too much information on websites or other media may create an unnecessary exposure or vulnerability to logical access attacks. Management is responsible for ensuring that users' access to the University's information is adequately restricted based on a need to know, need to use basis.

*Recommendation:* Management should review current information available to users via web browsers and determine if access to such information is appropriate. Management should also ensure that all servers are configured to only provide University information as intended.

*Auditee's Response:* Current information on ACS-maintained websites has been reviewed for appropriate access levels. Production logs referenced above have been password protected and are only accessible by University staff authorized to do so via the NC State University security system (ASAP). ACS-maintained websites will be reviewed on a quarterly basis.

## ACCESS CONTROLS

The access control 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 reviewed the access controls for the North Carolina State University critical operating systems. We found several significant weaknesses in access controls. Due to the sensitive nature of the conditions found in the control 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). We also found one other weakness in access controls that we considered non-sensitive, but critical.

### *AUDIT FINDING 2: MONITORING OF VIOLATION REPORTS*

The firewall violation reports are currently not reviewed or monitored for irregular or unauthorized activity. Firewalls create barriers in order to prevent unauthorized access to a network. It acts as a traffic light, which allows or disallows network traffic to and from the University's networks. Activity, which the firewall interprets as irregular or unauthorized, is recorded in a log daily. These logs also provide valuable information on the types of access attempts that were made to the network. Appropriate personnel should review these logs on a daily basis to detect possible unauthorized intrusions into the University's network. Software is available that will generate exception reports and automate the review process. Intrusions into the University networks could go undetected without the proper monitoring of firewall logs. Management is responsible for assigning resources and implementing written policies and procedures to ensure that monitoring of violation reports is occurring on a frequent basis to prevent unauthorized access to University information.

*Recommendation:* Management should develop written policies and procedures and assign resources to ensure that the review of critical and sensitive violation reports is occurring. Also, consideration should be given to purchasing software that can aid staff in the review of logs for unusual activities.

*Auditee's Response*: Written policies and procedures for monitoring the firewall environment are being developed and will be completed by December 31, 2002. Staff resources have been assigned to monitor the firewall logs and violation reports. Software has been ordered and should be operational in January 31, 2003.

## 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. Our audit did not identify 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. Our audit did not identify significant weaknesses in system 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. Our audit did not identify 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. Our audit did not identify 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. Our audit did not identify significant weaknesses in the operations procedures of the computer center.

## HELP DESK

The help desk function ensures that any problem experienced by the user is appropriately resolved. An effective help desk operations: 1) adequately registers all customer requests, 2) ensures that customer requests, which cannot be resolved immediately, are prioritized and assigned to appropriate personnel for resolution, and 3) ensures that procedures are in place for management to identify and monitor outstanding requests that have not been resolved in a timely manner. Our audit did not identify significant weaknesses in the help desk operations.

## 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 North Carolina State 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 significant weaknesses in the disaster recovery planning.

[ 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<br>The University of North Carolina |
| Dr. Mary Anne Fox | Chancellor<br>North Carolina State University |

## LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman
Senator Charlie Albertson
Senator Frank W. Ballance, Jr.
Senator Charles Carter
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 Howard N. Lee
Senator Jeanne H. Lucas
Senator R. L. Martin
Senator William N. Martin
Senator Stephen M. Metcalf
Senator Fountain Odom
Senator Aaron W. Plyler
Senator Eric M. Reeves
Senator Dan Robinson
Senator Larry Shaw
Senator Robert G. Shaw
Senator R. C. Soles, Jr.
Senator Ed N. Warren
Senator David F. Weinstein
Senator Allen H. Wellons

Representative James B. Black, Co-Chairman
Representative Martha B. Alexander
Representative Flossie Boyd-McIntyre
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, III
Representative W. Pete Cunningham
Representative Beverly M. Earle
Representative Ruth M. Easterling
Representative Stanley H. Fox
Representative R. Phillip Haire
Representative Dewey L. Hill
Representative Mary L. Jarrell
Representative Maggie Jeffus
Representative Edd Nye
Representative Warren C. Oldham
Representative William C. Owens, Jr.
Representative E. David Redwine
Representative R. Eugene Rogers
Representative Drew P. Saunders
Representative Wilma M. Sherrill
Representative Ronald L. Smith
Representative Gregg Thompson
Representative Joe P. Tolson
Representative Russell E. Tucker
Representative Thomas E. Wright
Representative Douglas Y. Yongue

# DISTRIBUTION OF AUDIT REPORT (CONCLUDED)

## Other Legislative Officials

| | |
|---|---|
| Representative Philip A. Baddour, Jr. | Majority Leader of the N.C. House of Representatives |
| 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 | Minority Leader of the N.C. House of Representatives |
| Representative Joe Hackney | N.C. House Speaker Pro-Tem |
| 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

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647