STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS

AT

WINSTON-SALEM STATE UNIVERSITY

WINSTON-SALEM, NORTH CAROLINA

JANUARY 2002

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS

AT

WINSTON-SALEM STATE UNIVERSITY

WINSTON-SALEM, NORTH CAROLINA

JANUARY 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
Board of Trustees, Winston-Salem State University
Dr. Harold L. Martin, Sr., Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the administrative computer operations at Winston-Salem State University (WSSU). 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 the University. The scope of our IS general controls audit included general security issues, access controls, systems development, program maintenance, physical security, operations procedures, system software, telecommunications, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

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

We wish to express our appreciation to the staff at Winston-Salem 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 1

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY 3

BACKGROUND INFORMATION 5

AUDIT RESULTS AND AUDITEE RESPONSES 7

DISTRIBUTION OF AUDIT REPORT 13

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at Winston-Salem State University from October 8, 2001 through October 31, 2001. 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 management has not provided adequate segregation of duties between the Systems Administrator, Operator, and Systems programmer. See Audit Finding 1, *Segregation Of Duties Between Security Administration, Systems Programming and Operations* 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 WSSU mainframe systems by analyzing the built-in security features of the operating system. We found that operating system access controls are not adequate to protect the critical and sensitive information from unauthorized access. See Audit Finding 2, *Adequacy of Access Controls Over the Operating System* for further information. Due to the sensitive nature of the conditions found in the other 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).

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.

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

System 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.

The computer service center's **telecommunication** activities should be operated in a way that protects the security and completeness of data being transmitted. Due to the sensitive nature of the conditions found, 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).

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. The University has disaster recovery plans for the computer center and major user departments. However, we found that back-up tapes were not rotated off- site as intended. See Audit Finding 3, *Rotation of Back-Up Tapes to the Off-Site Location* for further information.

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 Winston-Salem 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, systems development, program maintenance, physical security, operations procedures, systems software, telecommunications, and disaster recovery which directly affect the University's computer operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

This IS audit was performed in accordance with *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. Our methodology included:

- Reviews of policies and procedures.
- Interviews with key administrators and other personnel.
- Examinations of system configurations.
- Tours of the computer facility.
- On-line testing of system controls.
- Reviews of appropriate technical literature.
- Reviews of computer generated reports.
- Use of security evaluation software.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

Founded as Slater Industrial Academy on September 29, 1892, Winston-Salem State University is a public university whose primary mission is to offer high quality educational programs at the baccalaureate level for diverse and motivated students. Master's and intermediate level programs for professional study are also available in the Winston-Salem State University Graduate Center through inter-institutional agreements. While the primary focus is on teaching and learning, the University encourages scholarship and creative relationships with the community in ways, which complement its educational mission.

The mission of **Information Technology Systems** (ITS) is to support and strengthen the academic and administrative needs of faculty, staff and students at Winston-Salem State University. Information Technology Systems serves the faculty, staff and students by facilitating the enhancement of student development and services, teaching and learning, research, outreach and administrative operations through technology. The following are descriptions of the departments comprising WSSU ITS division.

Network and Communication Services

Network and Communications Services provides for the campus infrastructure, which consists of all router, switch, and hub equipment as well as the physical connections between these facilities. This department is also responsible for the video and media services on campus.

Computing and Client Services

Computing and Client Services provides implementation, monitoring and support for all desktop computing systems, server, and client/server applications. Included in this area are help desk operations, webmaster support, applications development, and database management. Special instructional, research and outreach projects that relate to technology are also facilitated via Computing and Client Services.

Administrative Data Center

The purpose of the Administrative Data Center is to support reporting needs of the university, to provide an automated way to collect, store and process the university's data, and provide technical expertise to departments as required.

CITTLE - Center for Innovative Teaching, Technology, Learning and Evaluation

CITTLE provides all faculty members with the opportunity to develop and/or enhance their knowledge and understanding of effective ways of using technology and the principles of teaching and learning to enhance student learning:

The goal of CITTLE is to provide opportunities to enhance the quality of teaching and learning for students and the quality of professional life for faculty through the infusion of technology and good principles of teaching and learning into the curriculum. The center offers a variety of programs to meet the diverse needs of the university community. These

programs are designed to facilitate teaching excellence in all departments for both experienced and novice instructors. Program offerings include workshops on post-secondary teaching and learning, technology support services, information and strategies for testing and evaluation.

Student Information Systems and Outreach

The Office of Student Information Systems serves as the coordinating area for the integrated student records management software programs utilized by the university to maintain all student records. The primary areas with which this office interacts are: Admissions, Billing and Receivables, Financial Aid, Student Records and Residence Life. Other secondary offices include the One Card Office, the Academic Advising Center, the Office of Institutional Effectiveness and Planning, and the Division of General Studies for inclusion of testing scores into the SIS Plus system. The office serves as the liaison between these offices and the Administrative Data Center and other areas of the university that must utilize the present software. The coordinator works with the ITS staff to analyze and help make decisions on future software packages that will interact with each other and to ensure that they are maintained at the highest efficiency level possible.

Video and Classroom Services

The Office of Video and Classroom Services serves as the coordinating area for the distribution and presentation of broadcast video and video support services. This area provides all classroom support services.

The following audit results reflect the areas where Winston-Salem State University (WSSU) 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.

AUDIT FINDING 1: SEGREGATION OF DUTIES BETWEEN SECURITY ADMINISTRATION, SYSTEMS PROGRAMMING AND OPERATIONS

We found inappropriate segregation of duties between Security Administration, Systems Programming and Operation functions. The Application Security Administrator also serves as the 1st Shift Operator, and the Systems Programmer serves as the Systems Security Administrator. The following responsibilities are usually associated with the following positions:

- The Security Administrator is responsible for the following functions; maintaining access rules to data and other IT resources, maintaining security and confidentiality over the issuance, maintenance of authorized user ID and passwords, monitoring security violations and taking corrective actions to ensure that adequate security is provided, periodically reviewing and evaluating the security policy, suggesting necessary changes to management, preparing and monitoring the security awareness program for all employees, and testing the security architecture to evaluate the security strengths and to detect possible threats.

- The Systems Programmer is responsible for maintaining the systems software including the operating system. This function may require unrestricted access to the entire operating system, and thus requires that management closely monitor their activities by requiring the systems programmers to keep logs of their work, and only having access to systems libraries necessary for them to perform their job duties.

- The Operator is responsible for ensuring that the computer runs efficiently and effectively and that the computer peripherals, magnetic media, and the data stored on the media is functioning accurately.

Because the review of logs and the establishment of access standards for both the systems programmer and operators are generally performed by the security administrator, objectivity is lost and monitoring is unreliable if these responsibilities are performed by the same individual.

According to Control Objectives for Information Technology (COBIT), senior management should implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs or positions. In particular, a segregation of duties should be maintained between the system development maintenance function, the processing operations function and the user Organization. In addition, the security responsibility should be clearly separated from the processing operations function.

Recommendation: The University should separate the duties of the security administrator and systems programmer, and the security administrator and Operator.

Auditee's Response: University management has reviewed this situation and the corrective action that we have taken to ensure that this will not occur again is the following:

- The duties of the VMS security administrator and systems programmer, and the Applications security administrator and operator have been separated.
- The first shift Operator duties have been changed to be responsible for all Security Administration (VMS and ZSS).
- The first shift Operator has been given another ID for security administration.
- Purchased Audit software.
- Audit software will protect and inform of unauthorized access to the VMS and ZSS security files and system.
- The Security Administrator now controls VMS security administration.
- The systems programmer duties will not include VMS security Administration duties.
- The duty of bringing up and shutting down of the computers has been removed from operations to the systems programmer.

ACCESS CONTROLS

The access control environment consists of access control software and information security policies and procedures. An individual or 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 WSSU mainframe systems by analyzing the built-in security features of the operating system.

AUDIT FINDING 2: ADEQUACY OF ACCESS CONTROLS OVER OPERATING SYSTEM

Access security controls for the WSSU operating system are not adequate to protect the critical and sensitive information from unauthorized access. We found some users of the system were granted more privileges than necessary to perform their job functions. We also found some accounts of terminated employees still active on the system. Misuse of such privileges could allow these users to access information for which they are not authorized. In an online information technology environment, management should implement procedures that provide access security control based on the individual's demonstrated need to view, add, change or delete data. Access rights for users should be at the minimum level required for them to perform their job responsibilities. Procedures should be in place to periodically review and confirm access rights.

Recommendation: The University should assess the level of access required to the mainframe. Management should ensure that access rights and privileges for users are at the minimum level required for them to perform their job responsibilities. Management should establish procedures to periodically review and confirm access rights and privileges, including inactivating terminated employees' user IDs.

Auditee's Response: University management has reviewed this situation and the corrective action that we have taken to ensure that this will not occur again is the following:

- Privileges have been assessed and adjusted to ensure that the access rights and privileges have been set at the minimum level for personnel to perform their jobs.

- University will conduct periodic review of access control privileges.

We noted other weaknesses in access controls. Due to the sensitive nature of the conditions found, 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).

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 any significant weaknesses in systems development.

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 any significant weaknesses in program maintenance.

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.

The University's 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. Our audit did not identify any significant weaknesses in operations procedures.

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 any significant weaknesses in Systems Software.

TELECOMMUNICATIONS

Telecommunications is the electronic transmission of any kind of information by radio, wire, fiber optics, microwave, laser, or any other electromagnetic system. It can be evaluated along

several lines including the type of system, the geographical organization and the service environment. The computer service center's telecommunications activities should be operated in a way that protects the security and completeness of data being transmitted.

We noted weaknesses in the controls over telecommunications. Due to the sensitive nature of the conditions found, 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).

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 of the 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.

AUDIT FINDING 3: ROTATION OF BACK-UP TAPES TO THE OFF-SITE LOCATION

All back-up production tapes are not rotated to the off-site location as intended. The current practice for off-site storage of backups is to keep some of the backup tapes on-site instead of carrying the tapes to the offsite location as instructed by the disaster recovery manual. This practice may not allow WSSU to recover critical data in the event of a disaster or disruption. According to Control Objectives for Information Technology (COBIT), back-up procedures for information technology related media should include the proper storage of the data files, software and related documentation, both on-site and off-site. Back-ups should be stored securely and the storage sites periodically reviewed for physical access security and security of data files and other items.

Recommendation: The University should survey the current users to determine their requirements and needs for recovery of data files. Based on the user's requirements and needs an appropriate backup and off-site tape rotation schedule should be established. The University should take the appropriate back-ups offsite on a regular basis.

Auditee's Response: University management has reviewed this situation and the corrective action that we have taken to ensure that this will not occur again is the following:

- Assessed users and determined their requirements and needs for recovery of data files.
- All back-up production tapes have been rotated to the off-site location.

[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 C. Broad	President, The University of North Carolina
Dr. Harold L. Martin, Sr.	Chancellor, Winston-Salem State University

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Charlie Albertson	Representative Martha B. Alexander
Senator Frank W. Ballance, Jr.	Representative Flossie Boyd-McIntyre
Senator Charles Carter	Representative E. Nelson Cole
Senator Daniel G. Clodfelter	Representative James W. Crawford, Jr.
Senator Walter H. Dalton	Representative William T. Culpepper, III
Senator James Forrester	Representative W. Pete Cunningham
Senator Linda Garrou	Representative Beverly M. Earle
Senator Wilbur P. Gulley	Representative Ruth M. Easterling
Senator Kay R. Hagan	Representative Stanley H. Fox
Senator David W. Hoyle	Representative R. Phillip Haire
Senator Luther H. Jordan, Jr.	Representative Dewey L. Hill
Senator Ellie Kinnaird	Representative Mary L. Jarrell
Senator Howard N. Lee	Representative Maggie Jeffus
Senator Jeanne H. Lucas	Representative Larry T. Justus
Senator R. L. Martin	Representative Edd Nye
Senator William N. Martin	Representative Warren C. Oldham
Senator Stephen M. Metcalf	Representative William C. Owens, Jr.
Senator Fountain Odom	Representative E. David Redwine
Senator Aaron W. Plyler	Representative R. Eugene Rogers
Senator Eric M. Reeves	Representative Drew P. Saunders
Senator Dan Robinson	Representative Wilma M. Sherrill
Senator Larry Shaw	Representative Ronald L. Smith
Senator Robert G. Shaw	Representative Gregg Thompson
Senator R. C. Soles, Jr.	Representative Joe P. Tolson
Senator Ed N. Warren	Representative Russell E. Tucker
Senator David F. Weinstein	Representative Thomas E. Wright
Senator Allen H. Wellons	Representative Douglas Y. Yongue

Appointees to the Joint Select Committee on Information Technology

Senator Austin M. Allran
Senator Charles Carter
Senator Daniel G. Clodfelter
Senator Eric Miller Reeves
Mr. Dwight Allen
Mr. Curtis Clark
Ms. Darleen Johns
Representative Joe P. Tolson
Representative Russell Edwin Tucker
Representative William L. Wainwright
Representative Trudi Walend
Mr. Rufus Edmisten
Ms. Robin Render
Ms. Janet Smith

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

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**