STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

JOHNSTON COMMUNITY COLLEGE

SEPTEMBER 2007

OFFICE OF THE STATE AUDITOR

LESLIE MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

JOHNSTON COMMUNITY COLLEGE

SEPTEMBER 2007

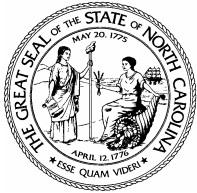# Office of the State Auditor

Leslie Merritt, Jr.,
CPA, CFP
State Auditor

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of Johnston Community College
Dr. Donald L. Reichard, President

Ladies and Gentlemen:

We have completed our audit of Johnston Community College. This audit was conducted during the period from July 5, 2007, through August 13, 2007. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate information systems (IS) general controls at Johnston Community College. The scope of our IS general controls audit included general security, access controls, systems software, physical security, 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 Johnston Community College has performed satisfactorily relevant to our audit scope, where improvements should be made, and where further study is necessary.

We wish to express our appreciation to the staff of Johnston Community College 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,

Leslie W. Merritt, Jr.

Leslie Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

We conducted an Information Systems (IS) audit at the Johnston Community College from July 5, 2007, through August 13, 2007. 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. Johnston Community College has established a reasonable security program that addresses the general security of information resources. We did identify a significant weakness in general security during our audit. *See Audit Finding 1, IT Security Polices and Procedures.*

The **access control** environment consists of access control software and information security policies and procedures. We found 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).

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.*

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 identify any significant weaknesses in physical security during our audit.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable Johnston Community College to recover from an extended business interruption due to the destruction of the computer center or other Johnston Community College assets. Our audit did note a weakness in disaster recovery. *See Audit Finding 2, Resumption of Computer Systems.*

[This Page Left Blank Intentionally]

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the *North Carolina General Statutes* 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 Johnston Community College.

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 software, physical security, and disaster recovery which directly affect Johnston Community College'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 general 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.

[This Page Left Blank Intentionally]

Johnston Community College, located in Smithfield, North Carolina, was founded in 1969. It received its first accreditation from Southern Association of Colleges and Schools on December 13, 1977, to award degrees, certificates, and diplomas. The College offers the Associate in Applied Science, Associate in Arts, Associate in Fine Arts, and Associate in Science degrees. A diploma is awarded for completion on a one-year Applied Technology program. The College awards certificates for completion of other courses of study. As a member of the North Carolina Community College System, it is a public, two-year post-secondary college with an open-door admission policy. Johnston Community College provides comprehensive occupational, general, and continuing education programs, as well as community service activities for Johnston County and surrounding areas. The College opens its doors to the community and seeks to provide for the fullest possible development of the potential of all students in order that they may develop occupational and educational proficiencies in accordance with their interests, talents, and aspirations; and that they may continue their personal growth. To that end, the College, in its programs, services and future plans, strives to reflect the unique demographic, economic, and culturally diverse area it serves.

The Division of Information Technology at Johnston Community College is headed by the Dean of Information Technology, who reports to the President of the College. The Division of Information Technology is charged with supporting student learning, faculty teaching, and College operations through the use of information technology. The division attempts to execute its charge by assisting in the accomplishment of the institutional goals. As part of this attempt to assist the institution in achieving its goals, the Division of Information Technology concentrates its efforts in two areas: continuing to upgrade and improve Johnston Community College infrastructure, and continuing to explore new ways to deliver services to students.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where Johnston Community College 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: IT SECURITY POLICIES AND PROCEDURES

Johnston Community College has not adopted formal information technology (IT) standards to help them address all critical areas of their IT security environment. The following critical policies and procedures were not addressed in their security program:

- Johnston Community College does not monitor its current system configuration against an approved baseline for system security that will assist the college in identifying unauthorized changes to the system. Without a baseline configuration for securing the critical operating system, the operating system may not be secure from commonly known vulnerabilities.

Johnston Community College should assume full responsibility for developing a framework policy, which establishes the organization's overall approach to security and internal control. The policy should comply with overall business objectives and be aimed at decreasing risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration.

Recommendation: Johnston Community College should develop an approved baseline for system security. North Carolina Community College System (NCCCS) is in the process of developing a baseline configuration that is scheduled for completion in July 2007. Johnston Community College should use the completed NCCCS baseline as a guideline for minimum security configurations, and document any differences between the college's baseline and the NCCCS baseline. Johnston Community College should develop procedures to monitor their system configuration against the College's developed baseline settings to detect any unauthorized changes to the system.

Auditee's Response: We concur with this finding. JCC is using the completed NCCCS baseline as a guideline for minimum security configurations and shall document any differences between the College's baseline and the NCCCS baseline. JCC is developing procedures to monitor the system configuration against the College's developed baseline settings to detect any unauthorized changes to the system.

ACCESS CONTROLS

The most important information security safeguard that Johnston Community College has is its access controls. The access controls environment consists of Johnston Community College's 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 a number of 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).

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 system software.*

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 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 weakness in physical security.*

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 College 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 2: RESUMPTION OF COMPUTER SYSTEMS

Johnston Community College has a disaster recovery plan to ensure the resumption of computer systems during adverse circumstances. However, the disaster recovery plan is incomplete. The plan does not include the following critical components:

- Executive management has not signed off on the plan on an annual basis.

- Statement of the assumptions, such as the maximum time without computing, underlying the plan.

In the event of a disaster, the aforementioned components are necessary to ensure the proper recovery of the computer resources. Also, a disaster recovery plan should be tested to ensure that the plan is effective. Management should ensure that a written plan is developed and maintained in accordance with the overall framework for restoring critical information services in the event of a major failure. The disaster recovery plan should minimize the effect of disruptions. Procedures should require that the plan be reviewed and revised annually or when significant changes to the College's operation occur.

Recommendation: Johnston Community College should include a statement of assumptions in the DRP and executive management should approve the plan.

Auditee's Response: We concur with this finding. Processes are under review and being modified to address the issues.

[This Page Left Blank Intentionally]

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at www.ncauditor.net. Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports 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