STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

BRUNSWICK COMMUNITY COLLEGE

DECEMBER 2007

OFFICE OF THE STATE AUDITOR

LESLIE MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

BRUNSWICK COMMUNITY COLLEGE

DECEMBER 2007

STATE OF NORTH CAROLINA
Office of the State Auditor

Leslie Merritt, Jr.,
CPA, CFP
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 Brunswick Community College
Dr. Stephen Greiner, President

Ladies and Gentlemen:

We have completed our audit of Brunswick Community College. This audit was conducted during the period from June 18, 2007, through July 24, 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 Brunswick 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 Brunswick 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 Brunswick 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

PAGE

EXECUTIVE SUMMARY 1

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY 3

BACKGROUND INFORMATION 5

AUDIT RESULTS AND AUDITEE RESPONSES 7

ORDERING INFORMATION 11

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the Brunswick Community College from June 18, 2007, to July 24, 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. Brunswick 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 Policies 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 the physical security.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable Brunswick Community College to recover from an extended business interruption due to the destruction of the computer center or other Brunswick 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 Brunswick 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 Brunswick 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]

BACKGROUND INFORMATION

Brunswick Community College was established by the North Carolina Legislature in July 1979 under the provisions of the General of North Carolina of North Carolina Chapter 115-A passed by the Legislature in 1963. It was chartered as Brunswick Technical Institute. The College was initially accredited by the Commission on Colleges of the Southern Association of Colleges and Schools in 1983 and was reaffirmed for accreditation in 1998. Brunswick Community College is located in the southeastern tip of North Carolina in Brunswick County, midway between Wilmington, North Carolina, and Myrtle Beach, South Carolina, on U.S. 17. The ultimate goal of the College is to provide accessible and affordable programs and services that meet the educational and cultural needs of the community and to provide opportunities for individuals to be successful. Brunswick Community College offers two-year associate degrees in arts, science, and applied science. It also offers certificate and diploma programs.

The Information Services Division at Brunswick Community College has the mission of providing computer services and staff to serve the College's students, faculty, and staff. This Division is headed by the Vice President of Information Services, who reports directly to the President. The function of the Information Services Division is to provide computer technical staff and support services for Brunswick Community College. Its staff provides individual and group software training opportunities. In addition, Information Services staff provides updated, adequate computer lab space to accommodate both instructional and open computer laboratory functions.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where Brunswick 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

Brunswick 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:

- Brunswick 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.

Brunswick 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: Brunswick Community College should develop an approved baseline for system security. North Carolina Community College System (NCCCS) developed a baseline configuration that was completed in July 2007. Brunswick 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. Brunswick 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: Brunswick Community College adopted and successfully installed the Baseline Configuration August 3, 2007 as approved by members of the IIPS organization at the summer conference July 21, 2007. President Stephen Greiner has signed off on this completion and retains a copy of the approved baseline configuration. Copies of the baseline configuration are also held in Brunswick Community College vault, by Vice President of Operations, Director of Information Technology, and by the System Administrator.

ACCESS CONTROLS

The most important information security safeguard that Brunswick Community College has is its access controls. The access controls environment consists of Brunswick 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. *Our audit did not identify any significant weaknesses 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

Brunswick Community College does not have a complete and approved disaster recovery plan to ensure the resumption of computer systems during adverse circumstances. The plan is being developed and is in draft form. Since the disaster recovery plan is incomplete and because the plan is not final, Brunswick Community College has not tested the plan. The plan should include the following critical components:

- Executive management's signature of approval of the plan.
- Statement of the assumptions, such as the maximum time without computing, underlying the plan.
- Identification of critical applications in each user department and the priority in which these applications will be restored if resources are limited.
- Identification of key personnel and their assignments during the restoration of processing.
- Alternate user department procedures to manage their workloads until processing resumes.
- Arrangements to use an alternate computer facility during the reconstruction of the replacement center if needed. This agreement should be written.
- An inventory of equipment, special stock and arrangements to acquire replacement equipment.
- A procedure to update the plan when there are major changes to the environment or at least annually.

In the event of a disaster, the aforementioned components are necessary to ensure the proper recovery of the computer resources. In addition, 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 operations occur.

Recommendation: Brunswick Community College should continue to develop the plan, ensure that aforementioned critical components are included in their plan, and should test the plan at least on a yearly basis. Also, Brunswick Community College should store a copy of the completed plan in an offsite location.

Auditee's Response: Brunswick Community College had to some degree modified a Continuity Plan/Disaster Recovery Plan from Asheville-Buncombe Community College with A-B Tech's approval for use. The plan had only basic changes made at the time the auditor received a copy for the summer audit 2007. Since that time Ronnie Bryant, Director of Information Technology has made major modifications and adapted the plan more to Brunswick Community College's specific needs analysis and detailed information pertaining to equipment, personnel, and contact information.

This plan will remain in constant modification and will be tested twice per year; (1) Winter semester will have a simulation mock test where the components will be tested but systems will not be shutdown; and (2) Summer semester will have a major mock test where a specific major disaster will be declared, systems will be taken offline and employees will be instructed what to do based on the plan. These two (2) mocks will be analyzed and have participation from outside sources such as; (1) Local Fire; (2) County Emergency Management; (3) County Sheriff; and others as designated.

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