STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

MCDOWELL TECHNICAL COMMUNITY COLLEGE

DECEMBER 2007

OFFICE OF THE STATE AUDITOR

LESLIE MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

MCDOWELL TECHNICAL 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 McDowell Technical Community College
Dr. Bryan Wilson, President

Ladies and Gentlemen:

We have completed our audit of McDowell Technical Community College. This audit was conducted during the period from September 20, 2007, through November 2, 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 McDowell Technical 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 McDowell Technical 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 McDowell Technical 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 McDowell Technical Community College from September 20, 2007, through November 2, 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. McDowell Technical 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. *See Audit Finding 2, Physical Security of Computing Facilities.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable McDowell Technical Community College to recover from an extended business interruption due to the destruction of the computer center or other McDowell Technical assets. Our audit did note weaknesses in disaster recovery. *See Audit Finding 3, 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 McDowell Technical 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 McDowell Technical 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

McDowell Technical Community College in Marion, North Carolina, is situated in the foothills of the beautiful Blue Ridge Mountains and is located 32 miles east of Asheville near the intersection of Interstate 40 and NC Highway 226 South.

Established in 1964, McDowell Technical Community College began as the Marion-McDowell Industrial Education Center near downtown Marion and operated as a satellite unit of Asheville-Buncombe Technical Institute until 1967. The College moved to its current 31 acre site in 1970 and was officially chartered in 1971 as McDowell Technical Institute. In 1979, the College's name was changed to McDowell Technical College and in 1988 to the current McDowell Technical Community College. Although the name has changed, the process of lifelong learning has remained as its primary focus.

McDowell Technical Community College is a member of the North Carolina Community College System, dedicated to providing student-centered accessible, high-quality educational opportunities and services which fulfill the personal development, training and employment needs of the residents, businesses, and industries of McDowell County and the surrounding areas through an open-door admissions policy.

The College recognizes each person's right to an education and seeks to contribute to the maximum development of a globally and culturally diverse workforce and improve the quality of life of the individuals in our community.

The College provides life-long learning opportunities by offering comprehensive academic transfer, professional/technical, developmental, basic skills and continuing education programs through traditional and non-traditional delivery methods; providing comprehensive student support services; interacting and assisting with others to encourage, promote and facilitate economic growth and community development; recruiting, retaining and developing a highly qualified and diverse faculty and staff who are dedicated to quality education and service to the College and the community; enhancing student life by sponsoring a variety of educational, cultural, and community services and activities.

The IT division is referred to as the Technology Department. A systems administrator, who reports to the President of the College, heads the department. The mission of the Technology Department is to provide an effective, efficient, and high quality service, which meets the management and administrative needs of the College and to support the College's strategic goals and objectives. The functions of the Technology Department is to provided and maintain hardware and software for support of the instructional program and for reliable and effective data processing and network/communications services for all areas of the College.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where McDowell Technical 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

McDowell Technical 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:

- McDowell Technical 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.

McDowell Technical 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: McDowell Technical 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. McDowell Technical 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. McDowell Technical 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: McDowell Technical Community College will implement the newly developed North Carolina Community College systems security baseline.

ACCESS CONTROLS

The most important information security safeguard that McDowell Technical Community College has is its access controls. The access controls environment consists of McDowell Technical 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 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).

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.

AUDIT FINDING 2: PHYSICAL SECURITY OF COMPUTER FACILITIES

The computer room is not reasonably secure from foreseeable and preventable threats to its physical continuity. We found the following physical security weaknesses:

- Access to the offsite storage area and the computer area are not restricted to authorized personnel. As a result, the physical security over McDowell Technical Community College computing resources is weakened and could allow unauthorized tampering of the data and unauthorized access to computer hardware. Because the critical operating system, which hosts the financial and student information, resides in this computer room, unauthorized personnel could directly access the main console and modify, delete, and corrupt data, or interrupt McDowell Technical Community College's computer processing capabilities.

- Fire extinguishers in the compter room are not inspected annually. All fire extinguishers are to be inspected annually.

Appropriate physical security and access control measures should be established for computer processing facilities in conformance with the general security policy. Access should be restricted to individuals who have been authorized to gain such access. Management should also assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g. fire, dust, power, excessive heat and humidity).

Recommendation: McDowell Technical Community College should develop procedures to ensure that the computer room is always secure from unauthorized personnel, and ensure that the computer room is secure from known environmental hazards, such as water leaks, fire, electrical fluctuations etc.

Auditee's Response: McDowell Technical Community College will develop procedures to ensure that only authorized personnel have access to the computer room. All efforts will be made to insure that environmental hazards are addressed as funding allows.

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 3: RESUMPTION OF COMPUTER SYSTEMS

McDowell Technical 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:

- Alternate user department procedures to manage their workloads until processing resumes;
- Also, a test of the Disaster Recovery has not been performed on a yearly basis; and
- The plan is not located in an offsite storage location.

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: McDowell Technical Community College should include all the aforementioned critical components in its plan and should test the plan at least on a yearly basis.

Auditee's Response: McDowell Technical Community College will include all the aforementioned components in its plan and will try to test the plan at least on a yearly basis.

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