STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

PIEDMONT COMMUNITY COLLEGE

JULY 2007

OFFICE OF THE STATE AUDITOR

LESLIE MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

PIEDMONT COMMUNITY COLLEGE

JULY 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 Piedmont Community College
Dr. H. James Owen, President

Ladies and Gentlemen:

We have completed our audit of Piedmont Community College (PCC). This audit was conducted during the period from May 4, 2007, through May 31, 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 PCC. 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 PCC 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 PCC 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

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the Piedmont Community College (PCC) from May 4, 2007, through May 31, 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. PCC 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 found a significant weakness in systems software during our audit. Due to the sensitive nature of the condition found in this weakness, we have conveyed this finding to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).

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 weaknesses in the physical security.

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

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 PCC'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

Piedmont Community College is a public two-year institution that provides diverse educational opportunities in a learner-centered environment. Piedmont Community College, located in Roxboro, North Carolina was founded in 1970. The Southern Association of Colleges and Schools accredits Piedmont Community College to award Adult Basic Skills (GED), Associate Degree Programs, Diploma, and Certificate Programs. The College offers both curriculum classes and continuing education classes. The mission of Piedmont Community College is to serve the citizens of Person and Caswell Counties by improving quality of life and acting as a catalyst for economic development.

The IT division at Piedmont Community College is referred to as the Administrative Computing Services division of the College. The Director of Management Information Services, who is responsible for the entire computing of Piedmont Community College, heads the Administrative Computing Services division. This position reports to the Vice President of Administrative Services. The mission of the Administrative Computing Services division is to insure the integrity of the administrative systems and infrastructure. The function of the Administrative Computing Services division is to provide installation, upgrade and support services for the administrative systems of the College and to develop, maintain, and upgrade the College information infrastructure in support of expanding technology goals.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where PCC 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

Piedmont Community College (PCC) 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:

- PCC 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.

PCC 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: Piedmont 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. PCC 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. PCC 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: This finding will be addressed at the July 2007 IIPS meeting where the IIPS organization and the NCCCSO will ratify the developed baseline configuration. PCC will conform to the NCCCSO baseline configurations and document differences. There are several open source monitoring tools which are being evaluated. PCC will install the most appropriate one after evaluation.

ACCESS CONTROLS

The most important information security safeguard that PCC has is its access controls. The access controls environment consists of PCC'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 identify a significant weakness in system software. Due to the sensitive nature of the condition found in the weakness, we have conveyed this finding to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).

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. PCC'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 a 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

Piedmont 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 is missing the following components:

- Executive management's signature of approval of the plan.
- Identification of key personnel and their assignments during the restoration of processing.
- Alternate user department procedures to manage their workloads until processing resumes.

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

Auditee's Response: PCC as an institution is in the process of developing and approving a College wide disaster recovery and business continuity plan which will include all departments and divisions. This process includes the PCC MIS department. The completion date for this process is December 2007. MIS will insure that key personnel are listed in the plan and annual testing of the college wide disaster recovery and business continuity plan is included.

[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