OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Sullivan County Community College

Information Technology

Report of Examination

Period Covered:

September 1, 2015 – February 27, 2017

2017M-123

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

October 2017

Dear Community College Officials:

A top priority of the Office of the State Comptroller is to help community college officials manage their college resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support college operations. The Comptroller oversees the fiscal affairs of community colleges statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and Board of Trustee governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard community college assets.

Following is a report of our audit of Sullivan County Community College, entitled Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law.

This audit's results and recommendations are resources for community college officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The Sullivan County Community College (College) is sponsored by Sullivan County and operates a main campus. The College is part of the State University of New York system and is governed by a 10-member Board of Trustees (Board) composed of a student trustee and nine appointed members. The Board is responsible for the general management and control of College financial and educational affairs. The President of the College (President) is the chief executive officer, and the Controller is the chief fiscal officer. The President and Comptroller are responsible, along with other administrative staff, for the College's day-to-day management under the Board's direction.

College officials, including the President, Vice President for Planning, Human Resources and Facilities and Director of Information Technology (IT Director), are responsible for the general management and control of the College's information technology (IT) assets and safeguarding those assets. The IT Director is responsible for overseeing the College's daily IT operations and functions, including supervising IT department staff. The College has approximately 600 computers and one server room. The College's financial and student information system (FSIS) software application contains personal, private and sensitive information (PPSI) of employees and students.

The 2016-17 budgeted IT appropriations were approximately $664,000.

Objective

The objective of our audit was to examine IT controls. Our audit addressed the following related question:

- Did College officials safeguard PPSI on College websites, applications and servers?

Scope and Methodology

We examined the College's IT controls for the period September 1, 2015 through February 27, 2017. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to College officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report. Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning

the value and/or size of the relevant population and the sample selected for examination.

Comments of College Officials and Corrective Action

The results of our audit and recommendations have been discussed with College officials, and their comments, which appear in Appendix A, have been considered in preparing this report. College officials agreed with our recommendations and indicated they planned to initiate corrective action.

College officials have the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage College officials to make this plan available for public review in the Secretary's office.

Information Technology

Computerized data is a valuable resource that College officials rely on to make financial decisions and report to State agencies. College officials are responsible for limiting access to their information systems and PPSI. If the computers on which this data is stored fail, or the data is lost or altered, either intentionally or unintentionally, the results could range from inconvenient to catastrophic. Even small disruptions can require extensive time, effort and expense to evaluate and repair. College officials are responsible for establishing policies and procedures to protect the College's computer equipment and data against the risk of loss, misuse or improper disclosure of sensitive data. These policies and procedures should address crucial security areas such as breach notifications and disaster recovery.

College officials need to improve safeguards over PPSI on College websites, applications and servers and ensure the data stored is adequately secured and protected against unauthorized use, access and loss. While College officials have taken steps to safeguard computerized data, we found unnecessary user accounts that were not disabled or removed and inadequate protection of server room equipment. Furthermore, the Board did not establish policies and procedures regarding breach notifications and disaster recovery plans. As a result, there is an increased risk that computerized equipment and data could be subject to unauthorized access and potential loss.

User Accounts

Employees and students rely on College officials to ensure that their PPSI is properly safeguarded. The IT department is responsible for protecting and preventing improper access to this information. To fulfill these responsibilities, the IT Director and department staff should ensure that unused user accounts are removed when access is no longer needed. To guide these efforts, officials should develop comprehensive written procedures for managing access and reviewing audit logs. Unnecessary accounts and permissions increase the risk of unauthorized access and potentially harmful modification, use or exposure of PPSI.

To minimize the risk of unauthorized access, user accounts should be limited to those students actively enrolled or employees who currently need access to one or more functions to perform their job duties. Access should be terminated promptly when a student is no longer enrolled or an employee leaves College employment or no longer needs access to perform their job duties, limiting the risk that PPSI will be exposed to unauthorized use or modification.

Access to PPSI on College websites, applications and servers is managed using network user accounts. We reviewed approximately 6,800 network user accounts for unnecessary and inactive accounts and found that 4,279 accounts (63 percent) have not been used to log onto the network in at least six months. Of these, 1,725 have never been used to log on. Another 58 were last used to log on between 2006 and 2012 (up to 11 years before we completed our audit test).

While 4,120 accounts are necessary student accounts and officials indicated that another 55 are necessary for current College employees and outside vendors, the remaining 104 are no longer needed and should be disabled or removed. Officials indicated that they would disable these user accounts as a result of our audit.

Access to PPSI in the FSIS is managed using FSIS user accounts. We reviewed approximately 21,000 accounts to determine whether there were any unnecessary or inactive accounts. We found that 14,822 accounts (71 percent) were never used to log on to College systems. Of those, 2,940 (20 percent) were candidate accounts[1] and 11,363 (77 percent) were student accounts. Another 3,779 accounts (18 percent) were not used to log on to College systems for at least six months. For accounts that were used to log on to College systems, the average elapsed time from the most recent log on to the date of our testing was 1.2 years, and the oldest log on date was almost 4 years ago.

The IT department had written guidelines for creating user accounts. However, these guidelines did not cover review of account activity and necessity or contain any other review procedures for removing inactive and unnecessary accounts.

Any user account on a network is a potential entry point for attackers, which increases the risk for unauthorized access to PPSI. Of particular risk are user accounts of former employees because these accounts could potentially be used for malicious activities. Further, unnecessary accounts require additional work to manage access, and the College has a greater risk that users could be inadvertently granted more access than needed to perform their jobs.

Physical Security

Effective physical security of server rooms includes both restricting access to IT system components and disaster prevention and recovery. Unrestricted access to the server that is not controlled or monitored, or the unmitigated effects of natural disasters or similar harsh conditions, leave the College's data and equipment vulnerable to

[1] An account created for any prospective College student, which allows the candidate to access various online forms and other web-based applications for the purposes of enrollment.

significant and potentially costly damage or loss. Accordingly, College officials should take measures to manage server room functionality, including controlling unrestricted access, controlling and monitoring temperature and humidity and installing fire suppression systems and equipment.

While server room access was secure and there was access to an uninterrupted power supply, the environmental factors that could affect server functionality, including temperature, humidity and fire suppression were inadequate. More specifically, the server room lacked fire suppression equipment and equipment to monitor and maintain proper temperature and humidity levels.

The server room's current location was not designed to function as a server room and does not contain the necessary infrastructure for environmental controls. College officials are aware of this and have taken some measures to control temperature using portable air conditioning units and provide fire suppression equipment near to (but outside) the room. Without proper environmental controls, a disaster affecting the servers could significantly disrupt College operations.

Breach Notification Policy

An individual's PPSI could be severely affected if the College's computer security is breached or data is improperly disclosed. New York State Technology Law requires the College to establish an information breach notification policy. Such a policy should detail how the College would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization. It is important for the disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore data system integrity.

College officials were not aware they needed a breach notification policy. By failing to adopt an information breach notification policy, in the event that private information is compromised, College officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals.

Disaster Recovery Plan

It is essential that College officials develop a formal disaster recovery plan that addresses the range of threats to its computerized system. The plan should focus on sustaining the College's critical business functions during and after service disruption. It is important that College officials analyze data and operations to determine which are the most critical and the resources needed to recover and support operations in the event of an emergency. Once the disaster recovery plan is finalized, College officials should distribute it to all

responsible parties, periodically test procedures to make sure they work as intended and update the plan as needed.

College officials were unaware of a need to develop a formal disaster recovery plan to address potential disasters. While officials created an emergency operations plan, this plan lacks detail and has not been tested or distributed to all responsible parties. Consequently in the event of a disaster, College personnel have no guidelines to minimize or prevent the loss of equipment and data or appropriately recover data. Without a disaster recovery plan, the College could lose important financial data and suffer a serious interruption to College operations, such as being unable to process checks to pay vendors or employees.

Recommendations

College officials should:

1. Create, adopt and implement written policies and procedures for:

    - The review and removal of inactive and unnecessary user accounts
    - Breach notification
    - Disaster recovery testing and updating.

2. Implement environmental controls to mitigate the risk of damage to servers, or consider other options for the server room's location that would provide a more appropriate environment.

3. Create a comprehensive disaster recovery plan.

APPENDIX A

RESPONSE FROM COLLEGE OFFICIALS

The College officials' response to this audit can be found on the following page.

SULLIVAN
COUNTY COMMUNITY COLLEGE
S · U · N · Y

112 College Road
Loch Sheldrake,
New York 12759-5151
845-434-5750
Fax: 845-434-4806

October 12, 2017

Mr. Gabriel F. Deyo
Deputy Comptroller
Office if the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor
Albany, NY 12236

Unit Name: Sullivan County Community College
Audit Report Title: Sullivan County Community College Information Technology Report of Examination
Audit Report Number: 2017M-123

This letter constitutes Sullivan County Community College's institutional response to the public audit of the college's information technology.

The campus community thanks the visiting team for their work on our behalf. The report accurately describes the conditions of SUNY Sullivan's information technology, and reflects the interviews and activities in which the team engaged while on campus. The College agrees with the recommendations. The College will submit a separate Corrective Action Plan (CAP).

Sincerely,

Jay Quaintance
President

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed College officials and employees and reviewed College policies and procedures to gain an understanding of the College's IT structure and governance and the policies and procedures over PPSI.

- We provided an Active Directory audit script to College IT personnel to run on one domain controller. We analyzed each report generated by the script to identify network user accounts with ineffective IT controls.

- We obtained computerized data from the IT department to determine the number of user accounts in the FSIS and whether these accounts were active and necessary.

- We observed the server room's physical security.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313