THOMAS P. DiNAPOLI
COMPTROLLER

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER
110 STATE STREET
ALBANY, NEW YORK 12236

GABRIEL F DEYO
DEPUTY COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY
Tel: (518) 474-4037 Fax: (518) 486-6479

September 2015

Anne Kress, President
Members of the Board of Trustees
Monroe Community College
1000 East Henrietta Road
Rochester, NY 14623

Report Number: P2-15-11

Dear President Kress and Members of the Board of Trustees:

A top priority of the Office of the State Comptroller is to help officials manage their resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support operations. The Comptroller oversees the fiscal affairs of local governments 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 governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard assets.

In accordance with these goals, we conducted an audit of three community colleges in western New York State. The objectives of our audit were to determine whether college officials are effectively and efficiently managing software licenses and whether security vulnerabilities exist in college websites, web applications or supporting servers. We included the Monroe Community College (College) in this audit. Within the scope of this audit, we examined the policies and procedures of the College related to information technology (IT), reviewed selected computers for installed software and performed web vulnerability testing for the period September 1, 2013 through March 31, 2015. Because of the sensitivity of some of this information, we did not discuss certain results in this letter, but instead communicated them confidentially to College officials. 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 report of examination letter contains our findings and recommendations specific to the College. We discussed the findings and recommendations with College officials and considered their comments in preparing this report. The College's response is attached to this report in Appendix A. College officials generally agreed with our recommendations and indicated they planned to initiate corrective action. At the completion of our audit of the three Colleges, we prepared a global report that summarizes the significant issues we identified at all of the Colleges audited.

Summary of Findings

We found that College officials and IT staff can more effectively and efficiently manage software licenses. The Board of Trustees (Board) has not adopted an adequate acceptable use policy. The policy does not detail practices for enforcement, such as monitoring computer[1] use and reviewing installed software. Additionally, users are not required to read and provide written acknowledgment that they will comply with the policy terms. The College provides all faculty and staff users with administrative rights, providing the ability for these users to download and install software without prior approval. We also found that College IT staff do not maintain a comprehensive inventory list of all software that the College currently owns and the total number of licenses for each software. The IT staff rely on individual departments to maintain this information; however, we found that the departments could not provide supporting documentation for two software programs installed on College computers. In addition, IT staff do not regularly monitor or review computers to ensure that all software installed is appropriate and legally obtained. Our detailed review of 36 computers identified four that contained gaming or couponing related software, as well as a virus. The installation of inappropriate or unlicensed software may be exposing College computers and networks to unnecessary risk, such as hacking or other malicious events.

Background and Methodology

The College is sponsored by and located in Monroe County. The College operates a main campus (Brighton Campus), four satellite campuses (Damon City Campus, Applied Technologies Center, Economic and Workforce Development Center and the Public Safety Training Center) and two extension centers (Greece Odyssey Academy and Webster Extension Center). The College is part of the State University of New York system and is governed by a 10-member Board which consists of nine appointed members and a student trustee. The Board is responsible for the general management and control of the College's financial and educational affairs. The President of the College is the College's chief executive officer and the Vice President of Administrative Services is the College's chief fiscal officer. Under the direction of the Board, these individuals are responsible, along with other administrative staff, for the day-to-day management of the College.

The College has an IT department headed by the chief information officer (CIO). The CIO is responsible for overseeing the College's daily IT operations and functions, including supervising IT department staff. The College's IT department has two divisions: Communications and Network Services and Computing and Information Technology Services. A Director or Associate Dean has been appointed to assist in the oversight of daily operations of each of these divisions. Between all campuses, the College has approximately 4,000 computers. Budgeted appropriations for IT for the 2014-15 fiscal year were approximately $8.9 million.

Software assets have become increasingly important to organizations. Not only are they a vital element of IT services that enable business-critical processes, but they also represent a large proportion of IT costs. Organizations also risk potential fines and penalties for using software

[1] The term computer refers to both desktops and laptops.

applications that are not properly licensed. Additionally, organizations risk significant payroll overtime, consulting fees or equipment costs when unapproved or non-authentic software is installed on their networks, introducing unwanted, uninvited and often unintended consequences such as unforeseen crashes, breaches or system failures. Therefore, organizations need an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. Additionally, website and related supporting servers are also an area of significance as attackers could identify vulnerabilities and use them to their advantage to gain unauthorized access to a network, possibly exposing a network or data to security threats. Strong website and related network security could result in decreased intrusions on a system and risks associated with data breaches.

Software management and website security are of particular importance to larger entities, such as colleges, that have many different users[2] that perform a variety of functions. Typically colleges will have several software applications and multiple licenses for each.

We examined installed software and licenses on College computers and website vulnerabilities for the period September 1, 2013 through March 31, 2015.[3] We interviewed College officials and staff and reviewed policies and procedures over IT to identify the controls established. We also reviewed 36 randomly selected[4] computers to determine if the installed software was appropriate and if the College had proper licenses.

We conducted this performance audit in accordance with generally accepted government auditing standards (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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

The management of software and licenses is essential to safeguarding College assets and data. Therefore, organizations need to have an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. The effective management of software also includes ensuring that only appropriate business or academic software is installed to reduce the risk of unwanted consequences that could result from unauthorized software. This can be done, in part, by establishing a strong acceptable use policy, limiting users' ability to install software, regularly reviewing computers to identify installed software and taking action to remove any unauthorized software. We found College officials and IT staff can more efficiently and effectively manage software licenses.

Acceptable Use Policy – Good controls over computerized data include an acceptable use policy that informs users about the proper use of College computers and require the monitoring of

[2] Such as students, staff and faculty

[3] Specific point-in-time testing for software installations was performed on January 13, 14 and 15, 2015 and February 9, 2015. Web vulnerability testing was performed over the period January through March 2015.

[4] We obtained a hardware inventory list of all College computers by location and user type. We selected a total of 36 computers for review based on the following categories: student-main campus (three computers), student-satellite locations (three computers), faculty/staff-main campus (25 computers) and faculty/staff-satellite locations (five computers).

computer usage to ensure compliance. An acceptable use policy defines the Board's goals for the use of equipment and computing systems and the security measures to protect the College's resources and confidential information. The policy should address, but not necessarily be limited to, the acceptable use of email accounts and Internet access and the installation of software on College computers. It is important that the policy provide provisions for enforcement and penalties for noncompliance and that system users provide written acknowledgement that they are aware of, and will abide by, the policy.

The Board has adopted a computer code of conduct, or acceptable use policy, that outlines limited guidelines related to software installation and usage. However, the policy does not detail practices for enforcement, such as monitoring computer use and reviewing installed software. Additionally, users are not required to provide written acknowledgment that they will comply with the policy terms.[5] The policy, approved by the Board in February 2011, is not regularly reviewed and does not show any further evidence of review or updating. An inadequate acceptable use policy significantly increases the risk that hardware and software systems and the data they contain may be lost or damaged by inappropriate use. This leaves the College vulnerable to risks associated with personal use, including computer viruses and spyware that could potentially be introduced by accessing nonbusiness or nonacademic related websites or downloading unauthorized software.

Software Inventory – The purpose of a software license is to grant an end user permission to use one or more copies of software in accordance with copyright law. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Organizations must obtain licenses commensurate with the number of copies in use. The implementation of a complete and comprehensive software inventory list is crucial to safeguard IT assets from potential unlicensed software being installed on computers. As a best practice, the list should include all College-owned software installed on computers and the number of copies currently in use. Furthermore, the list should be used in regularly reviewing all computers owned by the College to ensure that all software installed is properly approved and licensed.

We found that College IT staff do not maintain a comprehensive inventory list of all software that the College currently owns and the total number of licenses for each software. Individual departments are responsible for maintaining supporting documentation for software purchased and installed on department computers. Upon specific request, departments were able to provide the IT staff with records and documentation for most of the software that would have been included on such an inventory list.[6]

In addition, we found no evidence that College IT staff effectively performed regular audits of software installed on machines. There are no formal procedures for the regular review of individual computers or for removing nonbusiness-related software installed on College computers. The regular review of computers is critical for reviewing installed software because the College provides all faculty and staff users with administrative rights. Therefore, users are able to download and install software without prior permission or approval. As a result, the IT staff and

[5] A screen with the summarized policy terms prompts each time a user attempts to log on to the network. Users are required to click "OK" prior to logging in to the network, but this does not ensure that users are aware of the full policy and all its terms and expectations.

[6] See Software Monitoring section for more information.

department heads may not be aware of all software that users have installed. IT staff informed us that the practice for reviewing installed software has been more reactive than preventive. The IT staff will review computers that are reported to them with issues. If unlicensed software or a malicious installation is discovered, it is removed immediately; however, this does not ensure that the identification or removal of such installations is timely. The IT staff stated that there have been issues in the past because viruses are sometimes inadvertently downloaded. The installation of unlicensed software or malware[7] is due, in part, to faculty and staff users being given administrative rights without regular monitoring.[8]

Because IT staff do not maintain a comprehensive software inventory list or perform regular, formal reviews of College computers, there is an increased risk of unauthorized software being installed and not detected. Further, the lack of review and enforcement of software installations, the reactive rather than preventive actions of College officials and IT staff, and the practice of providing faculty and staff users with administrative rights resulted in nonbusiness or nonacademic-related software, as well as malware, being installed on certain computers. Therefore, there is a high risk that the network could be corrupted, and College equipment could be used for inappropriate or nonbusiness or nonacademic related activity without being detected timely.

Software Monitoring – The College developed a computer code of conduct, or acceptable use policy, to provide employees with guidelines for IT asset use and security. Specifically, authorized use includes appropriate College-related work. Additionally, users should ensure that downloads or modifications of programs do not violate copyright and patent laws. The policy defines general unauthorized use of IT assets, including engaging in malicious activity designed to harm College computers or networks and violating any federal, State or local laws or regulations.

To determine if installed software was authorized, had valid licenses when required, was for a legitimate business purpose and was in compliance with the College's acceptable use policy, we selected 36 computers[9] for review. We identified approximately 850 software installations,[10] of which 85 installations required licensing. We requested purchase orders,[11] license and user agreements to verify that the College had proper licensing to cover all copies of software installed on the computers reviewed. The departments could not provide purchase orders or other supporting documentation for two installed software programs that required licensing. We found these programs to serve a legitimate business purpose; however, without proper documentation, the College cannot ensure that the programs were properly licensed. In addition, on four computers, each used by a faculty or staff member, we found installed software[12] that was not reasonable for academic or business purposes. The inappropriate software included gaming and game editing programs and coupon applications. In addition, we also identified a virus that had been installed

[7] Software intended to damage or disable computers or computer systems

[8] IT staff stated that significant, repeated issues related to user accounts with administrative rights has and will result in revocation of these rights for the specific users.

[9] See Appendix B, Audit Methodology and Standards, for more information.

[10] A portion of these installations included upgrades and components of larger software programs.

[11] An effective and efficient method for purchasing and accounting for software licenses is through a purchase order system. A purchase order serves as the source document for vendor payment claims for various licenses obtained by the College and provides a record of licenses on hand to avoid duplicate purchases.

[12] Two of the computers each had an inappropriate installation and the remaining two computers each had two inappropriate installations. Therefore, there was a total of six inappropriate installations between these four computers, comprising four different types of software.

on one of these computers. Based on the nature of these programs, they do not serve a legitimate work-related purpose and are in violation of the College's acceptable use policy. Furthermore, non-College related programs may interfere with employees' work responsibilities. If user rights had been restricted on faculty and staff computers, these inappropriate and potentially harmful installations may not have occurred.

Because all faculty and staff users have administrative rights, thorough monitoring of College computers is not performed and the College does not enforce the acceptable use policy, certain inappropriate and malicious installations on machines went undetected. Potentially unauthorized software and software that does not serve a College business purpose may increase the risk that unauthorized access or modification to the computer system environment may occur and has resulted in individual computers and the College's network being exposed to harmful events such as viruses.

Recommendations

The Board should:

1. Update the computer code of conduct (acceptable use policy) to include specific guidance related to software downloads and installations, as well as enforcement. This policy should be regularly reviewed, updated and distributed to users to obtain their written agreement of compliance with the policy terms.

College officials should work with IT staff to:

2. Ensure that administrative rights are limited to only those College employees with a need for such access.

3. Maintain a complete, comprehensive software inventory list of all software that the College owns and the total number of licenses for each software.

4. Formalize procedures to perform reviews of software installed on College computers and compare results to the College's software inventory list.

5. Monitor users to ensure compliance with the computer code of conduct (acceptable use policy) and ensure software installed on College computers is business or academic appropriate.

The Board has 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 New York State 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 the Board to make this plan available for public review in the Secretary to the Board's office.

We thank the officials and staff of the Monroe Community College for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Gabriel F. Deyo
Deputy Comptroller

APPENDIX A

RESPONSE FROM COLLEGE OFFICIALS

The College officials’ response to this audit can be found on the following pages.

Monroe Community College
STATE UNIVERSITY OF NEW YORK

Anne M. Kress, Ph.D.
President

July 16, 2015

Mr. Edward V. Grant, Jr.
Chief Examiner
Division of Local Government and School Accountability
The Powers Building
16 West Main Street – Suite 522
Rochester, NY 14614

RE: Response to Audit Report Number: P2-15-11

Dear Mr. Grant:

This letter serves as the formal written response to the audit conducted by the Office of the State Controller (OSC) for Monroe Community College (MCC). The staff of MCC appreciates the opportunity to work with the auditing staff of the OSC and welcomes the findings as outlined in the preliminary report of June 16, 2015. We believe these recommendations will help to improve the Information Security and Technology operations within the College.

MCC is committed to a safe and secure computing environment and will address the recommendations of the audit as follows:

Recommendation #1

Update the computer code of conduct (acceptable use policy) to include specific guidance related to software downloads and installations, as well as enforcement. This policy should be regularly reviewed, updated and distributed to users to obtain their written agreement of compliance with the policy terms.

Response: MCC will modify the code of conduct to include specific guidance related to software downloads and installations, as well as enforcement and submit for Board of Trustees approval. Additionally, the code of conduct policy will be regularly reviewed, updated and distributed to users and be incorporated into the security training containing a module requiring users to accept and acknowledge the policy. An online version of security training was announced to employees on 6/23/15.

Recommendation #2

Ensure that administrative rights are limited to only those college employees with a need for such access.

Response: MCC will consider implementation of a more robust and random inspection of computers while assessing the business need for administrative access to the computer. If it is determined that adjustments are required because of an unacceptable level of risks, these will be achieved within the bounds of available resources via selective restrictions on faculty and staff.

Recommendation #3

Maintain a complete, comprehensive software inventory list of all software that the college owns and the total number of licenses for each software.

Response: MCC has created a software inventory list that will be maintained and regularly monitored. Additional verification and certification fields will be added to satisfy the OSC audit recommendations.

Recommendation #4

Formalize procedures to perform reviews of software installed on college computers and compare results to the college's software inventory list.

Response: MCC will implement a formal procedure and review process to enable detection of software not included on the official list maintained by the College. Following the sampling methodology of your audit team, throughout the year, MCC will sample 1% or approximately 38 campus computers randomly on an annual basis for an internal audit.

Recommendation #5

Monitor users to ensure compliance with the computer code of conduct (acceptable use policy) and ensure software installed on college computers is business and/or academic appropriate.

Response: Based on our previous responses to the recommendations, this will be accomplished by random audits.

We hope that you find our response to the recommendations accommodating and facilitate the issuance of your final report.

Sincerely,

Anne M. Kress

cc: Hezekiah Simmons, Vice President, Administrative Services
Michael Quinn, Controller
David Lane, Associate Vice President, Technology Services/CFO
Sheila Strong, Executive Assistant to the President

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objectives of our audit were to determine if College officials efficiently and effectively managed software licenses and whether security vulnerabilities exist in College websites, web applications or supporting servers. To accomplish our objectives, we reviewed IT controls and processes for the period September 1, 2013 through March 31, 2015. To achieve the objectives of this audit and obtain valid audit evidence, we performed the following audit procedures:

- We interviewed College officials and staff and reviewed IT policies and procedures to determine the internal controls in place.

- We obtained a computer inventory list for all campuses from IT staff and sorted this list by location and end user (i.e., students, faculty and staff). From the inventory lists, we randomly selected 36 College-owned computers for review: 25 faculty/staff and three student computers were selected at the main campus, and five faculty/staff and three student computers were selected at the satellite campuses. We used specialized audit software to obtain a list of all software installed on each machine. We reviewed the installations for licensing requirements and to determine if they served a legitimate business purpose.

- We reviewed the provided license agreements and purchase orders to determine if the College authorized all software and whether it maintained licensing for the software installed on each of the computers reviewed.

- We performed vulnerability testing on College websites, web applications and supporting servers using specialized scanners and audit tools.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.