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

Katherine P. Douglas, President
Members of the Board of Trustees
Corning Community College
1 Academic Drive
Corning, NY 14830

Report Number: P2-15-9

Dear President Douglas 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 Corning 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 January 30, 2015. Because of the sensitivity of some of this information, we do 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 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, or include penalties for noncompliance. Additionally, users are not required to read and provide written acknowledgment that they will comply with the policy terms. 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; however, the IT department does maintain detailed records of licenses purchased. In addition, College officials and IT staff do not regularly monitor or review computers to ensure that all software installed is appropriate and legally obtained and do not enforce removal of inappropriate software when identified. We found installations of nonbusiness and nonacademic related software on College computers through review of the software installations report provided by the College, including gaming, gambling and personal income tax preparation software. Our detailed review of 36 computers identified four that contained gaming or instant messaging related software. 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 Steuben, Schuyler and Chemung counties and operates a main campus, the Corning campus and four satellite campuses: Airport Corporate Park, Business Development Center, Elmira Academic Center and Goff Road Facility. The College is part of the State University of New York system and is governed by a 14-member Board of Trustees (Board) which consists of 13 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 (CFO). 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 Director of IT (Director). The Director is responsible for overseeing the College's daily IT operations and functions, including supervising IT department staff. The Technology/Information Steering Committee is responsible for the administration of certain IT policies. Between all campuses, the College has approximately 900 computers. Budgeted appropriations for IT for the 2014-15 fiscal year were approximately $1.05 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 applications that are not properly licensed. Additionally, organizations risk significant payroll

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

overtime, consulting fees and 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, websites 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 January 30, 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 requires the monitoring of computer usage to ensure compliance. An acceptable use policy defines the Board's goals for the

[2] Such as students, staff and faculty

[3] Specific point-in-time testing for software installations was performed on December 4, 8, 9 and 15, 2014. Website vulnerability testing was performed from December 2014 through January 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).

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 an 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, or include penalties for noncompliance. Additionally, users are not required to provide written acknowledgment that they will comply with the policy terms. The policy, approved by the Board in January 2009, is not regularly reviewed and does not show any evidence of further review or updating. The inadequacy of an 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. In addition, because the College's acceptable use policy does not require users to accept policy terms or include penalties for noncompliance, enforcement of policy terms may be limited.

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 the College does not maintain a comprehensive inventory list of all software that the College currently owns and the total number of licenses for each software. However, the IT department maintains organized detailed records of licenses purchased and, upon request, was able to provide records and documentation for software that would have been included on such an inventory list.[5]

In addition, the College did not effectively use available tools to perform regular audits of software installed on computers. Each time a College computer connects to the network, the software on the computer is inventoried. From this information, a report of all users and the software installed on their computers can be generated, as well as a report of all applications and the number of computers each application is installed on. However, there are no formal procedures for the regular review of these reports or individual computers, or for removing nonbusiness related software installed on College computers. The Director developed his own informal practice to generate and review these reports annually. As part of his review, he makes note of any nonbusiness-related

[5] See Software Monitoring section for more information.

applications installed on College computers and communicates this information to the CFO. The CFO informed us that the Director will informally discuss the inappropriate software with the faculty or staff member, but there are no incentives for the user to remove the software and the College does not force removal.

IT staff provided examiners with a current installed software inventory report at the beginning of audit fieldwork.[6] Using this report we identified several applications installed on College computers that were not appropriate for business or academic purposes, including those related to gaming, gambling and personal income tax preparation.[7] These programs were able to be installed, in part, because faculty and staff were given administrative rights.[8]

Because the College does 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, along with some users having administrative rights, resulted in nonbusiness or nonacademic related software being installed on certain computers.

Software Monitoring – The College developed an acceptable use policy to provide employees with guidelines for IT asset use and security. Specifically, authorized use includes support work, professional development, study, research, service or student activities consistent with the College's mission and goals. Employees are also allowed limited incidental personal use not otherwise prohibited by this policy. In general, use must be appropriate and in compliance with College policies; not violate the law, licensing agreements or intellectual property rights; and not interfere with the employee's work responsibilities. The policy defines general unauthorized use of IT assets, including users obtaining resources beyond their authorization.

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 800 software installations,[10] of which 82 installations required licensing. We requested purchase orders,[11] licenses and user agreements to verify that the College had proper licensing to cover all copies of software installed on the computers reviewed. The College was able to provide supporting documentation for all installed software programs that required licensing, all of which we also found to serve a legitimate business purpose. On four computers, each used by a staff or faculty member, we found installed software[12] that was not reasonable for academic or business purposes. The inappropriate software included gaming programs and an application that detects invisible users on an instant messaging program. Based on the nature of these programs, they do not serve a legitimate work-related

---

6 Report was provided on November 24, 2014.

7 Some examples of applications identified include Disney's Winnie the Pooh, Dora (the Explorer) Lost City and Party Poker.

8 IT staff stated that, as of November 2014, computers coming in for reimaging and updates would not be provided with administrative rights and all software installation requests would go through the IT department.

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 One application on each computer

purpose and are in violation of the College's acceptable use policy. Furthermore, non-College-related programs may interfere with employees' work responsibilities.

Because some users have administrative rights, thorough monitoring of College computers is not performed and the College does not enforce the acceptable use policy, certain inappropriate installations on computers went undetected and those detected were not removed. 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 the individual computer or network may be exposed to harmful events. In addition, because the College's acceptable use policy does not require users to accept the terms or include penalties for noncompliance, enforcement of the policy terms may be limited.

Recommendations

The Board should:

1. Update the acceptable use policy to include specific guidance related to software downloads and installations, as well as enforcement and penalties for noncompliance. 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. Maintain a complete, comprehensive software inventory list of all software that the College owns and the total number of licenses for each software.

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

4. Monitor users to ensure compliance with the acceptable use policy and ensure software installed on College computers is business and/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 Corning 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 page.

corning community college
State University of New York

Office of the President

1 Academic Drive
Corning, New York 14830-3297
607-962-9232 800-358-7171 x 232
Fax: 607-962-9485
www.corning-cc.edu

June 30, 2015

Gabriel F. Deyo, Deputy Comptroller
Division of Local Government and School Accountability
Office of State Comptroller
110 State Street
Albany, NY 12236

Dear Mr. Deyo:

This is to inform you that we have completed our review of the draft findings referenced in your memorandum dated June 2, 2015. As part of that review, we met with members of your staff on June 25, 2015, to further discuss those findings. This is to inform you that we concur with your findings and recommendations and have begun the process of developing a corrective action plan to address them.

The Regional Board of Trustees and I appreciate the level of professionalism and expertise displayed by your team, and we are grateful for their observations and suggestions for improvement. We look forward to receiving your final report.

Sincerely,

Dr. Katherine P. Douglas
President

Cc: Dr. Cornelius J. Milliken, Chair of the Regional Board of Trustees
Mr. Thomas Carr, Vice President of Administrative Services
Mr. Bruce Campbell, Director of Information Technology
[redacted]

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 objective, we reviewed IT controls and processes for the period September 1, 2013 through January 30, 2015. To achieve the objective 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 computer. 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 reviewed the installed software log maintained for any obvious installations that were not appropriate for business or academic purposes.

- 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.