REPORT OF EXAMINATION | 2018M-130

Suffolk County Community College

Information Technology

NOVEMBER 2018

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Suffolk County Community College

Audit Objective

Determine whether College officials adequately safeguarded the College website, financial and student information system and online banking from unauthorized access and misuse.

Key Findings

- The College has:
  - 824 network user accounts (15 percent) that have not been used within the last six months and do not match current employees.
  - Four network user accounts with unnecessary administrative permissions and 131 financial and student information system user accounts with questionable permissions.
- Employees responsible for safeguarding the College website are not required to attend cybersecurity training.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to College officials.

Key Recommendations

- Enforce written policy for managing network and system access.
- Ensure employees receive relevant cybersecurity training at least annually.
- Address the confidentially communicated IT recommendations.

College officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The Suffolk County Community College (College) is governed by a Board of Trustees (Board), which is composed of nine appointed members and one elected student trustee. The Board is responsible for the general oversight of operations including adopting policies to safeguard IT assets.

The Vice President for IT Services oversees IT operations and is responsible for securing IT assets, including the website and the financial and student information system. The Vice President for Business and Financial Affairs, is responsible for overseeing business operations which includes online banking.

Quick Facts	
2017-18 IT Appropriations	$8.1 million
Employees	5,002
Servers	82
Computers (including laptops and tablets)	4,571
Network User Accounts	5,426

Audit Period

September 1, 2015 – October 31, 2017

Information Technology

The College's IT assets are valuable resources that officials rely on to share information with current and prospective students, conduct financial transactions via the Internet and maintain financial, personnel and student records. Safeguarding these IT assets from unauthorized access and misuse will help to ensure that information used to make decisions is secure, reliable and available when needed. If these assets are compromised, the results could range from being inconvenient to catastrophic and could lead to damage requiring extensive effort and resources to evaluate, repair and recover. While effective IT controls will not guarantee safety, a lack of effective controls significantly increases the risk that data, software and hardware may be stolen, lost or damaged by unauthorized access and misuse.

What Are Effective IT Controls?

College officials should develop comprehensive written procedures for managing access to the college network and the financial and student information system (information system). These procedures should include periodic reviews to ensure network and system accounts and permissions are necessary and appropriate. Officials should disable or remove unnecessary user accounts as soon as no longer needed to decrease the risk of unauthorized access or misuse. In addition, officials should ensure employees receive cybersecurity training at least annually. Training should address current threats, such as phishing,[1] ransomware[2] and current attack techniques relevant to college systems and assets accessible by employees. Because the IT environment is changing so quickly, it is important that IT policies and procedures be updated routinely.

College Officials Did Not Adequately Manage User Access

Although the Board adopted a policy for managing access to the network and the information system, College officials did not enforce the policy. Consequently, the College has 824 network user accounts that do not match current employees and have not been used within the last six months. Of these, 616 accounts have never been used and another 69 accounts have not been used in more than three years. Officials told us that some network accounts are limited to email access and others are kept active due to contractual requirement.

Because any account on a network or in the information system is a potential entry point for unauthorized users and if unnecessary accounts are not disabled or removed as soon as they are no longer needed, there is an increased risk

1 Sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software.

2 A type of malicious software that prevents users from accessing their computer systems or electronic data until a ransom payment is made.

of unauthorized access or misuse. In addition, four network user accounts had unnecessary administrative access,[3] which had complete control over all servers and computers on the network, and can perform activities such as installing software, creating user accounts and manipulating security settings. If such an account is compromised, the attacker (or program developed by the attacker) would have the same permissions as the compromised account. To minimize the damage, which would result from a compromise, administrative network permissions should be limited to those users who need such permissions to perform their job duties. Officials told us that they removed all unnecessary administrative permissions as a result of our audit.

We also found that 131 accounts (14 percent) had questionable user permissions in the information system. These included the permissions granted to five employees, who were not department heads,[4] with system accounts in the department manager/approver finance group and 46 employees, who were not deans and associate deans or in equivalent job titles (e.g., director), with accounts in the deans and associate deans financial aid group. Access to this group provides individuals with access to personal financial information that may not be necessary to perform their job duties.

Of the remaining 80 accounts with questionable permissions, 52 were general faculty members with permissions to update faculty assignments and student test scores and/or authorize permit overrides.[5] IT officials told us that they do not make permission decisions. Supervisors make permission requests, which are approved by department heads. IT Services then enables those permissions. However, users should only be granted the permissions necessary to perform their job duties and any unnecessary permissions increase the risk of unauthorized access or misuse.

Employees Did Not Receive Relevant Cybersecurity Training

While some employees recently attended general cybersecurity training, this training was not mandatory for all employees and did not cover techniques relevant to college systems and assets accessible by employees. Most notably, employees responsible for safeguarding the website generally were not required to attend the training and had not been formally trained on common web application risks such as code injection and authentication vulnerabilities. Lack of

3 These user accounts included an assistant director, a systems analyst, and two generic accounts.

4 These employees included a senior purchasing agent, purchasing agent, purchasing technician, principal account clerk and an accountant.

5 A permit override allows an employee to override a restriction to process a student registration for a particular course.

relevant cybersecurity training increases the risk that employees will not be aware of and take steps to prevent such vulnerabilities, leaving the website at risk of unauthorized access or misuse.

Officials Established Effective Controls Over Online Bank Transfers

Although College officials have no formal policies governing online banking, we found that they had effective informal procedures in place for secure online banking and fund transfers.

The College has written agreements with its banks that outline the scope of services provided. Transfers are initiated by one of two authorized employees, and then approved by an associate dean. Access to the online banking account is controlled with a unique username and password and a token that generates numbers that are necessary to log in for added security.

We reviewed all 17 online transfers totaling $29.7 million from the College's two main bank accounts for the period August 3 through September 30, 2017 and found they were for valid purposes. The transfers were either money moved to other College accounts or payments to government taxing authorities.

What Do We Recommend?

The Assistant Vice President for IT Services should:

1. Enforce policy for managing network and system access. Procedures should include periodic reviews to ensure network and system accounts are appropriate, and permissions are disabled or removed as soon as no longer needed.

2. Ensure employees receive relevant cybersecurity training at least annually. Training should address current threats and attack techniques relevant to college systems and assets accessible by employees.

Appendix A: Response From College Officials

Suffolk
COUNTY COMMUNITY COLLEGE

Office of Information Technology Services

November 13, 2018

Ira McCracken, Chief Examiner
Division of Local Government & School Accountability
Office of the State Comptroller
110 State Street
Albany, New York 12236

Re: Suffolk County Community College Response to Information Technology Report of Examination 2018M-130 and Information Technology Security Controls Letter, Period Covering September 1, 2015 – October 31, 2017

Dear Mr. McCracken:

Suffolk County Community College ("the College") is in receipt of the preliminary draft findings of your recent audit of the College entitled *Information Technology, Report of Examination 2018M-130* and the *Information Technology Security Controls Letter* for the period covering September 1, 2015 – October 31, 2017. On behalf of the College's Board of Trustees, the College President, and the College's Administration, please allow me to extend our thanks to you and to your staff for your efforts and diligence in ensuring that the College maintains effective information technology ("IT") security controls. The College strives to be a College of Excellence and constructive criticism is necessary if we are to maintain that goal.

Please consider this letter as both the College's response to the audit and the requested corrective action plan (CAP), consistent with the State Comptroller's established guidelines.

Response to the Draft Audit Report

Management of User Access

With regard to the examiners' findings relating to the College's management of network and system access, we acknowledge that the College has a number of user accounts that are not attached to active employees. By our calculation of the number of these accounts is significantly smaller than the examiners' calculation, and many, but not all, of these accounts are necessary to the College's operations.

The nature of the College's adjunct and faculty emeritus workforce is such that user accounts for these employees must be maintained from semester to semester, even when these employees are not on payroll in the current semester. Adjunct employees and retired faculty with emeritus status bid on adjunct (part-time) assignments for future semesters through a College portal that requires a College user account. This system assists the College in ensuring that its collective bargaining agreement with its Faculty Association and

seniority-based assignment system is followed. The Faculty Association contract also requires that adjuncts on the College's adjunct seniority list be retained until the adjuncts have not worked for **eight semesters**. Accordingly, unless the adjuncts have given clear indication that they wish to be removed from consideration for future assignment, they must remain active for purposes of user account access until they have not had an assignment for eight consecutive semesters. To the extent these user accounts factored into the examiners' calculation of the number of user accounts not attached to "active employees," we are required by a collective bargaining agreement to maintain these accounts for the required number of semesters.

Similarly, ITS identified 371 generic user accounts that would not be attached to the name of a College employee in the online directory. We understand why this would appear problematic at first glance; however, these generic user accounts are in fact controlled and utilized for specific purposes. Of the 371 generic user accounts, 71 were actual user accounts that are generic but are used for back-end processes. The rest are service accounts or group mailboxes that users cannot log into; the passwords are randomized and are not given out. This will explain why it would appear that the accounts are not being used.

With regard to the findings regarding access permissions on user accounts, we reiterate that ITS does use generic accounts for back-end processes and service accounts, but access to these accounts is controlled. As also noted in the draft findings, we have removed all unnecessary administrative permissions as a result of the examiners' audit. Regarding the remaining accounts the examiners identified as having questionable user permissions and this issue more generally, we are appreciative of the examiners' observations and recommendations and will review the existing procedure for granting and reviewing user permissions to identify the best way to address this on a prospective basis.

Based on the draft findings, the examiners made a key recommendation that the College should enforce written policy for managing network and system access. We are appreciative of the recommendation made by the examiners and intend to act accordingly.

ITS has undertaken a clean-up of the user accounts. The [redacted] will be compared to the College's [redacted] system and reviewed on a semester-to-semester basis. There is an expectation that accounts will still be needed for specific purposes, but any account not attached to an active user will have a description added to justify its existence. The College has a termination report already in place that is acted upon such that, in most cases, if an employee is no longer with the College, the account will be disabled. The report that will be run on a weekly basis will catch those that were not disabled. Policies and procedures for granting and reviewing user permissions will be reviewed and revised if necessary to ensure appropriate access controls are maintained.

Cybersecurity Training

With regard to the examiners' findings relating to the College's provision of relevant cybersecurity training, we acknowledge that there is no mandatory training required for all employees at the College. Instead one module of the College's online training for all employees through Workplace Answers is "Security and Safe Remote and Mobile Computing." The objective of this training is to assist employees in identifying and avoiding remote and mobile computing risks. Employees' completion of the training is monitored but not uniformly enforced.

Additional employee awareness initiatives are undertaken periodically to assist employees in avoiding potential cybersecurity threats, including phishing attempts. ITS has begun annual phishing campaigns. An initial cycle of phishing tests across ITS staff, College leadership, and College faculty and staff was completed between

March and May 2018. The results of this campaign will allow ITS to concentrate awareness training for groups within the College that need additional information security education. College-wide communications about these initiatives remind employees of the procedure for notifying Information Technology Services of any suspicious email activity.

Based on the draft findings, the examiners made a key recommendation that the College should ensure employees receive relevant cybersecurity training at least annually. The College is appreciative of this recommendation and will review its existing policy and procedures for deploying mandatory training initiatives and monitoring compliance accordingly.

Effective Controls over Online Bank Transfers

The College is pleased that the examiners found effective procedures in place at the College for secure online banking and fund transfers. The College will continue to utilize these procedures to ensure that its online banking and fund transfers remain secure.

Confidentially Communicated IT Recommendations

Please refer to the separate enclosed response to the confidentially communicated IT recommendations.

Corrective Action Plan

1. Audit Recommendation: Enforce policy for managing network and system access. Procedures should include periodic reviews to ensure network and system accounts are appropriate, and permissions are disabled or removed as soon as no longer needed.
    a. User Accounts
        i. ITS will complete an initial clean-up of existing user accounts. **Undertaken; expected to be complete by December 31, 2018.**
        ii. ITS will review user accounts on a semester-to-semester basis for maintenance or termination determination. [redacted] will be compared to the College's [redacted] system. Accounts still needed for specific purposes will be maintained, but any account not attached to an active user will have a description added to justify its existence. **Begin in next semester; continue on ongoing basis each semester.**
        iii. The College will continue the use of termination reports so that terminated employees' accounts will be disabled. **Ongoing.**
    b. Account Permissions
        i. ITS will remove all unnecessary administrative permissions. **Complete.**
        ii. ITS will review the existing procedures for granting and reviewing user permissions for possible revision to ensure appropriate access controls are maintained. **Begin by December 31, 2018 with planned completion by end of Quarter 2 of 2019. For [redacted] access permissions, possible solutions will be explored as part of the College's planned migration to [redacted]**
2. Audit Recommendation: Ensure employees receive relevant cybersecurity training at least annually. Training should address current threats and attack techniques relevant to College systems and assets accessible by employees.
    a. The Office of Legal Affairs will redeploy "Security and Safe Remote and Mobile Computing" online training to all College employees with deadline for completion. **Request made to online training provider for anticipated re-deployment of training before January 2019.**

i. The Office of Human Resources will ensure appropriate follow-up takes place with employees who did not complete the training. **After deadline for completion in Spring 2019.**

b. ITS will continue implementation of phishing campaigns and identify areas needing additional targeted cybersecurity training. **Undertaken in Spring 2018; continue on ongoing basis.**

c. ITS will provide additional cybersecurity guidelines and training to coincide with the College's planned migration to [redacted] for employees. **Planned to take place in December 2018.**

d. ITS, in consultation with the Office of Legal Affairs and the Assistant Vice President for Employee Resources, will develop a policy for mandatory cybersecurity training that will include training modules relevant to employees' duties. **Policy to be developed by end of Quarter 1 of 2019. Trainings to be developed or identified by end of Quarter 1 of 2019. Trainings to be delivered starting in Quarter 2 of 2019. Trainings to be delivered annually thereafter.**

Once again, we thank the examiners for their efforts and recommendations. We will use this as an opportunity to enhance our IT controls, policies, and procedures.

Very truly yours,

Shady Azzam-Gomez
Vice President, Information Technology Services

Enclosure (Response to Confidentially Communicated IT Recommendations with CAP)

cc: Board of Trustees
Dr. Shaun L. McKay, President
Louis J. Petrizzo, College General Counsel / Executive Vice President
Gail Vizzini, Vice President, Business & Financial Affairs

Appendix B: Audit Methodology and Standards

We conducted this audit 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. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed College officials and employees to obtain an understanding of the College's IT operations.
- We reviewed College records for any IT related policies and procedures and reviewed those policies and procedures to obtain an understanding of the College's IT operations.
- We provided an audit script to officials to gather network user account data and examined the gathered data to identify accounts that had not been recently used.
- We obtained a report of system user account data and examined the provided report to identify accounts that had not been recently used.
- We compared a list of network user accounts and a list of information system user accounts to a list of current employees to identify accounts that are not affiliated with the College or that have unnecessary permissions.
- We reviewed training records for relevant IT staff to determine the type of training each employee received and whether it sufficiently addressed cybersecurity threats specific to their job duties.
- We reviewed online banking controls and selected the two main operating accounts at two different banks[6] for review. We reviewed all 17 online transfers totaling $29.7 million for the period August 3 through September 30, 2017 to determine whether they were for valid purposes. We judgmentally selected this period because it was close to the beginning of our audit field work. The bank accounts selected were the main operating accounts – one used for operating expenditures to pay vendors and one used to collect tuition.

Our audit also examined the adequacy of certain IT controls. 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 this performance audit in accordance with GAGAS (generally accepted government auditing standards). 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.

6 College officials had 17 bank accounts at seven different banks during our audit period.

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 relevant population size and the sample selected for examination.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided 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 the Board to make the CAP available for public review in the Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/localgov/academy/index.htm

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

Local Government and School Accountability Help Line: (866) 321-8503

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6530 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller