Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued August 11, 2020

Holyoke Community College

For the period July 1, 2017 through March 31, 2019

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

August 11, 2020

Dr. Christina Royal, President
Holyoke Community College
303 Homestead Avenue
Holyoke, MA 01040

Dear Dr. Royal:

I am pleased to provide this performance audit of Holyoke Community College. This report details the audit objectives, scope, methodology, finding, and recommendations for the audit period, July 1, 2017 through March 31, 2019. My audit staff discussed the contents of this report with management of the college, whose comments are reflected in this report.

I would also like to express my appreciation to Holyoke Community College for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Robert W. Gilbert, Jr., Chair of the Board of Trustees, Holyoke Community College
Carlos Santiago, Senior Deputy Commissioner of Academic Affairs, Massachusetts Department of Education

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of Holyoke Community College (HCC) for the period July 1, 2017 through March 31, 2019.

In this performance audit, we reviewed HCC's information security training and awareness practices to determine whether system users had completed information security training and signed acceptable use policies.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1 **Page 5**	HCC did not ensure that required information security training was completed or retain copies of signed acceptable use policies.
Recommendations **Page 7**	1. HCC should develop, document, and disseminate to personnel an information security training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. 2. HCC's Information Technology Department should continuously monitor compliance with the policy to ensure successful completion of information security training for all system users. 3. HCC should have signed acceptable use policies[1] on file for all system users. 4. HCC should negotiate collective bargaining agreements to include information security training requirements for all system users.

[1] According to the SysAdmin, Audit, Network, and Security Institute, acceptable use policies outline the acceptable use of computer equipment by an organization's computer system users.

OVERVIEW OF AUDITED ENTITY

Holyoke Community College (HCC) was established by Section 5 of Chapter 15A of the Massachusetts General Laws and currently operates under the direction of an 11-member board of trustees. The board is responsible for operating under the regulations promulgated by the state's Board of Higher Education. Officers of the board of trustees include a chair, vice chair, and secretary, as well as the president of the college, who is an ex officio member.

HCC is a member of the Massachusetts public higher-education system, which consists of 15 community colleges, nine state universities, and five University of Massachusetts campuses. HCC is an accredited public two-year institution, offering more than 65 associate degree programs and certificate programs. HCC's main campus is located at 303 Homestead Avenue in Holyoke; HCC has additional off-campus locations in Holyoke, Ludlow, and Ware. According to its website, for fiscal year 2018, HCC had 10,749 students enrolled in credit and non-credit classes.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of Holyoke Community College (HCC) for the period July 1, 2017 through March 31, 2019.

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

Below is our audit objective, indicating the question we intended our audit to answer, the conclusion we reached regarding the objective, and where the objective is discussed in the audit findings.

Objective	**Conclusion**
1. Does HCC administer an information security training and awareness program, for individuals who have access to its computer system, that is in accordance with Section 6 of the Commonwealth's Executive Order 504; Sections 6.2.3 and 6.2.8 of the Executive Office of Technology Services and Security (EOTSS) Information Security Risk Management Standard IS.010; and Controls AT-1(a)(1), AT-2(a), and PS-6 within the National Institute of Standards and Technology[2] Special Publication 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*?	**No; see Finding 1**

To achieve our objective, we gained an understanding of the internal controls related to the objective by reviewing applicable policies and conducting interviews with HCC officials. In addition, we performed the following procedures to address our audit objective.

To determine whether HCC had administered an information security training and awareness program that was consistent with Commonwealth and industry standards, we obtained a list of the 813 users of HCC's Banner operating system who had active user accounts during the audit period. From this list, we selected a nonstatistical random sample of 60 users. For each user in our sample, we reviewed the electronic records maintained in HCC's information security training and awareness program, noting the

[2] According to its website, the National Institute of Standards and Technology promotes industry best practices in "innovation and industrial competitiveness by advancing . . . technology through research and development in ways that enhance economic security."

date training was assigned and the date it was completed. We noted that HCC had implemented information security training in October 2018 and had allowed users 60 days to complete initial training. We examined the documentation and tested to determine whether each user was assigned initial information security training in October 2018 or, if s/he was hired after October 2018, within 30 days of his/her hire date in accordance with EOTSS's Information Security Risk Management Standard IS.010. We compared the assigned training date to the completion date to determine whether each user who was assigned training had completed it in the required timeframe.

To determine whether users had signed acceptable use policies, we requested acceptable use policies from the Human Resources Department for each system user in this same sample. We reviewed the acceptable use policies to ensure that all users had signed them, noting their agreement with HCC's acceptable use terms.

Because we used a nonstatistical approach for our audit sample, we could not project our results to the entire population of system users.

Data Reliability

We obtained a list of Banner users from the Information Technology Department and assessed its reliability by comparing it to the Human Resources Department's list of personnel employed during the audit period. As a result of our data reliability analysis and trace testing, we found that the data in the Banner user list were reliable for the purpose of our audit objectives.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. Holyoke Community College did not ensure that required information security training was completed or retain copies of signed acceptable use policies.

Holyoke Community College (HCC) did not ensure that its system users received required information security training and did not retain copies of users' signed acceptable use policies. Without educating all system users on their responsibility of helping protect the security of information assets by requiring training and formal user acknowledgment of acceptable use policies, HCC is exposed to a higher risk of cybersecurity attacks and financial and/or reputation losses.

HCC did not establish a program to ensure that users received information security training until October 2018, and after a program was established, HCC did not ensure that all users were trained under the program. We reviewed 60 Banner users to determine whether HCC administered an information security training program to individuals who had access to its systems when it implemented its security awareness training on October 11, 2018.

From our sample of 60 system users, 1 user was terminated before the training was rolled out, and 8 users (6 employees, 1 work-study student, and 1 contract employee) were not assigned training. Of the remaining 51 users, 6 completed the training within 60 days, as required by HCC, and 2 completed the training after the required date. The other 43 users were assigned training but did not complete it.

For the same sample of 60 users, HCC could produce only 35 (58%) of the required signed acceptable use policies.

Authoritative Guidance

Massachusetts Executive Order 504 (effective September 19, 2008 through October 25, 2019) states,

> *All agency heads, managers, supervisors, and employees (including contract employees) shall attend mandatory information security training within one year of the effective date of this Order.*

In addition, the Executive Office of Technology Services and Security's *Information Security Risk Management Standard* (IS.010), effective October 15, 2018, states,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. . . . The New Hire Security Awareness course must be completed within 30 days of new hire orientation. . . .*
>
> *6.2.8 All new hires must sign the acceptable use policy.*

The National Institute of Standards and Technology (NIST)[3] Special Publication 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*, defines the controls to be implemented as a best practice to ensure the security of an entity's information technology. These controls include the following:

> *AT-2 The organization provides basic security awareness training to information system users . . .*
>
> *a. As part of initial training for new users. . . .*
>
> *PS-6 [The organization ensures] that individuals requiring access to organizational information and information systems:*
>
> *1. Sign appropriate access agreements.*

Reasons for Issues

HCC told us that no information security training program was implemented until October 2018 because the administration struggled with determining which department (Human Resources or Information Technology) should be responsible for ensuring the training of system users. As cybersecurity issues became an escalating threat in 2018, HCC decided the Information Technology Department would manage information security training.

HCC also does not have an information security training policy that documents its requirements for monitoring the information security training program, including the collection of user-signed acceptable use policies. According to NIST Special Publication 800-53r4, this type of policy could address areas such as "purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance."

[3] According to its website, NIST promotes industry best practices in "innovation and industrial competitiveness by advancing . . . technology through research and development in ways that enhance economic security."

HCC officials also stated that members of the Massachusetts Community College Council union[4] would not take training without additional compensation. The officials stated that the existing union contracts lacked specific language requiring the information security training and that HCC therefore could not require it.

Recommendations

1. HCC should develop, document, and disseminate to personnel an information security training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2. HCC's Information Technology Department should continuously monitor compliance with the policy to ensure successful completion of information security training for all system users.
3. HCC should have signed acceptable use policies on file for all system users.
4. HCC should negotiate collective bargaining agreements to include information security training requirements for all system users.

Auditee's Response

> *HCC's [Information Technology] department did in fact administer an industry standard training program from [the SysAdmin, Audit, Network, and Security Institute], which is the same program that the state supplies to their users. We did not implement this training until 2018 because there were multiple positions in the [Information Technology] department that were in transition, and we also did not have an Information Security Officer in place.*
>
> *Once we started implementing the training program, we were able to monitor the completions by running reports. We could not enforce the completion of the training because of union issues. We have since bargained with the [Massachusetts Community College Council] and [American Federation of State, County and Municipal Employees] unions to allow us to mandate the training. To better enforce the completion of the training, we will run reports and send lists to supervisors and deans so that they can assist in getting their staff to comply with the mandate and restrict access until completed.*
>
> *We also have multiple reminders setup to alert users about the training:*
>
> 1. *An initial email goes out to all employees whether they are new, or are in need of taking the annual training, with a link to the training and a deadline to complete the training.*
> 2. *A reminder email goes out 15 days before the due date to remind users to complete the training. We are going to increase the number of reminders to 7 days, and 30 days.*

[4] According to its website, "The Massachusetts Community College Council represents the faculty and professional staff at the fifteen community colleges of the Commonwealth of Massachusetts."

3. *Lastly, we have a notification that goes out 1 and 7 days after the training is overdue to alert users that they have not completed it.*

Human Resources disseminates the Acceptable Use Policy to all new employees through their onboarding process. The users have to read and accept the policy by completing a task in the onboarding system, which is stored electronically. Access to Banner, [the Massachusetts Management Accounting and Reporting System], and [the state's Human Resource Compensation Management System] will not be granted until completed. . . .

HCC will disseminate a policy and will ensure all users acknowledge receipt on an annual basis to continue to have access to enterprise systems. . . .

HCC runs reports monthly on completion of the training. We will enforce this completion by working with supervisors and deans in accordance with union contractual agreements. . . .

HCC will maintain an electronic record of users' acknowledgment of the College's Acceptable Use Policy. . . .

HCC successfully impact bargained the change with the unions and they have agreed to do security training.