



The State University  
of New York

**RECEIVED**  
EXECUTIVE CORRESPONDENCE

SEP 12 2016

OFFICE OF THE STATE COMPTROLLER  
THOMAS P. DiNAPOLI  
COMPTROLLER

Office of the  
Chief Financial Officer

State University Plaza  
Albany, New York 12246

[www.suny.edu](http://www.suny.edu)

September 7, 2016

Honorable Thomas DiNapoli  
Comptroller  
110 State Street  
Albany, New York 12236

Dear Mr. DiNapoli:

In accordance with Section 170 of the Executive Law, this is our 90-day response showing actions taken to address the recommendations contained in the State Comptroller's Audit Report on Compliance with Payment Card Industry Standards, State University of New York (2015-S-65). Our specific comments to the recommendations follow.

**To SUNY schools visited**

Recommendation 1: Implement the recommendations contained in the detailed preliminary reports.

*Response: The campuses visited have made significant progress in completing the recommendations included in the preliminary reports. External PCI consultants are assisting some campuses in their efforts to fully comply with PCI requirements.*

**To System Administration**

Recommendation 2: Develop strategies to enhance compliance with PCI DSS and improve monitoring of PCI compliance at all SUNY colleges.

*Response: Each SUNY campus has an Information Technology Department, inclusive of an Information Security Officer. Additionally, SUNY System Administration continues to offer support to campuses through many efforts, including:*

- *Our Security Operations Center offers campuses certain security testing;*
- *Procedure 6608 provides guidelines and standards for information security;*
- *SUNY Enterprise Risk Management has identified PCI compliance as well as information security as priorities;*
- *SUNY is working to implement an Information Security Policy, and the related procedures and reporting will include consideration for PCI compliance. This will include a requirement to annually complete a campus self-assessment questionnaire on information security, including PCI compliance; and*
- *The Office of the University Auditor has completed five audits that included PCI evaluations; and will share the results of this recent OSC audit with SUNY's business officers.*

To Learn  
To Search  
To Serve

the Power of



Recommendation 3: Revise contract templates for affiliates to address PCI DSS regulations and require affiliates' compliance.

*Response: SUNY has enhanced language in affiliate contract templates for SUNY campus-related entities. These templates will be made available to campus procurement officers, and others, to help ensure affiliates, as well as vendors, comply with PCI standards.*

Thank you.

Sincerely,



Eileen McLoughlin  
Senior Vice Chancellor for Finance and  
Chief Financial Officer

Copy: Chancellor Zimpher  
Provost Cartwright  
Mr. Abbott  
Ms. Hengsterman  
Ms. Labate  
Ms. Liapis  
Mr. Powalyk  
Ms. Vattimo