Committee Meeting: Policy Committee	Date: February 9, 2017
Committee Chair: Kathleen Masiello	
New or Edited: New	

POLICY NAME: Cardholder Data Policy

POLICY TYPE: Managerial

SUBMITTED BY: Daniel Bartkowiak, Information Security Officer, ITS

ISSUE OR STATEMENT OF PURPOSE:
This security policy has been created to abide by standards set forth by the Payment Card Industry Data Security Standard (PCI DSS).

CORRECTIVE ACTION PLAN RECOMMENDATION (if any): N/A

NEW OR EDITED POLICY: New

Introduction
This security policy has been created to abide by standards set forth by the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is not required by law, but failure to comply will put the college's ability to accept credit card payments at risk and may subject the college to fines.

Applicability and Authority
This policy applies to all employees that interact with cardholder data. Throughout the rest of this document, this group of people will be referred to as merchants. Authority to enforce controls and regulations established in this document come from the Chief Information Officer.

Payment Processing
No cardholder data should be transmitted into or stored in any medium including, but not limited to paper, cell phones, files or e-mail accounts. The sole exception is the console at the point of sale during the time of the transaction.

Training Requirements
Merchants must participate in PCI DSS awareness training upon hire and at least annually. Merchants must also review this policy annually. Multiple methods of communicating awareness is required. Methods may include, but are not limited to, posters, web based training, and memos.

Procedure Reference
The accompanying procedure referenced in the **Resources** section of this document outlines appropriate physical and technical instructions

POLICY NAME: Cardholder Data Policy **Continued**

Policy and Procedure Management
SUNY Erie's Information Technology Services (ITS) department may modify policies and procedures from time to time as required, provided that all modifications are consistent with federal laws, New York laws and SUNY policies.

Exhibit A: Cardholder Data Procedure:
https://myecc.ecc.edu/ITS-Security/Documents/CardholderDataProcedure.docx

ITS-Security at SUNY Erie:
https:/myecc.ecc.edu/ITS-Security/Pages/default.aspx
Laws, Policies, and Procedures that are applicable to SUNY Erie

DOES IT SUPERCEDE A POLICY/WHICH ONE: No

POLICY COMMITTEE RECOMMENDED ACTION:
Policy Committee recommends the Board of Trustees accept the Managerial policy under the Report of the Chair, Ad Hoc Committee Reports, and Policy Committee. This Policy supersedes all prior policies/procedures and practices related to Cardholder Data Policy**.**

POLICY COMMITTEE MEMBERS PRESENT: Trustee Kathleen Masiello, Student Trustee Rebecca Krakowiak, Provost of Academics Richard Washousky, Executive Vice President of Institutional Advancement and Efficiency Michael J. Pietkiewicz, Vice President of Enrollment Management Steven Smith, Director of Registrar Paul Lamanna, and College Senate Representative Michael Delaney

DATE OF BOARD ACCEPTANCE: February 22, 2018

POLICY COMMITTEE TEAM FOLLOW-UP:
Following Trustee acceptance, this Managerial will be included in the SUNY Erie Managerial Policy Manual and distributed to Officers defined above.

INFORMATION/INPUT CONSIDERED DURING POLICY COMMITTEE DELIBERATIONS:
The Policy has been reviewed and discussed at the Policy Committee meeting of February 9, 2018.
Documentation Referenced:
M&T's Auditing Body https://www.securitymetrics.com/
Payment Card Industry Standards https://www.pcisecuritystandards.org/
ITS-Security's PCI Compliance Project https://myecc.ecc.edu/ITS-Security/Pages/PCI-Compliance.aspx

EXHIBIT A

Introduction

SUNY Erie must follow standards set forth by the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is not required by law, but failure to comply will put the college's ability to accept credit card payments at risk and be subjugated the college to fines from the Payment Card Industry. This procedure includes internal controls as well as periodic compliance training.

Definitions:

Cardholder Data - Full magnetic stripe or the PAN as well as cardholder name, expiration date and service code.

Cardholder Data Environment - Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

Console - Screen, computer, keyboard, mouse, and card swipe used by merchant to input cardholder data and transmit cardholder data to the Payment Gateway.

Compromise - Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.

Encryption - Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse encryption) against unauthorized disclosure.

Input methods:
Card swipe - USB device that reads magnetic strip on the back of the credit card and outputs the data to the matching fields on the Payment Gateway.

Manual entry - Typing in the cardholder data on the merchant's keyboard.

Network Security Scan - Automated tool that remotely checks ECC's external IP addresses for vulnerabilities. Non-intrusive test involves reporting on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network.

Payment Gateway - The website in which the cardholder data is entered.

Point of sale (POS) - The physical area in which the customer supplies the card to the merchant.

Applicability and Authority

This procedure is for the use of all employees that interact with cardholder data. Authority to enforce controls established in this document come from the Chief Information Officer. Employees must acknowledge and agree to follow this procedure when there is a suspected compromise of hardware or data. Merchants must acknowledge and agree to the principals outlined in this policy.

Cardholder Security Roles
Merchant Staff - The merchant staff are any employees with direct access to cardholder data at the point of sale. It is up to the merchant staff to report suspicious activity of any kind.

Merchant Management - Merchant management is responsible for reporting any security concerns to ITS Administration. Merchant management is also responsible for coordination of training and dissemination of materials. Materials include this procedure for incident escalation.

ITS Staff - Employees that support applications and hardware. ITS staff must look out for any suspicious activity and report it to ITS Administration. ITS Staff also must perform an annual inventory of Merchant devices.

ITS Administration - ITS Administration will work with merchant staff and ITS staff to resolve any escalated security events.

Service Providers
PCI DSS requires that all service providers are validated annually. Erie Community College currently uses PayPal as their lone service provider. The Information Security Officer is responsible for validation of PCI compliance.

Payment Processing
The only permissible entry and transmission of cardholder data is in the PayPal Payflow Gateway website using Internet Explorer, Firefox, or Chrome web browser. Ellucian redirects the card entry transactions to the PayPal Payflow Gateway and is entirely segregated from the credit card transaction.

All transactions that involve the transfer of credit card information must be performed on systems approved by Erie Community College's ITS department.

Payments in which the physical credit card is taken at the point of sale must be swiped and only into the PayPal Payflow gateway.

Training Requirement
Merchants must receive training on the following topics:

- Verify persons claiming to be a service or repair person before allowing them access to POS Equipment.
- Not installing or replacing devices without verification.
- Report suspicious activity on all POS equipment.
- Escalation of security issues to appropriate personnel.
- The principals outlined in this policy.

Inventory
ITS staff will keep an inventory of Credit Card swipe devices. An audit will be done annually in which the physical device's serial number is checked against the recorded inventory. Additional observations will be noted as well (unexpected attachments, cables plugged into device, missing security labels, broken or different colored casing, different serial number and other external markings). Audits will have proper documentation reviewing results and time the audit was run.

Technical Controls
Merchant point of sale computers must have virus definitions updated at least daily. The PayPal Payflow gateway uses encryption to transmit cardholder data to PayPal. Every year, an external IP address scan of the Payment Gateway is required.

Validation
M&T Bank, our acquirer, calls for us to validate PCI Compliance annually. They have partnered with Security Metrics for validation requirements. ITS's Information Security Officer must complete the Self-Assessment Questionnaire and perform an external IP address scan of the payment gateway. Any vulnerabilities detected by the scan must be resolved by ITS staff in a timely manner.

Escalation Method
Upon the discovery of malicious activity, it is the Employee's duty to immediately report the incident or activity to the suitable personnel. Appropriate methods involve direct phone calls to their respective management contact. Emails, text messages, and other methods may be too slow and can be overlooked. If the management person contacted does not answer the phone or is not available, proceed to call the next applicable management contact. Management personnel to speak with in the event of a compromise are listed below.

Escalation Procedure for Merchant Staff and ITS Staff

1. Once compromise has been noticed or possible compromise may occur, contact the appropriate management personnel.
2. Describe, in detail, the reason for suspicion of compromise, when the incident happened, where the issue was discovered, and any ideas of the scope of the compromise.
3. Answer the management personnel's follow-up questions honestly and accurately.
4. Carry-out subsequent instructions.
5. When report of the incident is complete, document the incident in a service desk ticket and reference the management person the incident was reported to.

Escalation Procedure for Merchant Management and ITS Administration

1. Listen to the employee's account of the incident or potential incident.
2. Ask any follow-up questions to attain pertinent information about the incident and how to contain or prevent it.
3. Direct the employee to document the incident in a service desk ticket and to add your name to the ticket for reporting purposes.
4. Either direct the employee to continue work or to wait for further instruction depending on the severity and status of the security incident.
5. Contact the Information Security Officer and share all details of the escalated report. If the Information Security Officer is unavailable, call the Director of Communication Systems or Network Administration Specialist.

Escalation handling for Information Security Officer or available ITS Administration member

1. Inquire about any possible relevant details. If needed, visit the site to inspect the hardware or application in question.
2. Locate the source of the compromised system and disconnect breached systems from the network.
3. Research the logs and access reports to find intrusion points to patch vulnerabilities exploited.
4. Assess scope of the damage.
5. Meet with ITS-Security team to share findings and discuss a path forward.
6. Follow up with employee or employees that discovered and escalated the incident.

Merchant Management Contacts	ITS Administration Contacts
Business Manager 716-851-1856	Information Security Officer 716-270-2951
	Director of Network Systems Administration 716-270-2954

Resources
ITS-Security PCI Compliance Project:
https://myecc.ecc.edu/ITS-Security/Pages/PCI-Compliance.aspx