

Auburn University at Montgomery

Policies and Procedures

Title: Physical Security for Payment Card Data

Responsible Office: Office of Technology

I. PURPOSE

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

The standards are designed to protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with the University.

II. POLICY

The physical security surrounding equipment contained within the Auburn University at Montgomery Card Holder Data Environment will be regulated in such a manner to (at a minimum) ensure compliance with the provisions of the Payment Card Industry Data Security Standards.

III. EFFECTIVE DATE

September 1, 2017

IV. APPLICABILITY

This policy applies to all departments, faculty, employees, students and contracted personnel that collect, maintain or have access to credit card information on behalf of the university.

V. RESPONSIBILITY

Policy Responsible Office: Office of Technology

Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

Cardholder Data Environment (CDE) refers to people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

PCI DSS stands for Payment Card Industry Data Security Standard, and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

VII. PROCEDURES

1. All equipment that is involved in the CDE must be maintained in a secure environment appropriate for the device (e.g., Servers should be located in locked cabinets within data centers, POS devices should be properly secured behind locked doors after working hours, paper containing cardholder data should be stored in locked drawers or safes when not in use, etc.).
2. All equipment that is connected to the CDE must have an affixed asset tag that maps the equipment to an inventory control list and a tamper-resistant seal.
3. Implicit management approval must be granted for access to the data center or other secure areas. Such access shall be based on individual job function.
4. Individual authorization and access mechanisms to the data center or other secure areas must be revoked immediately upon termination.
5. The data center must limit access via badging, lock, or some other management approved security. Logs (electronic or paper) of ingress to the center must be maintained.
6. Authorized Personnel entering the data center or other secure areas must be badged or easily distinguished from the public.
7. Visitors to the data center or secure areas must be escorted by authorized employees at all times while in the secure area.
8. Restrict physical access to CDE network jacks, wireless access points, and routers. Unless in use, switch and router ports will be disabled or physically secured to prevent unauthorized connections.
9. Audit logs showing access to data center or other secure areas must be retained for at least 1-year.
10. Physically secure all paper and electronic media that contain cardholder data. "Working documents" containing cardholder data must be stored in a safe or approved storage facility when not actively being used.
11. Equipment used for receiving or processing cardholder data must be secure when not in use.
12. All sensitive and credit card data must be kept secure at all times.
13. Data centers must utilize cameras and electronic controls to protect devices and facilities.
14. Review of logs and camera systems shall be completed periodically and at least on a monthly basis.
15. Procedures must be in place and personnel trained to ensure device physical security.
16. PCI-designated employees and/or contracted personnel must utilize the Daily Credit Card Machine Checklist which includes checking for simple abnormalities (e.g., a missing screw or seal, extra wiring, newly connected USB devices, etc.).

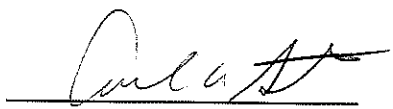
VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy will be considered a Group I infraction under the University Personnel Manual and

is subject to disciplinary action, up to and including dismissal. In addition, some violations may constitute criminal offenses under local, state or federal laws.

IX. EXCLUSIONS
NONE

X. INTERPRETATION
The Office of Technology CIO has the authority to interpret this policy.

APPROVAL TO PROCEED:  **DATE:** 8/11/17

APPENDICES

Daily Credit Card Machine Checklist

Auburn University at Montgomery PCI Terminal Security/Tamper Inspection Checklist

Check each terminal against the characteristics listed below.	Café 1		Café 2		Café 3		Coffee Shop		C-Store	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
Are there any obvious signs of tampering to the terminal?										
Is the terminal in its usual location?										
Is the manufacturer's name correct?										
Is the model number correct?										
Is the printed serial number correct?										
Is the tamper proof seal in tact?										
Are the color and general condition of the terminal as described with no additional marks or scratches? (especially around the seams)										
Are all connections to the terminal as described, using the same type and color of cable?										
Does the number of connections to the terminal agree with what is expected?										
Are all displays or other merchandising within the vicinity of this terminal as described, with no additional boxes or display materials near the terminal?										
Is the condition of the ceiling above the terminal the same as described, with no additional marks, fingerprints or holes?										
Is the total number of terminals in use the same as the number of terminals officially installed?										
Where surveillance cameras are in use, is the total number of cameras in use the same as the number of cameras officially installed?										

If "No" is checked for any of the questions, do not use the terminal and immediately contact a cafeteria manager and ITS (Robert Adams - ext 3465 or radams6@aum.edu).