INDEX

I. PURPOSE

II. APPLICABILITY

III. AUTHORITY AND RESPONSIBILITIES
   A. Card Processing Authority within the University of Maine System
   B. Credit Card Coordinator Responsibilities
   C. Merchant Department Contact Responsibilities

IV. SERVICE PROVIDER SOLUTIONS AND PROCESSES
   A. E-Commerce and Software Solutions
   B. Credit Card Processing Solutions
   C. Outsourced Merchant Accounts
   D. Mobile Device Solutions

V. PROCESSING CARD TRANSACTIONS
   A. Processing Payments
   B. Settlement, Transmission, Reconciliation, and Chargeback Responsibilities

VI. SECURITY PROCEDURES FOR PROCESSING, TRANSMITTING, STORING, AND DISPOSING OF CARD DATA

APPENDIX I - Definitions

APPENDIX II - Overview of TouchNet Credit/ACH Solutions

APPENDIX III - Approved Credit Card Service Providers

APPENDIX IV - Inspection of Equipment

APPENDIX V - Employee Acknowledgment Form - Credit/Debit Card Responsibilities
I. PURPOSE

This APL establishes procedures and requirements for University of Maine System (UMS) departments accepting payments by credit/debit card, including information about:

- Safeguarding personal cardholder information provided to the UMS, or its vendors on behalf of the UMS, to protect against theft or other misuse of the data; and
- Complying with the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

This APL will be reviewed at least annually and will be revised as appropriate to stay current with changes in the business and regulatory environment.

II. APPLICABILITY

This APL applies to all departments, individuals, and entities (including contracted third parties) involved in acceptance of credit/debit card payments on behalf of the UMS.

This APL applies to processing solutions where a UMS credit card merchant is used as well as point of sale (POS) or e-commerce solutions where the UMS pays a fee for use of a vendor’s credit card merchant account.

III. AUTHORITY AND RESPONSIBILITIES

A. Card Processing Authority within the University of Maine System

1. Each campus chief financial officer will designate an employee to coordinate all credit/debit card processing for their campus (Credit Card Coordinator). Any UMS department wishing to begin acceptance of credit/debit cards must have the approval of their respective Credit Card Coordinator who will communicate the request to the UMS Director of Finance and Controller (Controller) or designee.

2. The Controller’s Office and University Services: IT (US: IT) will assist the campus and department in determining the best solution for the business need.

3. Every department that processes credit/debit cards, or desires to do so, must identify a contact (Merchant Department Contact). See section III-C for related responsibilities. When a new merchant identification number (Merchant ID) is required, the Controller or designee will request the number from the UMS merchant acquirer (e.g., Global Payments). Establishment of a merchant ID with any merchant acquirer without the written approval of the Controller is prohibited.
B. **Credit Card Coordinator Responsibilities**

1. Each Credit Card Coordinator will maintain a list of:
   - All campus merchant IDs and Merchant Department Contacts.
   - As provided by Merchant Department Contact, an inventory of all devices to include the make, model, serial number, and location of each device.
   - Employees who are authorized to use the respective devices.

2. The Credit Card Coordinator will provide an updated list to the Controller whenever changes occur regarding items in the first two bullets.

3. Each Credit Card Coordinator will distribute this APL to all Merchant Department Contacts upon assignment to the position. The Credit Card Coordinator will also ensure that all employees (including temporary employees and students) involved in credit/debit card transactions have taken PCI training and understand the requirements and their related responsibilities on an annual basis. PCI training is available online. A form at Appendix V is provided for this purpose. The campus may use an alternate form or process provided it accomplishes the same objectives as this form.

4. The Credit Card Coordinator, campus department staff, and appropriate University Services staff will work together to ensure that card processing equipment and/or software integrates with third party vendors, the general ledger, and existing software systems. The Credit Card Coordinator will work with campus departments and IT staff to determine which networks are authorized for the placement of credit card processing equipment.

C. **Merchant Department Contact Responsibilities**

1. Each Merchant Department Contact will maintain an inventory of all devices to include the make, model, serial number, and location of each device and will provide this inventory to the Campus Credit Card Coordinator whenever changes occur. Each merchant contact will maintain a list of employees who are authorized to use the respective devices and will provide this list to the Campus Credit Card Coordinator at least annually.

2. The Merchant Department Contact will ensure that all devices (e.g., credit card terminals, cash registers, computers, card readers) used in the processing of cardholder data are labeled with:
   - Campus initials (e.g., UM, USM),
   - Department or Campus Credit Card Coordinator name or Merchant Department Contact Name,
   - Merchant ID(s), and
   - Department Name.
3. The Merchant Department Contact will be responsible for ensuring proper procedures are in place including security (complete list in Sections V and VI), timely settlement, transmission, and reconciliation of transactions.

4. The Merchant Department Contact will be responsible for ensuring merchant compliance with Global Payments Card Acceptance Guide (see section IV-A.1) in this APL, APL VI-C Employee Protection of Data, UMS Policy Section 901 - Information Security, and the Payment Card Industry Data Security Standard (PCI DSS).

5. The Merchant Department Contact must notify the Campus Credit Card Coordinator and the Controller prior to making any changes in their method of credit/debit card processing.

6. The Merchant Department Contact must notify the Campus Credit Card Coordinator and the Controller when credit/debit card processing is no longer required. The Controller will then notify the merchant acquirer; otherwise, the merchant acquirer will continue to charge monthly maintenance fees even though the account is inactive.

IV. SERVICE PROVIDER SOLUTIONS AND PROCESSES

A. E-Commerce and Software Solutions

1. When enabling the acceptance of credit and/or debit card transactions over the internet, the UMS’ policy is to use a designated third-party electronic payment system provider to gather card information. The provider may be linked from existing UMS web sites and shall serve as the secure remote repository of cardholder information.

2. The UMS has engaged TouchNet to provide e-commerce solutions, including secure processing and secure hosting of electronic payment information. TouchNet has partnerships with many vendors, called TouchNet Ready Partners, who provide applications that may be beneficial for various UMS related services. Information about these TouchNet Ready Partners may be found at: http://www.touchnet.com/prod/touchnet-ready-program.html. In addition, to learn more about these solutions, you may refer to the Overview of TouchNet Credit Card/ACH Solutions provided at Appendix II.

3. Merchants will process payments on behalf of others using computers attached to the campus PCI Compliant Network, with access limited to only those sites necessary for completing the payment process.
4. When an area is considering initiating e-commerce activity, the responsible person must contact US: IT to review and understand current solutions and to evaluate options. For example, the manner in which the provider’s web site is linked from the UMS web site determines the potential risk, the costliness of the protections, and the level of assessment (SAQ). Acquisition and use of e-commerce solutions other than existing TouchNet provided applications may require a business case following the guidelines described in APL VI-A (Business Case Process for Information Technology Projects).

5. All new e-commerce solutions will require review and written approval by the UMS Chief Information Officer (CIO) and the UMS Chief Information Security Officer (CISO) to determine compliance with the Payment Card Industry Data Security Standard (PCI DSS). Upon approval, the Controller will be informed so that a complete inventory can be maintained.

B. Credit Card Processing Solutions

1. When using a point of sale software solution, the use of a service provider is required to process the payment. Internal software applications (including web-based administrative access to applications) will not be developed, and third-party applications will not be modified in house.

2. A credit card service provider is a business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This includes companies that provide other services that control or could impact the security of cardholder data and also includes outsourced merchant providers. Approved Credit Card Service Providers are provided at Appendix III.

3. A university department may only contract with approved credit card service providers included in Appendix III; an updated list is maintained by the Office of Information Security. If a department is able to demonstrate that another service provider is preferable, the department must provide this information to and obtain the approval of the UMS CIO and CISO prior to entering into any contract with an alternative service provider.

4. Before engaging with a credit card service provider, server-based software applications or point of sale (POS) systems (i.e., cash registers, event ticket distribution) that collect and transmit credit card data, proper due diligence must be done to ensure compliance with the Payment Card
ADMINISTRATIVE PRACTICE LETTER

SUBJECT: CREDIT/DEBIT CARD STANDARDS

Industry Data Security Standard (PCI DSS) and must also be determined to comply with the Payment Application Data Security Standard (PA DSS).

5. Departments doing business with a credit card service provider must have a written agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data in its possession. Information about which PCI DSS requirements are managed by the service provider and which are managed by the merchant must be understood and documented.

6. Service providers involved in processing, transmitting, or storing cardholder data must acknowledge, in writing, their responsibility for securing the data and must be required to provide, and must provide, PCI DSS compliance evidence annually.

C. Outsourced Merchant Accounts

1. An outsourced merchant provider is a business entity that provides a payment, point of sale or e-commerce solution and also provides use of its credit card merchant for a fee, making a university credit card merchant account unnecessary.

2. The use of an outsourced merchant account may reduce the University’s scope, however it does not eliminate the requirement of being PCI compliant. The merchant would still need to address their people and processes internally and all technology used to connect to or transmit to the cardholder data environment.

3. Continue to address policies and procedures for cardholder transactions and data processing.

   • Protect cardholder data when you receive it, process charge backs and refunds.
   • All applications and card payment terminals must comply with respective PCI standards and not store sensitive cardholder data. Requesting a certificate of compliance annually from the outsourced merchant should be practiced.
D. Mobile Device Solutions

When using a mobile payment solution, special considerations are needed to ensure the security of data. US: IT must evaluate any proposed solution to ensure proper implementation.

1. Mobile payment vendors may allow the use of the vendor’s Merchant ID in lieu of a UMS Merchant ID. If not properly implemented, this may add significant complexity to UMS’ PCI compliance requirements.

2. Hardware is required to meet P2PE-HW compliance standards in order to permit payment transactions to transit the UMS wireless network.

3. When using mobile payment peripheral technology (e.g., Square, PayPal Here), US: IT must ensure the hardware will be properly integrated with a UMS owned and maintained mobile device (e.g., iPad, Android phone). The resulting system will be dedicated to the processing of payments and until such time as the solution is certified for P2PE-HW encryption, no transactions will traverse the UMS wireless network but will employ third-party cell-based service.

V. PROCESSING CARD TRANSACTIONS

A. Processing Payments


2. In-Person (Card Present) Transactions:

   When the card and card holder are present, employees or applicable vendors will:
   - Always swipe the card through the terminal/point of sale device, if applicable. If the card cannot be read by the terminal, input information manually.
   - Obtain authorization for every card sale via the terminal.
   - Obtain the signature of the cardholder.
• Compare the last four digits of the account number on the credit card to the four digits of the account number displayed on the terminal to ensure they match.
• Compare the name and signature on the card to those on the signed transaction receipt generated from the credit card terminal/point of sale device.

3. Phone (Card Not Present) Transactions:
   When card information is taken over the phone, employees or applicable vendors will:
   • Obtain the cardholder name, billing address, shipping address (if applicable and different from billing address), card account number, and card expiration date.
   • Verify the customer’s billing address either electronically (by entering the zip code in the POS device) or by calling the credit card automatic phone system (Address Verification System (AVS)).
   • Request the CVV number (the four digit code on the front or three digit value on the back of the card) and validate the code at the time of authorization either electronically (through the POS or virtual terminal device) or by calling the credit card automated phone system. This code must be crosscut shredded, incinerated, or pulped, such that there is reasonable assurance the hardcopy materials cannot be reconstructed once validated; it must not be stored physically or electronically.
   • Process the payment through the terminal as outlined above, properly securing or crosscut shredding, incinerating, or pulping, such that there is reasonable assurance the hardcopy materials cannot be reconstructed and any notations made on paper as soon as approval is received via terminal.

B. Settlement, Transmission, Reconciliation, and Chargeback Responsibilities

1. On a daily basis, units will settle and forward properly encrypted credit card data to the UMS’s merchant acquirer. On a daily basis, units will also finalize and ensure proper posting of all card transactions to the UMS’ general ledger and subsidiary systems (i.e., student accounts) if appropriate.
2. Each Merchant ID activity will be timely reconciled to the general ledger and related subsystems. Any issues will be immediately communicated to the Controller.
3. Credit card receipts shall be electronically received into a designated campus specific bank account. Nightly, the bank sweeps these account balances into the UMS’ general operating account. Each campus should review bank activity daily to ensure activity is reasonable and unusual transactions are
researched and resolved immediately. Bank reconciliations may be performed
daily but, at a minimum, must be performed monthly.

4. When a customer contests a charge, the customer’s issuing bank will forcibly
initiate a chargeback, or return of funds, from the UMS to the customer. The
UMS may also reverse a transaction. UMS personnel must timely post entries
to subsidiary systems, as applicable, and the general ledger to reflect
chargebacks and reversals. Such posting will be for the daily amounts to ease
reconciliation and aid in researching transaction history.

VI. SECURITY STANDARDS FOR PROCESSING, TRANSMITTING,
STORING, AND DISPOSING OF CARD DATA

Each department that accepts credit and/or debit card payments shall have appropriate
procedures for securely processing and disposing of credit card information. Procedures
must be in place to comply with this APL, APL VI-C Employee Protection of Data, UMS
Policy Section 901 - Information Security, and the Payment Card Industry Data Security
Standard (PCI DSS). Procedures are to be developed from the list of standards below, not
considered to be an all-inclusive list, which must be followed to achieve compliance with
PCI DSS depending on the individual circumstances of each merchant.

1. If a credit card swipe terminal is used, a dedicated phone line or internet
connection to the campus PCI Compliant Network is required.

2. If an internet based virtual terminal method is used, a dedicated workstation
is required, connected to the campus PCI Compliant Network, with internet
access limited to sites necessary for credit card processing. Contact the
appropriate campus IT department for setup assistance.

3. Computers or kiosks, provided specifically for student or customer use for
making credit card payments, must be connected to the campus PCI
Compliant Network, with internet access limited to sites necessary for credit
card processing and those sites related to the intended use. General internet
availability is prohibited on this type of computer. Contact the appropriate
campus IT department for setup assistance.

4. Wireless capability must be disabled on any device used for manual entry of
credit card transactions. All computers used for virtual terminal processing
must use a wired connection. If the campus determines that wireless
communications are needed, then approval is required as with all critical
technologies in accordance with the next paragraph.

5. If use of critical technologies, such as remote access, wireless technologies,
removable electronic media, laptops, tablets, email or internet usage, are
needed in the cardholder data environment, written approval by the CIO and
the CISO is required. Requests require a description of the purpose and acceptable use, inventory of devices in scope, list of authorized users, means of authentications (e.g., ID and password), and specific placement on the network, usage policies, and a statement on how PCI requirements surrounding these types of devices are to be met. Requests for remote access, including remote access for vendors or business partners, will meet requirements for remote access below.

6. Sensitive cardholder data (everything at the end of a red arrow in the diagram below is sensitive cardholder data). Anything on the back side and CID (American Express) shall not be stored on any UMS computer, server, or removable electronic media (e.g., thumb drives, CDs, external hard drives). Onsite electronic storage of sensitive cardholder data is prohibited.

7. Paper documentation, containing sensitive cardholder data, shall be kept only as long as required to complete the credit card transaction. Responsible personnel shall crosscut shred, incinerate, or pulp all sensitive cardholder data immediately upon processing. In rare circumstances where storage of paper documents containing card information is necessary, UMS personnel shall store such documents in locked files and/or locked work areas until destruction, and shall maintain the documents only for as long as there is a business, legal or regulatory requirement. In these extenuating circumstances, documentation regarding reason and timeframe or event that would end storage shall accompany the records. Under no circumstances shall card validation values (CVV) or personal identification numbers (PIN) be stored in any form for any reason. Any department needing to retain cardholder data must establish clear written retention and destruction practices and obtain approval from the Campus Credit Card Coordinator and Controller.
8. All physical cardholder data, that is no longer deemed necessary or appropriate to store, must be properly destroyed. Proper destruction of documents requires a process, such as cross-cut shredding, incinerating, or pulping, making reconstruction of the data impossible. Storage containers used for materials that contain information to be destroyed must be properly secured.

9. Any stored paper documents containing cardholder data must be stored in such a way that the documents can be easily inventoried and a detailed inventory of the data is required at least quarterly.

10. Employees must obtain Credit Card Coordinator approval prior to relocating any stored paper documents containing cardholder data to another storage location or to any outside entity.

11. If cardholder data is received in person, by phone, or in the mail in an area that does not have access to credit card processing and must be transferred to another employee for processing, such data must not be left unattended or unsecured. When transferred to another employee for processing, it must be marked as “Confidential” and delivered personally or by secured courier service. Cardholder data must not be transferred to other individuals via end user messaging technologies, such as email or instant messaging. Encrypted messaging is prohibited when it would result in electronic storage of cardholder data by the UMS. Cardholder data must not be sent by campus mail, or by a non-trackable mail service. Campus Credit Card Coordinator approval must be obtained if a department wishes to accept credit card payments where credit card information must be transferred in this manner.

12. If a UMS merchant scans paper forms that contain cardholder data into an imaging or other system, the account number must be removed from the document or rendered unreadable prior to scanning. If the cardholder also provided a CVV and/or PIN, these must be removed or rendered unreadable as well.

13. Access to documents containing cardholder data must be limited to only those employees who have a legitimate business need to access them based on job classification and function.
14. Cardholder data must be transmitted securely (e.g., encrypted). UMS personnel, or vendors operating on its behalf, may not request or submit cardholder information via email or instant messaging. Should such information be received by email, or instant messaging, the items shall be retrieved and processed as soon as possible, hardcopies properly destroyed, all data removed from the email system and the “trash cans” emptied and purged from computer systems, (deleting alone is not sufficient). Contact IT for assistance. The UMS personnel or vendor shall advise the sender of appropriate ways to make any future payments, taking care to exclude any cardholder information in any response.

15. Should UMS personnel erroneously come into contact with credit card data in any form (e.g., paper, electronic), he or she should handle the information professionally and expeditiously. If the intended recipient is indicated or known, that employee should be contacted and the information transferred securely. If the intended recipient is not known, the Campus Credit Card Coordinator should be contacted.

16. Credit card processing equipment must mask the primary account number (PAN) by truncating all but the last four digits of the cardholder account number on customer receipts and reports retained by the UMS.

17. When hiring an employee whose job responsibilities will include having access to cardholder data, the UMS must perform appropriate background checks in accordance with UMS Policy Section 415 – Employment Background Screening and associated Human Resources procedures. Such background checks will include criminal and possibly credit checks, as appropriate, depending on the circumstances. The Merchant Department and Campus Credit Card Coordinator shall make this determination, seeking advice from Human Resources and the Controller, where appropriate. Consideration should be given to a number of factors, including the responsibilities, access, and volume of card activity related to the position for which the candidate is applying.
18. Any person authorized to handle credit card transactions will be assigned a unique ID on any device or database involved in processing, storing or communicating cardholder data. Strict control should be maintained over the addition, deletion, and modification of user IDs, credentials and other identifier objects. Use of shared IDs is prohibited. Access must be restricted to the least privileges required to perform the necessary job responsibilities.

19. If a security incident is suspected, follow the steps detailed in APL VI-B Information Security Incident Response with the first action to report the incident to IT. The Office of Information Security maintains specific procedures in the event of a payment card related incident.

20. Each Merchant Department will perform an annual risk assessment to identify threats and vulnerabilities to overall merchant security and address the results of this assessment as appropriate. This will include completing the PCI DSS Self-Assessment Questionnaire (SAQ).

21. All computer systems that process, transmit, or store cardholder data must have an external vulnerability scan done at least quarterly. Merchant Departments are responsible for scheduling required scans using the TrustKeeper system. PCI DSS requires four quarters of passing scans. Hence, remediation actions and re-scans are required until the system passes.

22. All computer systems that process, transmit, or store cardholder data must have anti-virus mechanisms that are up-to-date, actively running, and generating audit logs. The Merchant Department is responsible for ensuring compliance, consulting with campus IT as needed.

23. Users who access computer systems that process, transmit, or store cardholder data must follow the password standards described in the UMS Policy Section 901 – Information Security Policy and Standards for creating, protecting and changing passwords.
24. Any remote access into networks and devices involved in the processing of credit card information must be encrypted (e.g., SSH, VPN, or TLS) and automatically disconnect after 10 minutes of inactivity. Copying, moving, or storing of cardholder data onto any media is prohibited under any circumstance including during remote access. Remote access to devices or networks involved in processing credit card information will be granted only as needed to vendors or business partners for proper maintenance and ongoing operation of equipment. UMS personnel responsible for the vendor relationship or providing the access must immediately deactivate such access after use.

25. All computer system components that process, transmit, or store cardholder data must have vendor supplied security patches installed within three months of release. Critical patches must be installed within one month of release.

26. The Merchant Department Contact will develop procedures to periodically inspect devices surfaces to detect equipment substitution or tampering, such as addition of card skimmers or other added hardware that could be used to exfiltrate data.

This Administrative Practice Letter has been approved by the Treasurer of the University of Maine System.

Related Documents
- APL VI-A Business Case Process for Information Technology Projects
- APL VI-B Information Security Incident Response
- APL VI-C Employee Protection of Data
- APL VII-A University of Maine System Purchasing Procedures
- UMS Policy Section 415 - Employment Background Screening
- UMS Policy Section 901 - Information Security Policy and Standards
- Global Payments Card Acceptance Guide
- Payment Application Data Security Standard
- Payment Card Industry Data Security Standard (PCI DSS)
- PCI Security Standards Council Homepage (https://www.pcisecuritystandards.org/)
APPENDIX I - Definitions

Address Verification System (AVS): A system which verifies a cardholder's address and zip code (entered at the time of the transaction) to information stored at the issuing bank.

Card Validation Value (CVV) or Code: There are two types of codes. The first one is for the data element on a card’s magnetic stripe to reveal any alternation or counterfeiting. The other is the unique code associated with each individual credit or debit card that ties the card account number to the plastic. This code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit un-embossed number printed above the card number on the face of all payment cards. More specifically, the code names by card network are:
  - CID Card Identification Number (American Express and Discover payment cards)
  - CAV2 Card Authentication Value 2 (JCB payment cards)
  - CVC2 Card Validation Code 2 (MasterCard payment cards)
  - CVV2 Card Verification Value 2 (Visa payment cards)

Cardholder Data: Full magnetic stripe or the Primary Account Number (PAN) plus any of the following:
  - Cardholder name
  - Expiration date
  - Service Code

Code 10: A Code 10 authorization request alerts the credit card issuer to suspicious activity, without alerting the customer. During a Code 10 call, a person processing a credit card transaction will call the authorization center and, in a normal tone of voice, ask for a Code 10 authorization. By doing so, you put the center on alert without letting the customer know you are suspicious. The operator will ask questions and provide instructions on any necessary action. This type of authorization request may result in a call to law enforcement.

Convenience Fee: Is a fee charged in addition to the original transaction amount for the privilege of being able to use an alternate payment method. This fee is payable to the third-party providing the payment mechanism.

Credit Card: A card issued by a financial institution to access a line of credit. Visa, MasterCard, American Express and Discover all issue credit cards.
Debit Card: A card issued by a financial institution to directly access a demand deposit account (DDA). There are two types:

- **Online** – requires a Personal Identification Number (PIN) or Point of Sale (POS).
- **Offline** – has Visa or MasterCard logo and processes the same as a credit card transaction.

**Electronic Payment System Provider (EPSP):** A third party (e.g., TouchNet, Paytrace, Plug’n Pay) who the UMS has contracted with to provide services including secure processing and the secure hosting of electronic payment information.

**Merchant Identification Number:** The unique number assigned to credit card processing units - either software packages or terminals. This number accompanies the financial credit card transaction throughout processing by financial institutions and third party vendors.

**Merchant Acquirer or Acquiring Bank:** Bankcard association member (e.g., Global Payments, Vision Payment Solutions, and Bank of America Merchants) that maintains relationships with merchants for the purpose of acceptance, clearing, and settlement of the merchant’s credit or debit card sales.

**P2PE-HW:** Point-to-point Encryption (P2PE) applies to merchants who process cardholder data only via hardwire payment terminals included in a validated and PCI SCC-listed Point-to-Point Encryption (P2PE) solution. SAQ P2PE-HW merchants do not have access to clear-text cardholder data on any computer system and only enter account data via hardware payment terminals. Merchants who fall under P2PE-HW may be either card-present or card-not-present merchants.

**Payment Card:** A payment card can be a credit card (i.e., Visa, AMEX, MasterCard, Discover) or a debit card.

**Payment Card Industry Data Security Standard (PCI DSS):** The PCI DSS is a set of comprehensive requirements for enhancing payment account data security, developed through a collaborative effort by Visa, MasterCard, and other payment brands. The purpose is to help facilitate the broad adoption of consistent data security measures on a global basis and includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. Since June 30, 2005, any entity who stores, processes, transmits, or comes into contact with cardholder data, is required to be PCI compliant. Information about PCI requirements may be found at [https://www.pcisecuritystandards.org/index.shtml](https://www.pcisecuritystandards.org/index.shtml)
Point of Sale (POS) System: POS systems use computers or specialized terminals that are combined with cash registers, bar code readers, optical scanners, and magnetic stripe readers for accurately and instantly capturing sales transactions and maintaining inventory records.

PCI DSS Self-Assessment Questionnaire (SAQ): is a validation tool for merchants and service providers that are not required to undergo an onsite data security assessment per the PCI DSS Security Assessment Procedures. The purpose of the SAQ is to assist organizations in self-evaluating compliance with the PCI DSS, and organizations may be required to share it with their acquiring bank. Each SAQ includes a series of yes-or-no questions about the organization’s security posture and practices. The SAQ allows for flexibility based on the complexity of a particular merchant’s or service provider’s business situation.

Primary Account Number (PAN): is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called an Account Number.

Sensitive Cardholder Data: Protected information (e.g., PAN, expiration date, CID (American Express only), chip information, magnetic stripe data track 1 and 2, and security code) which when held in possession of a person other than the owner of the card would permit unauthorized use.

Service Code: Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.

Service Provider: Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS, and other services as well as hosting providers and other entities. Entities, such as telecommunications companies, that only provide communication links without access to the application layer of the communication link are excluded.

Virtual Terminal: A web-browser based access to a processor or third party service provider website that allows manual entry and authorization of credit card transactions.
APPENDIX II – Overview of TouchNet Credit Card/ACH Solutions

TouchNet provides the UMS with three different web-based tools for processing credit card and ACH payments. TouchNet has been acquired by the System to provide secure payment methods and facilitate compliance with the Payment Card Industry Data Security Standard (PCI DSS) for protecting customers’ credit card data. All applications are maintained in the TouchNet datacenter. No credit card data is stored on UMS servers when TouchNet is used to process the transactions.

1. **TouchNet Marketplace uStores:** TouchNet Marketplace uStores enable campuses to build and operate secure, web-based shopping cart applications without expensive programming costs. It combines the online storefronts with inventory control, order fulfillment, and reporting. It facilitates secure payment with credit card or web-check ACH.

2. **TouchNet Marketplace uPay:** TouchNet Marketplace uPay is a web application that UMS departments can use for customers to make secure one-time or recurring payments that are connected to existing web applications and web sites. Customers are transferred to the secure TouchNet uPay site to make a secure payment and transferred to a specified web page upon completion.

3. **TouchNet Payment Gateway Operation Center:** The TouchNet Payment Gateway Operation Center (TPG) provides a facility for staff members to process online credit card transactions for payment requests taken by mail or phone. The TPG is also the tool used to manage and report on payments processed through uStores and uPay described above.

Computers used to process the payments on behalf of others using any of these options must be connected to the campus PCI Compliant Network, with internet access limited to only those sites necessary for completing the payment process.

Requests for further information or implementation of a TouchNet application for your department should be directed to your Campus Credit Card Coordinator. The current Coordinators by campus are located in the UMS Portal under Information Security:
APPENDIX III – Approved Credit Card Service Providers

Listed below are the University of Maine System’s approved credit card service providers.

A university department may only contract with a service provider on this list. If a department is able to demonstrate that another service provider is preferable, the department must provide this information to and obtain the approval of the UMS CIO and CISO prior to entering into any contract with an alternative service provider.

**UMS Approved Credit Card Service Providers**

- TouchNet Information Systems
- Paytrace Payment GatewayGlobal Payments – Global Transport
- Verifone
- Plug’n Pay
- Beanstream
- PayPal

*(New providers may be found on the UMS Portal under Information Security.)*

**UMS Approved Vendor Merchant Providers**

- TouchNet Information Systems – PayPath
- Ticket Turtle, Inc.
- Vendini, Inc.
APPENDIX IV – Inspection of Equipment

Inspection of devices provides timely detection of tampering or replacement. Specifically, physical inspection of the devices’ surfaces can identify unauthorized additions, such as card skimmers, inline key-logging, or hidden cameras/recording devices.

Likewise, it is important to be sure that the entire device has not been substituted. Conducting a proper inventory that records the make, model, and serial number of each device is important.

Procedures that include regular inspections need to be developed and employed. The frequency of the inspection depends on the exposure of the device to the public. Such procedures should include verifying the identity of persons claiming to be repair or maintenance personnel and reporting of suspicious activity.

Some items to check for:
- Check the area for cameras that might perform electronic “shoulder surfing.”
- Pull on the card slot/swipe area to be sure there is not an unauthorized add on.
- Wiggle the keypad to be sure that a fake keypad has not been added on top.
- Check for added wires or components.
- Check to be sure the device is the inventoried device.

Methods to take to improve checks:
- Compare with photographs of devices in original configuration.
- Use a secure marker pen, such as a UV light marker to mark surfaces.
- Use tamper-event stickers/seals.
- Use non-removable inventory stickers.
APPENDIX V - Employee Acknowledgment Form - Credit/Debit Card Responsibilities

Employee Name: ____________________________________
Supervisor’s Name: ____________________________________
Merchant Department Contact: ________________________
Department:  ____________________________________
Campus:  ____________________________________

Purpose:

This form provides documentation that the above named employee has reviewed the training on Credit/Debit Card Standards (available at: www.courses.maine.edu) and understands the compliance responsibilities related to their job functions. Where the employee has questions or concerns, the employee has communicated with their supervisor, the Campus Card Coordinator, and/or System personnel to reach resolution.

Employee Certification:

I, ____________________________, certify that I have reviewed the Credit/Debit Card Standards and related documents and understand my compliance responsibilities. I have reported any concerns to my supervisor, Campus Card Coordinator, and/or appropriate System personnel so that any issues may be addressed. I understand the sensitive nature of the information to which I have access and my responsibilities to keep this information private and secure.

__________________________ _____________
Signature    Date

Note: This completed form will be retained by the Campus Card Coordinator responsible for the Merchant ID for which the above named employee has access. Forms will be kept on file for three years to document that employees have been informed about their PCI DSS related responsibilities and other associated information. Auditors or members of management with PCI responsibilities may review the information periodically to ensure University of Maine System’s obligations in this area are met.