Payment Card Industry (PCI) Compliance Policy

Summary

The purpose of this policy is to help prevent loss or disclosure of credit card customer information, including credit card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and the university.

Policy Statement

The University at Buffalo (UB, university) complies with the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS is a mandated set of requirements agreed upon by the major credit card brands (e.g., Visa, MasterCard, Discover, and American Express) to protect credit card data, regardless of where that data is processed or stored. Everyone in the UB community must adhere to these standards to protect our customers and to continue to process payments using payment cards.

The university complies with the current version of the PCI DSS at all times. All card handling activities and related technologies are required to comply with the PCI DSS in its entirety. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI DSS.

The university prohibits the retention of complete payment card primary account numbers (PAN) or sensitive authentication data in any university system, database, network, computer, tablet, cell phone, or paper file. The storage of truncated numbers, in approved formats (first six digits OR last four digits), is permissible.

Details regarding allowable use of credit card data and security requirements are found in the Credit Card Handling Chart.

At no time will the requirements of the PCI DSS supersede local, state, and federal laws or regulations.
Payment Card Industry Data Security Standards (PCI DSS) V3.2
The following is the complete list of the PCI DSS compliance requirements.

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td>Network and Systems</td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability</td>
<td>5. Protect all systems against malware and regularly update antivirus software or programs</td>
</tr>
<tr>
<td>Management Program</td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td>Control Measures</td>
<td>8. Identify and authenticate access to system components</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td>Networks</td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
<tr>
<td>Security Policy</td>
<td></td>
</tr>
</tbody>
</table>

The university is required to comply with all relevant standards. However, not all of the PCI DSS requirements are relevant to UB. The university has implemented various policies that reduce the compliance scope, including prohibiting storage of credit card information electronically, restricting transmission through fax and email, and utilizing third-party vendors for web based credit card processing rather than university networks.

Background

The PCI DSS is a mandated set of requirements agreed upon by the six major credit card companies: VISA, MasterCard, Discover, American Express, Diners Club International, and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants or organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org)

In order to accept credit card payments and avoid penalties, the university must comply with the PCI DSS. UB’s PCI Compliance Policy and additional supporting policies (See Related Information) provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions. This is done in order to reduce the institutional risk associated with the administration of credit card payments by university departments and to promote proper internal control and compliance with the PCI DSS.
Applicability

UB’s PCI Compliance Policy applies to those involved with payment card handling including: faculty, staff, students, third-party vendors, individuals, systems, networks, and other parties with a relationship to the university including auxiliary service corporations, alumni associations, student associations and governments, Research Foundation (RF), UB Foundation (UBF) and any unit using third-party software to process credit card transactions. This includes transmission, storage, and processing of payment card data, in any form (electronic or paper), on behalf of UB.

Definitions

Cardholder
Someone who owns and benefits from the use of a membership card, particularly a credit card.

Cardholder Data (CHD)
Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date, and the Service Code.

Cardholder Name
The name of the Cardholder to whom the card has been issued.

CAV2, CVC2, CID, or CVV2 data
The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-present transactions.

Disposal
CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes and USB storage devices in accordance with the Record Retention and Disposition Policy. The approved PCI DSS disposal methods are:
- Cross-cut shredding, incineration, approved shredding, or disposal service

Expiration Date
The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

Magnetic Stripe (i.e., track) data
Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

Merchant
Any department or unit (can be a group of departments or a subset of a department) which has been approved to accept credit cards and has been assigned a Merchant identification number.

Payment Card Industry Data Security Standards (PCI DSS)
The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands:
- Visa, MasterCard, American Express, Discover, JCB
PIN or PIN block  Personal Identification Number entered by cardholder during a card-present transaction, or encrypted PIN block present within the transaction message.

Primary Account Number (PAN)  Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

Self-Assessment Questionnaire (SAQ)  The PCI DSS self-assessment questionnaires (SAQs) are validation tools to assist merchants and service providers report the results of their PCI DSS self-assessment.

Sensitive Authentication Data  Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN or PIN block.

Service Code  The service code that permits where the card is used and for what.

Responsibility

All members of the university community
- Safeguard cardholder data.
- Report occurrences of possible incidents and data breaches to your supervisor or UB’s Information Security Officer.
- Review and Comply with the following university policies:
  - UBIT Password Policy
  - Protection of University Data

PCI Compliance Committee
The PCI Compliance Committee is composed of representatives from Financial Management, Information Security Office, Office of the Vice President and Chief Information Officer, Internal Audit, and UB merchants.
- Monitor the university’s compliance with PCI DSS requirements.
- Act as a steering committee for PCI DSS.
- Support PCI DSS compliance efforts.
- Review the required annual SAQ self-assessment.

UB Information Technology (UBIT)
- Maintain security standards as required by PCI DSS.
- Keep current with PCI DSS regulations and make applicable changes to systems and processes as appropriate.
- Consult on technical PCI DSS issues.
- Assist with mandatory annual training sessions.
Financial Management

- Keep current with PCI DSS regulations and make changes to processes, as appropriate.
- Maintain an inventory of all UB schools and departments that process credit card transactions using an approved merchant account, the UBF Checkout, or other compliant methods.
- Provide and monitor annual training that meets the PCI DSS requirements.
- Coordinate the completion of the appropriate annual self-assessment documents (SAQs).
- Collect departmental PCI Procedures as part of the annual SAQs.
- Evaluate compliance to PCI as part of the scheduled cash handling reviews.

Department or Unit Heads (Accepting Credit Card Payments other than through approved online methods)

- Review and comply with the following university policies:
  - Credit/Debit Card Merchant Requirements Policy
  - Safeguarding Cash and Cash Equivalents
- Complete the required annual PCI self-assessment (SAQ).
- Complete the annual PCI Training through Financial Management.
- Require appropriate staff complete the annual PCI Training through Financial Management.
- Maintain departmental PCI procedures and verify staff has an understanding of the procedures and their responsibilities.

Credit and Debit Card Handlers and Processors

- Follow the established cash receipts procedures for the appropriate funding source.
- Complete the annual PCI Training through Financial Management.
- Review and comply with the following university policies:
  - Credit/Debit Card Merchant Requirements Policy
  - Safeguarding Cash and Cash Equivalents

Third Party Payment Card Processors

- Provide confirmation of compliance.

Contact Information

<table>
<thead>
<tr>
<th>Contact</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tricia Canty</td>
<td>716-645-2639</td>
<td><a href="mailto:tscanty@buffalo.edu">tscanty@buffalo.edu</a></td>
</tr>
<tr>
<td>PCI Compliance Committee</td>
<td></td>
<td><a href="mailto:PCI@buffalo.edu">PCI@buffalo.edu</a></td>
</tr>
</tbody>
</table>
Related Information

University Links

Credit/Debit Card Merchant Requirements

Data Access Procedure
http://www.buffalo.edu/ubit/policies/guidance-documents/data-access-procedure.html

Data Governance @ UB
http://www.buffalo.edu/provost/oia/data-governance.html

Data Risk Classification Policy

Safeguarding Cash and Cash Equivalents Policy
http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/safeguarding-cash1.html

Protection of University Data Policy

UBIT Password Policy
http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/ubit-password.html

Disclosure of All Funds Generated Through the Use of University Faculty or Staff Time and/or the Use of University Facilities
http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/disclosure-all-funds.html

Pre-Employment Background Screening (Pilot)
http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/pre-employment-background-screening.html

Forms

Department PCI Procedure Template – pending
Electronic Payment (ePay) Application
eStore New Payment Request - TBD

Related Links

PCI DSS Compliance Guidance for Campuses of the State University of New York
National Institute of Standards and Technology (NIST) 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
New York State Enterprise Information Security Office - Breach Notification
New York State Office of Information Technology Services
New York State Office of Information Technology Services - Information Security Policy
PCI Security Standards Council
Credit Card Handling: State, UBF, RF

<table>
<thead>
<tr>
<th>Don’t</th>
<th>Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t - Store cardholder data unless truncated (first six digits OR last four digits)</td>
<td>Do - Properly destroy all hardcopy forms containing cardholder data (cross cut shred, incinerate or pulp). Placing in a secured bin provided by a disposal service is acceptable.</td>
</tr>
<tr>
<td>Don’t - leave cardholder information unattended on a desk, screen, or in any public area</td>
<td>Do - Physically secure all hardcopy cardholder data pending processing.</td>
</tr>
<tr>
<td>Don’t - Send cardholder data outside of approved areas</td>
<td>Do – Only retain cardholder data received by phone or mail long enough to complete the transaction, then destroy the hardcopy.</td>
</tr>
<tr>
<td>Don’t – Share your user name, password or credentials</td>
<td>Do – Have a unique user name and password for your work and only use it for work purposes, not personal</td>
</tr>
<tr>
<td>Don’t – Install, move, replace or return devices without verification with Financial Management</td>
<td>Do – Restrict access to devices to people duly approved and who need the access for their job.</td>
</tr>
<tr>
<td>Don’t – Use any computer or mobile device to enter cardholder data that is not specifically configured and dedicated to processing payments.</td>
<td>Do – Verify the identity and credentials of all unknown persons prior to granting them access to modify or troubleshoot devices.</td>
</tr>
<tr>
<td>Don’t – Enter cardholder data online as the customer.</td>
<td>Do – Keep an up to date list of all credit card processing devices and inspections.</td>
</tr>
<tr>
<td>Don’t – Request or send any cardholder data by email, fax, chat, instant message, SMS, or any similar end-user messaging technology.</td>
<td>Do - Report immediately to your supervisor and the Information Security Officer if you suspect tampering with a device or credit card information has been lost, stolen, exposed, or otherwise misused.</td>
</tr>
<tr>
<td>Don’t – Store any contents of the magnetic stripe</td>
<td></td>
</tr>
</tbody>
</table>

If cardholder data is received via Email, Fax or Voicemail – Destroy the sensitive data or message, contact the sender to inform them that this method is not secure, ask for the information over the phone or other compliant and secure media, and let them know we will not accept information sent using this method in the future.

If Financial Management has approved the need for cardholder data to be distributed internally, it must be physically secured. This includes using locked transmittal bags.

PCI questions?

Contact Tricia Canty in Financial Management by email tscanty@buffalo.edu or by phone at (716)645-2639
Or the PCI Compliance Committee by email PCI@buffalo.edu