Payment Compliance Review
Agenda

- Security of Credit Card Data
- Credit Card Procedures
- Review
Security of Credit Card Information
Security of Credit Card Information

- The purpose of the policy is to comply with the Payment Card Industry Data Security Standard (PCI DSS).
  - PCI DSS is regulated by the payment card industry (Visa, MasterCard, etc.)
  - PCI-DSS is not endorsed or enforced by the State of Kansas. We must comply even though it is not a state or federal regulation.
- Compliance with PCI DSS is required of all merchants (i.e. WSU) that process, store or transmit cardholder data.
What Is PCI-DSS

➤ Purposes of PCI-DSS?
  – Promote consistent global security standards.
  – Protect cardholder data from fraud and security breaches.

➤ The Six Objectives of PCI
  – Build and maintain a secure network.
  – Protect cardholder data.
  – Maintain a vulnerability-management program.
  – Implement strong access-control measures.
  – Regularly monitor and test networks.
  – Maintain a written Information Security Policy.
PCI DSS: 6 Goals, 12 Requirements
(Summary of over 200+ Standards for Compliance)

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| 1. Build and maintain a secure network                | 1. Install and maintain a firewall configuration to protect data  
|                                                        | 2. Change vendor-supplied defaults for system passwords and other security parameters                                                   |
| 2. Protect cardholder data                            | 3. Protect stored data  
|                                                        | 4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks                                  |
| 3. Maintain a vulnerability management program        | 5. Use and regularly update antivirus software  
|                                                        | 6. Develop and maintain secure systems and applications                                                                                   |
| 4. Implement strong access control measures           | 7. Restrict access to data to a need-to-know basis  
|                                                        | 8. Assign a unique ID to each person with computer access  
|                                                        | 9. Restrict physical access to cardholder data                                                                                           |
| 5. Regularly monitor and test networks                | 10. Track and monitor all access to network resources and cardholder data  
|                                                        | 11. Regularly test security systems and processes                                                                                         |
| 6. Maintain an information security policy            | 12. Maintain a policy that addresses information security                                                                                  |
PCI-DSS applies to YOU!

- Everyone involved in any part of processing payment-card transactions must understand and follow PCI-DSS.

- We ALL share an interest and a responsibility to protect cardholder data.
Non-Compliance costs include:

- Fines
- Lawsuits
- Investigation, notification and credit-watch expenses
- Loss of reputation and customer confidence
- Loss of ability to accept payment cards

PCI-DSS violations may lead to discipline, including termination.
What is the PCI DSS trying to protect?

What’s in your wallet?

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Magnetic Stripe
- Card Verification Value (CVV)
Covered Data Elements

Standards were written to protect the following data:

1) **Cardholder data**: primary account number, cardholder name, expiration date and security code
   - Storage of cardholder data is permitted as long as stored per standards

2) **Sensitive authentication data**: magnetic stripe, CVV and PIN
   - Storage of sensitive authentication data is NEVER permitted
## Covered Data Elements

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Service code</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiration date</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Sensitive authentication data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Magnetic stripe</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td>PIN/PIN block</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
</tbody>
</table>
Who Must Comply?

Do you or your department collect, store, process or transmit cardholder data?

- Do you COLLECT cardholder data...
  - On paper?
  - Over the internet via a website (referred to as E-Commerce transactions)?
  - Over the phone or through the mail?
  - Enter directly into a PC, Point of Sale, a mobile device, etc.?

- Do you STORE cardholder data?...
  - On paper?
  - In an electronic document (ie. Spreadsheet, word document, etc.)?
  - Temporarily or permanently?

- Do you PROCESS cardholder data...
  - Using any process (software application, hardware, etc.) to process cardholder data?

- Do you TRANSMIT cardholder data...
  - To a third party in an effort to collect payment for goods or services?

IF YOU ANSWERED YES TO ANY OF THE ABOVE QUESTIONS, THEN PCI-DSS APPLIES TO YOU!
Common PCI DSS Myths

“I don’t store credit card numbers, so I have no compliance obligation with the PCI DSS.”

“I only process a few credit card transactions per year, so I am exempt from compliance with the PCI DSS.”

“I only need to be mostly compliant with the PCI DSS.”
Important Steps to Compliance

PCI-DSS requires WSU to **identify** all “payment points”
- “Payment Points” are places where cardholder data is being collected, stored, processed or transmitted.

PCI-DSS requires WSU to **secure** the “payment points”
- Secure the PC and the credit card terminal per PCI-DSS.
- Grant access only to those who are trained in proper credit card procedures per PCI-DSS.
- Connect the “payment points” to a **private credit card network** that is used specifically for credit card processing ONLY.

“Payment points” are connected to a **WSU private network** whose sole purpose is to process credit cards.
WSU Regular Network
These PC’s are not in PCI Scope

WSU Private Credit Card Network
This PC MUST be secured per PCI-DSS

“We can do everything on our regular business machines except process credit cards…”

“All I can do is enter credit card payments on this PC. I can’t read my email or do my regular work duties…”
Which are “payment points” that WSU must secure?

Card Swipe Machine? **YES**

Office Workstations?
**YES** - if entering credit card data. Computer should not be used for ANYTHING else (i.e. email, daily job)

Student in dorm entering his own credit card on his own computer? **NO**

Payment kiosk that department offers?
**YES** - any designated PC for the convenience of making payments.

Computer Lab? **NO** - PCs are for general use not specific for payments.

Phone Transaction Taken on a Laptop?
**YES** - Laptop cannot be wireless.
Credit Card Procedures
Credit Card Procedures

- For a full list of procedures, refer to the "Campus Departments – Credit Card Procedures" document.

- These procedures are for WSU departments currently accepting credit card payments for goods or services.
Location of Security Code for Different Card Types
Credit Card Procedures - Collection

Collection of credit card information:

- **Not Permitted:**
  - Electronic mail (email) - NEVER process a transaction using cardholder data from an email!

- **Permitted if proper procedures are followed:**
  - Phone
  - Mail
  - In person
  - Fax (discouraged, but permitted)
    - Fax machine should be accessible to departmental staff only.
    - Faxes with card holder data should print only when departmental staff are available to pick up fax page. (Fax option-code to print)
    - Departments accepting card holder data via fax cannot use the option that converts faxes to electronic documents (viewed through email).
Credit Card Procedures - Access

- Transportation of credit card information:
  - Only employees who have been approved by the Office of Financial Operations & Business Technology and have regular access to credit card information should transport credit card information.
  - Credit card information should always be treated as cash and transported in a locked bag.

- Limit access to credit card information to department employees on a “need-to-know” basis only.
  - Unauthorized personnel should have NO access to cardholder data.
Any employee authorized to handle credit cards must be certified annually.

All users must use their own ID/Password to access software used when processing cardholder data.

Student workers processing bulk credit card transactions must have a background check.

All users must complete FERPA training prior to accepting credit card payments.
Credit Card Procedures - Storage

- **Electronic storage** of credit card information is NOT permitted.

- **Temporary physical storage**
  - ANY document containing credit card information must be stored (maximum 2 days) in a locked cabinet/file.
  - After credit card information has been processed:
    - Destroy entire document or physically remove the credit card information from the paper form (cut out or off).
    - Use a cross-cut or micro shredder to destroy credit card information.

- **Permanent physical storage** of credit card information within campus departments is NOT permitted.
Credit Card Procedures – Prevention of Tampering with Devices

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, supervisor, security officer, or Financial Operations Accounts Receivable).
Credit Card Acceptance Procedures

- The credit card software and hardware (PC or terminal) being used must be approved by or assigned by Financial Operations & Business Technology.
  - **TouchNet, Inc.** is WSU’s preferred software vendor for all WSU credit card processing needs.
  - Credit card terminals must be issued and maintained by Financial Operations & Business Technology.
  - Any device used to collect, process, store or transmit cardholder data must be issued and maintained by Financial Operations.
  - Exceptions to the above may be granted by Financial Operations & Business Technology.
Credit Card Incident Response Plan

- An "incident" is defined as a suspected or confirmed "data compromise".

- A "data compromise" is a situation where there has been unauthorized access to a system or network where cardholder data is collected, stored, processed or transmitted.
Credit Card Incident Response Plan (cont)

In the event of a suspected or confirmed “incident”

See WSU – Credit Card Incident Response Plan for specific details.

- Contact a member of Response Team AND send email to creditcards@wichita.edu with your contact information.

- If the incident involves a payment station
  - DO NOT Turn off the PC.
  - Disconnect the network cable connecting the PC to the network jack (cut the cable if you do not have access to the jack key).

- DO NOT DISCUSS the incident with anyone except your direct supervisor and Response Team.

- Refer all inquiries regarding the incident to the Response Team.
Credit Card Best Practices

In Person:
✓ Keep card in customer’s line of sight.
✓ Match signatures on signed receipt to back of card.
✓ Ask for ID if no signature exists on back of card.

Phone/Mail/Fax:
✓ Obtain security code on back of card for all phone sales.
✓ Write cardholder information only on designated forms.
✓ Store all documents containing cardholder data in a secure, locked area.
✓ When no longer needed for business or legal reasons, shred cardholder information using a cross-cut or micro shredder.

Email:
✓ Never send cardholder data through email.
✓ If you receive cardholder data through email, Do NOT process transaction.
✓ Delete email and empty your “deleted items” folder. Reply to customer with a NEW email.

General:
✓ Process refunds to the card used for original purchase.
✓ Never share cardholder information outside of work environment.
Additional Best Practices

- NEVER store credit card numbers in any database or spreadsheet.
- Mask all but last 4 digits of credit card number.
- Permit only those employees who have a legitimate “need-to-know” access to cardholder information.
- Do not allow unauthorized persons access to areas where credit card data is stored.
- Document departmental procedures.
- Segregate duties – the individual performing reconciliation should not be involved in processing credit card sales or refunds.
Related Information

- Policy & Procedure 13.01 / Deposit of Cash Receipts provides guidance concerning all deposits of University funds. Cash receipts includes all of the following:
  - U.S. Currency, U.S. Coins, Personal Checks, Credit Cards, Wire Transfers, Bank Drafts, Money Orders, Traveler’s Checks, Cashier’s Checks, and Foreign Drafts (but not foreign currency)

- WSU Controls Assessment Tool
  - [http://webs.wichita.edu/inaudit/cat3.htm](http://webs.wichita.edu/inaudit/cat3.htm)

- All employees authorized to accept funds on behalf of the University are required to be trained on Cash Handling procedures every two years.
Review
What does the Payment Card Industry Data Security Standard help to alleviate?

a) Debt
b) Vulnerabilities and Breaches
c) Theft of Cardholder Data
d) Heartburn
e) Both b & c

Answer: e) The PCI DSS protects both the cardholders and the University from fraudulent use of cardholder information through stringent practices and security measures.
Review

The PCI DSS consists of:

a) Comprehensive Requirements
b) Lots of Mumbo Jumbo
c) Regulations for Generating Card Numbers
d) Technical and Operational System Components
e) Both a & d

Answer: e) The PCI DSS has 12 comprehensive requirements that are both technical and related to office processes.
Review

The full credit card numbers should never be stored after authorization.

a) True
b) False

Answer: a) True. To reduce the risk of fraudulent achievement of cardholder data, all card numbers should be truncated and stored securely.
Review

Physical access to cardholder data should be:

a) In a Secure Area
b) Locked Up
c) Destroyed When No Longer Needed
d) On a “Need to Know Basis”
e) All of the Above

Answer: e) All of the Above. To reduce the risk of fraudulent achievement of cardholder data, all the above needs to be followed.
What does PCI DSS stand for?

a) Personal Card Industry Data Security Standard  
b) Payment Card Industry Data Security Standard  
c) Payment Card International Data Standards Site  
d) None of the Above

Answer: b) Payment Card Industry Data Security Standard
Review

When accepting payment card in person you should hold onto the card for the whole transaction and compare signatures on the card and the receipt.

a) True
b) False

Answer: a) True. The few extra seconds it takes to verify a signature can save your department from dealing with fraud.
Review

When accepting a payment card over the phone you should never ask for the cardholder’s phone number.

a) True
b) False

Answer: b) False. Obtaining a cardholder’s phone number can help you contact them.
You are walking through campus and see that a student group is taking credit cards for a service they are offering. You aren’t sure, but it doesn’t look like they are following PCI-DSS standards. What do you do?

a) Ignore them.
b) Ask them if the processing has been approved by Financial Operations?
c) Give them your credit card information and purchase their service.
d) Email creditcards@wichita.edu to see if the student group has been approved.

Answer: b or d, or both. For the protection of cardholder data and the University, it is ALWAYS good to report any questionable credit card processing on campus.
You see that a sales receipt contains the full primary account number of a customer. What should you do?

a) Use a pen and mark it out.
b) Put it in the trash.
c) Continue the transaction because receipts should have the full account number
d) Email creditcards@wichita.edu AND call Financial Operations to inform the University of the problem.

Answer: d) The full primary account number should never be printed on a receipt or report. Any violation should be reported immediately.
Which of the following best describes PCI-DSS compliance?

a) A goal  
b) A process  
c) A game  
d) An achievement

Answer: a) PCI-DSS is a never ending process. Original achievement of PCI-DSS compliance is only the beginning. Continued proof of compliance must occur on an annual basis.
QUESTIONS?

Call Accounts Receivable at ext. 3070 or email creditcards@wichita.edu
To certify that you have completed Payment Compliance Review, please click on one of the links below:

If you are the designated Primary Business Contact for your department, click on the link below to complete the agreement for your department which includes certification of your training.

https://webapps.wichita.edu/WebnowAuth?form=eF_fobt_deptccagree

If you are a departmental employee involved in credit card processing, click on the link below to complete the certification of your training.

https://webapps.wichita.edu/WebnowAuth?form=eF_fobt_empccagree