Agenda

☸ PCI DSS overview
☸ The Basics
☸ Your responsibilities
☸ University Policies
☸ Best Practices
So...what is PCI-DSS?

- Created by the PCI Data Security Council (Visa, MasterCard, American Express, Discover, and JCB)
- Created a common set of industry standards developed to increase the controls around cardholder data to reduce credit card fraud.
- These standards consist of 6 goals and 12 Requirements...
### PCI DSS Standards

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

PCI Requirement 12.6.1

Educate personnel!!!
Background Information

Over the past few decades...

- Increases in payment card usage
- Increases in e-commerce
- Increases in more “convenient” payment methods
In our desire for convenience, we have left ourselves vulnerable
As a public institution we have an obligation to our students, vendors, donors, stakeholders, and the community at large to ensure that account information is safe when processing credit card payments @ UWF.
PCI DSS—It Can Help Prevent Data Breaches!
Non-Compliance—What’s at Stake

Could result in the revocation of our ability to accept card payments

Causes damage to consumer trust and our reputation

Fines our acquiring bank $5,000 to $100,000 per month*

$7.01 million = Average organizational cost of a data breach**

*The bank will likely pass this fine along...
**2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute
Agenda

• PCI DSS overview
• The Basics
• Your responsibilities
• University Policies
• Best Practices
The Basics: Credit Card Anatomy (Front)

- Account Number
- Cardholder’s Name
- Expiration Date
- EMV Chip
- Holographic Security Emblem
- Card Logo

MasterCard
The Basics: Credit Card Anatomy (Back)

- **Magnetic Stripe**: Contains CH name/address; account #; expiration date; and security information to detect fraudulent cards.

- **Signature Panel**: Authorized Signature. Not Valid Unless Signed.

- **Security code also known as CVV2/CID*/CAV/CVC2**: Typically located on the back of the card.

---

*American Express refers to this code as the CID and it is located on the front of the card.*
What is Cardholder Data (CHD)? ...technically

Primary Account Number (PAN): Consists of the full credit/debit card number

CHD consists of the PAN plus any one of the following:

- Cardholder name
- Expiration date
- Security Code
The Last 4 Digits

Storage of the *last four digits* of a credit card number is allowed & does not constitute CHD.

Customer receipts should not show more than the *last four digits* of the credit card number.

Computer systems and software used to process credit card transactions should not display more than the *last four digits* of the credit card number.
Cardholder Data Procedures: 
*Magnetic Stripe/PIN/Code*

The University *does not* permit the storage of the codes found on the magnetic stripe, PIN/PIN block data, or the card validation code.
Cardholder Data Procedures: 
Access Control

All employees that have access to CHD must keep this information in the strictest confidence, and protect it from unauthorized access or disclosure.

Access to this information should be on a need-to-know basis only.
Cardholder Data Procedures: 
*Electronic Records*

CHD should NEVER be stored in electronic format*

CHD should NEVER be included in email or other electronic messages

*Entering CHD into e-market portals (Lumens/HigherOne/CashNet/etc.) does not qualify. As this data is not being stored on our campus network.*
Cardholder Data Procedures:

**Paper Records Procedures**

Paper documents must be protected, stored securely, and disposed of securely.

Avoid the use of paper documents whenever possible.

If unavoidable, please refer to the paper document standards/procedures provided on the UWF Financial Services PCI Compliance webpage.
Agenda

• PCI DSS overview
• The Basics
• Your responsibilities
• University Policies
• Best Practices
Workstation Responsibilities

Each workstation **must be a dedicated, PCI compliant, ITS approved payment machine**

Each user is required to have a **unique login** for operating POS device

Keep login **credentials confidential** and do not share with others

Secure the credit card environment from non cashier personnel
Log off whenever stepping away from machine

Log off another cashier and login with your own credentials when processing transaction

Turn off POS device at night and secure area

Keep your workstation clear of any sensitive materials
Agenda

• PCI DSS overview
• The Basics
• Your responsibilities
• University Policies
• Best Practices
Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Standards (PCI DSS) is a set of 12 guidelines that all entities that process, store, or transmit credit card information must follow. These standards are designed to protect sensitive data and prevent data breaches that could result in financial losses and legal consequences.

Introduction

The University of West Florida (UWF) is committed to protecting the privacy and security of personal information, including credit card information. The university has implemented the PCI DSS standards to ensure the confidentiality, integrity, and availability of all information processed on the university's systems.

Authorized Users

Only authorized users are permitted to access credit card information. All users must follow the PCI DSS standards to ensure the security and confidentiality of all sensitive data.

Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Council has established Data Security Standards that must be complied with by all entities that accept credit card transactions. These standards include controls for handling and protecting credit card information, and related computer and Internet security. UWF is dedicated to full compliance with PCI DSS.

Contacts

The following personnel may be contacted for questions or further information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linda Mowrey</td>
<td>email: <a href="mailto:mowreyl@uwf.edu">mowreyl@uwf.edu</a></td>
</tr>
</tbody>
</table>
PCI DSS Security Policy

Technologies **NOT** allowed to access the cardholder environment:

- Open or public WIFI (non VPN)
- Removable electronic media (USBs, etc.)
- Laptops
- Tablets
- Smartphones
PCI DSS Security Policy

Activities **NOT** allowed while accessing and/or connected to the cardholder environment

- Checking email
- Visiting any website not directly associated and pertinent to the actions being performed
- Make internet or intranet connections that are not explicitly necessary
Agenda

• PCI DSS overview
• The Basics
• Your responsibilities
• University Policies
• Best Practices
Best Practices

Maintain strong passwords and update regularly

- Password Dos and Don’ts

Be on the lookout for skimming devices

- Familiarize yourself with the point-of-sale equipment and check regularly for modifications

Be sure your station is physically secured at all times
Best Practices Continued

- Destroy CHD immediately* (cross-cut shredder)
- Notify the Compliance Officer or Financial Services immediately if there is a change in personnel
- Never send CHD via electronic messages/email
- Never share your login credentials
- Be on the lookout for phishing/social engineering attempts to steal your credentials

*Only write down CHD when absolutely necessary... it usually is not.

• Avoiding phishing and social engineering attacks
Questions?

mpackard@uwf.edu | 850.857.6070