FGCU PCI DSS Compliance Training
Training Audience

The following training module should be completed by all University Staff that handle and/or process cardholder data.

- Employees that process payments or issue refunds
- Managers who have employees that have direct contact with credit card processing and data
- Any employee that oversees, manages, or works with credit card processing software or hardware
Training Objectives

Once you have completed this training module, you should have a comprehensive understanding of the following:

• General background of PCI DSS

• Best Practices

• Expectations and responsibilities for you as a FGCU Merchant or FGCU employee handling payment card information

• Potential penalties for non-compliance

• Overall security requirements

• Protecting cardholders & FGCU
FGCU Policy

• All FGCU merchants, employees, and third parties with access to cardholder data are responsible for safeguarding the information and associated cardholder data that is entrusted in their care. Credit card and cardholder data can only be shared with others when it is done as a part of normal business procedures, such as processing payments or giving transaction receipts to a supervisor at the end of a shift.

• Accepted Forms of Electronic Payment
  • FGCU merchants accept all major credit cards
    • Visa
    • Mastercard
    • Discover
    • American Express
    • DinersClub
    • JCB
    • CarteBlanche
    • ChinaUnionPay
FGCU Restricted Data Policy

What Is Restricted Data?

Restricted Data: Restricted data is data in any format: Collected, developed, maintained or managed by or on behalf of the University, or within the scope of the University activities that are subject to specific protections under federal or state law or regulations or under applicable contracts, and whose loss or unauthorized disclosure would impair the functions of the University, cause significant financial or reputational loss, or lead to potential legal liability, such as patrons social security numbers, or credit card numbers.

Please click here for the University Policy
FGCU Acceptable Use Policy

• Florida Gulf Coast University’s information technology resources are a vital component of the teaching, researching and business environment of FGCU. It is the responsibility of all in the University community to use these resources in a responsible, legal and ethical manner.

• The purpose of this policy is to provide employees with guidance on the appropriate and inappropriate use of technology resources at FGCU.

Please click here for the University Policy
FGCU Procedures

FGCU requires a number of standards to protect cardholder data held and/or used at the University.

University Merchant Location Employees:

• Must have a criminal background check performed by Human Resources before access to cardholder data is granted. Employees with an inappropriate background will not be permitted access to cardholder data.

• Must attend a credit card security training session, or utilize the online training guide, and take the online quiz offered by FGCU.

• Must sign the Employee Code of Responsibility form in order to document his/her understanding of and willingness to comply with all University credit card policies and procedures. This certification will be maintained in the employee’s personnel file.

• Must have access to cardholder data limited to least privileges necessary to perform job responsibilities and based on individual personnel job classification and functions.
FGCU Procedures (Continued)

- Must have a unique password that must be changed every sixty days to access cardholder data.
- Must protect cardholder data so that only the last four digits of the credit card number are displayed or printed.
- Must store only cardholder data that is critical to business – name, account number, and expiration date.
- Must store only cardholder data that is encrypted or truncated.
- Must never store the three- or four-digit validation code in any form.
- Must not release cardholder data in any form unless there is a legitimate business purpose and then only after the request for information is reviewed and approved by the unit’s management.
FGCU Procedures (Continued)

• Must store and secure cardholder data in locked containers identified and classified as “confidential” in secured areas with limited access. Examples include electronic data, customer receipts, merchant duplicate receipts, reports, etc.

• Must perform an annual review of critical data storage to ensure that all security requirements are met.

• Must dispose of copies of cardholder data after five fiscal years by overwriting or degaussing magnetic media; paper must be cross-shredded.

• Must provide all third party merchants with a copy of University credit card policies.

• Must provide all third party merchants with a unique user ID that includes a password that must be changed every sixty days.
FGCU Procedures (Continued)

• Must give all third party merchants access to cardholder data only after a formal contract is signed that outlines the security requirements and requires adherence to the Payment Card Industry Security requirements.

• Must not store cardholder data on laptop, notebook, mobile computing devices or any removable media at any time.

• Must use strong encryption wherever cardholder data is transmitted or received over open public networks e.g. SSL/TLS or IP SEC.

• Must not use wireless network or WIFI to process any cardholder data.

• Must not send any unencrypted cardholder data by email. University email system is not encrypted.

• Must not share username or password.

• Must "lock" their computer station prior to leaving it unattended.
FGCU Procedures
Third Party Merchant Locations

• Must provide documentation of being PCI compliant and guidelines on how they securely store, transmit and dispose of cardholder data and encryption keys.

• Must not use wireless network or WIFI to process any cardholder data.

• Must not send any unencrypted card holder data by email. University email system is not encrypted.
FGCU Rules

• All FGCU merchants and employees must follow basic card acceptance rules for all electronic transactions.

• Dollar Minimum & Maximums
  • Honor valid credit cards, regardless of the dollar amount of the purchase. Imposing minimum or maximum purchase amounts is a violation of our merchant services agreement.

• No Surcharging
  • Treat electronic transactions like any other transaction; that is, you may not impose any surcharge on a credit card transaction.

• Taxes
  • Include any required taxes in the total transaction amount. Do not collect taxes separately in cash.
PCI DSS BACKGROUND

- Purchase Card Industry Data Security Standards is most commonly referred to as PCI DSS.
- The requirements were developed by founders of the PCI Security Standards Council which includes Visa, MasterCard, American Express, Discover, and JCB.
- Regulations apply to anyone who stores, processes, and transmits cardholder data.
- Provides a baseline of technical and operational requirements designed to protect cardholder data.
- Applies to all forms of payment card acceptance: Mail, phone, fax, point-of-sale, and online.
- Identifies and corrects vulnerabilities by ensuring appropriate levels of security are maintained.
PCI Terms

• **Payment cards** – credit cards, debit cards, and other cards that facilitate cardholder payments

• **Card present transactions** – the cardholder presents the actual card to the merchant for processing. Usually swiped into a register or terminal and a signature is obtained.

• **Card not-present transactions** – the cardholder enters card information to complete transaction online, gives his/her payment card information over the phone or sends his/her card information on a designated form. A form may include a signature, however, signatures are usually not obtained for this type of transaction.
What are the Requirements?

• PCI DSS is comprised of 12 high-level requirements, which includes over 200 sub requirements

[https://www.pcisecuritystandards.org/document_library](https://www.pcisecuritystandards.org/document_library)

• Requirement 12.6.1 is the mandate to educate personnel who handle credit cardholder information upon hire and at least annually. In other words, the reason for this training.
What is in scope for PCI requirements?

• All personnel with access to cardholder data.
• All system components that capture, store, process, or transmit cardholder data. This includes servers, workstations, network devices, and applications, along with anything on the same network segment.
PCI Data Security Standard (DSS)

12 High-Level requirements – deceptively simple

| 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 |
THE IMPORTANCE OF PCI

• Florida Gulf Coast University has an obligation to students, vendors, alumni, and others to keep their account information safe when processing credit card payments.

• FGCU Merchants must maintain compliance at all times - meaning any FGCU location accepting electronic payments as legal tender.

• A proactive step that helps FGCU protect customer account information, including:
  o Magnetic stripe/track data, Primary Account Number (PAN), expiration date, card security code, pins, and other personal information
PCI DSS v3.0

Requirement 9.9 – Payment Terminal Protection

This requirement is to ensure that merchants have controls and countermeasures in place to protect devices that capture payment card data via physical interaction with the card from tampering and substitution.

The protection requirements are:

• Maintain an up-to-date inventory of your terminals/devices

• Departments are required to periodically inspect credit card equipment (card swipe terminals, connection, etc.) to detect tampering or substitution of a fraudulent device. Any suspicious indications should be reported to the Office of the Controller immediately.

• Train personnel to be aware of suspicious behavior and to report tampering or substitution of terminals/devices
Inspecting Terminal/Device

Terminals will have a sticker attached to the underside, which provides details of the product and will include a serial number. The majority of terminals will also have a method of displaying the serial number electronically.

As part of your regular checks, note the serial number on the back of the terminal and check this against the electronic serial number.

Additionally, run your finger along the label to check that it is not hiding a compromise.
Inspecting Terminal/Device

Terminals often have security stickers, or company stickers placed over screw holes or seams that will act as indicators if the case has been opened.

Criminals often remove these labels when compromising terminals and may replace them with their own printed versions.

When you first receive the terminal, make careful note of label position, color, and materials used. Taking a picture of the device is a good practice.

Also look for any signs that the label may have been removed or tampered with.
Inspecting Terminal/Device

Skimming devices hidden within the terminal will not be visible, and neither the merchant staff nor the cardholder will know that the card has been skimmed.

This picture shows a skimming device inserted in a terminal. This would have been hidden by the SIM card cover plate.
Inspecting Terminal/Device

EMV or chip cards are not immune to skimming. Staff and consumers should be aware of modifications or wires to the smart-card slot. If anything appears different with the device, it should be reported immediately.
Inspecting Terminal/Device

Staff should also be aware of the addition of overlays. An overlay can be a small sticker that forms to the device and covers the keyboard area.

Overlays may hide damage due to tampering or wires that can allow for keyboard logging. Overlays should not be used.
## PCI Data Fields - What can never be stored!

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Render Stored Data Unreadable per Requirement 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Service Code</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Full Track Data&lt;sup&gt;3&lt;/sup&gt;</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>CAV2/CVC2/CVV2/CID&lt;sup&gt;4&lt;/sup&gt;</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>PIN/PIN Block&lt;sup&gt;5&lt;/sup&gt;</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
</tbody>
</table>

2. Sensitive authentication data must not be stored after authorization (even if encrypted).
3. Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere
4. The three- or four-digit value printed on the front or back of a payment card
5. Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message

*Payment Card Industry (PCI) Data Security Standard, v3.2*

© 2006-2016 PCI Security Standards Council, LLC. All Rights Reserved.
BEST PRACTICES FOR CREDIT CARD PROCESSING

• Segregate duties when possible
  • The individuals that processes credit card transactions and refunds should not be involved in reconciling

• Do not send or accept credit card information via email
  • Notify a supervisor in the event you receive such an email
    • Do not process a payment based on the information provided in the email; delete the email immediately; do not print or forward the email containing payment card information; notify the sender that you are unable to process the payment

• Remember to NEVER store payment card data in any form for any reason, including:
  • Primary Account Number (PAN), expiration date, track data, security codes, and PIN number
BEST PRACTICES FOR CREDIT CARD PROCESSING (CONTINUED)

• After the transaction is complete store no more than the last four numbers of the PAN

• Store all necessary credit card documentation in a secure location

• Only allow employees who have a legitimate business need to access cardholder information

• Restrict physical access to areas where credit card information is handled and stored

• Store payment card receipts for the current fiscal year and three previous fiscal years in a secure location

• Each user needs their own user ID, coupled with a secure password that is changed regularly
Card-Present Procedures

Card-Present transactions are those in which both the card and cardholder are present at the point of sale.

• Swipe at Terminal
  • On the back of every credit and debit card, you will find a magnetic stripe. It contains the cardholder name, card account number, and expiration date, as well as special security information designed to help detect counterfeit cards.

• If Card Won’t Read when Swiped
  • In some instances, when you swipe a card, the terminal will not be able to read the magnetic stripe or perform an authorization. When this occurs, it usually means one of three things:
    • The terminal’s magnetic-stripe reader is dirty or out-of-order
    • The card is not being swiped through the reader correctly
    • The magnetic stripe on the card has been damaged or demagnetized

• If you determine the terminal is working properly and the cardholder is swiping the card correctly, you’ll need to request another card to process the transaction.
Card-Not-Present Procedures

• Every day, the number of purchases conducted via the mail, telephone, and internet increases. These transactions are significantly different from in-store sales, in that the customer and credit card are not present during the transaction, making it especially difficult to detect fraud.

• Card acceptance procedures for these Card-Not-Present transactions are different from in-store purchases. FGCU employees who conduct Card-Not-Present transactions must exercise extreme caution and follow procedures precisely in order to verify—to the greatest extent possible— the cardholder’s identity and the validity of the purchase.

• TouchNet software is the preferred University’s method to process Cards-Not-Present transactions through an online payment system, and meets all PCI Data Security Standards which enables FGCU to offer a consistent, streamlined approach to E-Commerce.
Card-Not-Present Best Practices

- Florida Gulf Coast University’s Office of Finance and Accounting has developed best practices for accepting credit card payments via fax, telephone, and mail to ensure we are protecting the cardholder’s information.

- Please note that the departments that have traditionally accepted these types of payments will be transitioned to a TouchNet product that will best fulfills their needs, and ensures a secure payment portal that meets the PCI Data Security Standards.
Best Practices for Fax:

• If your department receives credit card information via fax, the fax must be in an area not accessible by unauthorized individuals.

• Paper forms received with credit card information must be stored in a safe, inside a secure location, and inaccessible to unauthorized personnel.

• The documents must be clearly marked as containing sensitive information (ie. folder marked “Confidential”)

• Destroy fax after processing payments, using an approved shredding device or shredding service.
Best Practices for Mail:

• Paper forms received with credit card information must be stored in a safe, inside a secure location, and inaccessible to unauthorized personnel

• The documents must be clearly marked as containing sensitive information (ie. folder marked “Confidential”)

• Destroy form after processing payments, using an approved shredding device or shredding service.
Best Practices for Telephone:

• Telephone sales should directly be keyed into credit card processing system.

• No cardholder information should be written down or stored.
Fraud Prevention

If you experience or suspected a security breach, you should:

• Immediately contain and limit the exposure. **Do not** turn off the compromised machine.

• To prevent any further loss of data, conduct a thorough investigation as soon as possible. Investigations must be conducted within 24 hours of the compromise.

• If you suspect a compromise of data:
  ◦ Describe the credit card security breach
  ◦ Provide the Office of Finance & Accounting your contact information including name, phone number, and e-mail address
  ◦ The Office of Finance & Accounting will determine the extent of the breach and notify the necessary departments to take the appropriate actions

• Do not access or alter compromised systems. Do not log on to the machine or change passwords.

• Preserve logs and electronic evidence. Log all actions taken.
POTENTIAL SECURITY BREACHES

• Secure filing cabinets being left open
• Lost or stolen keys
• Computer work station breach, infection, compromise
• New, unidentifiable equipment in point-of-sale area (skimming device)
• User ID and password stolen or given out
• Unusual/unexplained credit card transactions
Security Tips

- Remember to lock your computer station prior to leaving unattended
- Do not share username or password with anyone
- If you cannot access the system, contact the Office of Finance & Accounting
- Do not store cardholder data
THE IMPORTANCE OF COMPLIANCE

The various methods and intelligence of malicious attacks are constantly increasing and ever changing, therefore so should our due diligence with regard to compliance.

Penalties for a Breach:

• Significant fines per incident
• Increased audit requirements
• Potential loss of the ability to accept payment cards
• Loss of staff time during security recovery
• Loss of business revenue due to loss of public image
• Cost of forensic investigation
Through your continued vigilance and implementation of PCI standards, you and your department assist FGCU in maintaining compliance and achieving a PCI mandate.

- You are the first line of defense against fraud at FGCU
- Recognize unusual or suspicious activity/transactions
- If you recognize procedures/regulations not being followed contact the Office of the Controller immediately
- Be ever vigilant when interacting with payment card data and credit card transactions
CONGRATULATIONS!

You have completed your annual PCI Security Awareness Training