WHO NEEDS PCI TRAINING?

THE FOLLOWING TRAINING MODULE SHOULD BE COMPLETED BY ALL UNIVERSITY STAFF THAT:

- PROCESS PAYMENTS

- HAVE DIRECT CONTACT WITH PAYMENT CARD TRANSACTIONS

- OVERSEES, MANAGES, RECONCILES, OR WORKS WITH PAYMENT CARD TRANSACTIONS
WHY DO YOU NEED TO KNOW ABOUT PCI COMPLIANCE?

• To enhance employee skills in maintaining the security and safety of the ODU payment card environment.

• Compliance is mandated by the Payment Card Industry (PCI) for all organizations handling credit card data.

• As an ODU employee, it is your responsibility to be knowledgeable of policies and procedures pertaining to your job duties. It is very important that all credit card information be safeguarded. All departments that collect credit card payments must ensure all staff members adhere to these standards.
WHEN DOES IT NEED TO BE TAKEN?

- For employees currently handling cardholder information, at least annually.
- For new employees or current employees taking over cardholder duties, upon hire and annually thereafter.
PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)

- PCI DSS standards were developed and agreed upon by VISA, MasterCard, American Express, Discover, and JCB.

- The main purpose of PCI DSS is to protect cardholder data by requiring mandatory data security standards for any department that processes, stores, or transmits cardholder data.

- By properly following the PCI DSS twelve elements or requirements, ODU can reduce the risks of payment card fraud, hacking, and other sources that result in compromised data.

- Applies to all forms of payment card acceptance: mail, phone, fax, point-of-sale, and online.
## 12 Elements of PCI DSS Requirements

<table>
<thead>
<tr>
<th>Build and Maintain a Secure Network and Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protect Cardholder Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintain a Vulnerability Management Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Protect all systems against malware and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implement Strong Access Control Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td>8. Identify and authenticate access to system components</td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regularly Monitor and Test Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td>11. Regularly test security systems and processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintain an Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
WHAT DOES THIS MEAN FOR ODU?

It is the University’s responsibility to prevent and detect fraud. ODU has an obligation to students, vendors, alumni, and others to keep their account information safe when processing credit card payments.

The University must:

• Identify and evaluate all credit card acceptance activities.

• Develop policies/procedures for payment card acceptance.

• Ensure that credit/debit card activities comply with established procedures.
Employees must:

• Protect student and customer account information including: credit card account number, expiration dates, security codes, pins, and any other personal information.

• Strictly follow and adhere to the department’s payment processing procedures.

• Complete an **Annual PCI training** review and sign the Payment Card Security and Confidentiality Agreement form.
Why?

• We live and work in a global community. Most of us give very little thought to handing over our credit or debit card to complete strangers or entering our card data into a website.

• We do this in good faith, expecting that our information will be protected. Yet, each year millions of Americans are affected by credit card theft.
They depend on us.....

Each day, people engage in payment card activity or transactions with ODU, with the expectation that we will protect their data from thieves. We work hard to maintain a secure data environment.
Therefore, we ALL Have a Role to Play to Comply with PCI DSS.

We depend on all University employees to assist in securing all customer cardholder data and other personal information.

When working with sensitive information, handle it like it was cash or your own card information.
IT CAN HAPPEN SO EASILY

- Payment card information should always be secured.
- Most payment card frauds are crimes of opportunity:
  - Door left open,
  - Computer left unprotected,
  - Filing cabinet left open, unattended, or unlocked,
  - Unauthorized access to secure areas,
  - Sensitive data left sitting on a desk,
  - Thrown away in a trashcan.
FOLLOW THESE RULES:

• Never accept credit card numbers in an email, text, voicemail or instant message.
  • DO NOT process the transaction.
  • Send an email back to the individual without the credit card information included and state that the University will not process any credit card number received through email.
  • Delete the email.
  • If accepting credit/debit card information over the phone, process while customer is on the phone. Any documents that contain card information must be shredded immediately upon processing of payment.
• Do NOT store or retain paper or electronic data that contains the customer’s payment card number.

• Primary Account Number (PAN) is the card number shown on front. Render this unreadable anywhere it’s stored. Usually, the PAN will be truncated: ************1234 or Only the first six and last four should be stored. Please note: Redacting with black marker is not sufficient, use a hole puncher to cut out numbers or shred in cross-cut shredder.

• Expiration dates.

• Validation codes (also known as CVV/CVC code) – The 3 digit security code on the back of VISA, MasterCard and Discover or a 4 digit code on an American Express card.

• CVV/CVC code MUST be destroyed upon authorization of the transaction.
• Do not simply throw away credit card information – always cross-cut shred or burn when disposing of the information.

• When possible, check for signature and verify signed receipt. If card is not signed, ask cardholder to present a valid government photo ID, and compare signatures and name, including the one on the sales receipt. Remember: Visa cards begin with a 4, MasterCard starts with a 5, Discover starts with a 6, and AMEX starts with a “34” or “37”. Do not accept a credit card with a number that does not correspond to the credit card type.

• Do not enter full credit card numbers into general purpose computers, laptop computer, tablet, smart phone or other portable devices. Never store credit/debit card data on removable media such CDs, USB drive or memory cards.

• Segregate duties when possible. The individuals that processes credit card transactions and refunds should not be involved in reconciling.
• ALWAYS KEEP PAYMENT CARD TERMINALS LOCKED IN A SECURE LOCATION.

• NEVER REVEAL YOUR PASSWORD TO ANYONE. NEVER TRANSMIT A PASSWORD IN AN EMAIL.

• DO NOT ALLOW PUBLIC ACCESS TO SENSITIVE DATA AREAS.

• RESTRICT EMPLOYEE ACCESS TO PAYMENT CARD DATA TO A “NEED TO KNOW” BASIS. DON’T ALLOW UNAUTHORIZED INDIVIDUALS AROUND PCI DEVICES.

• KEEP ANTI-VIRUS SOFTWARE UPDATED.

• KEEP ALL PAYMENT CARD DATA SECURE AND CONFIDENTIAL.

• ONLY ACCEPT CREDIT CARD NUMBERS IF RECEIVED IN REGULAR MAIL, IN PERSON, OVER THE PHONE, OR OVER A SECURE FAX. (A SECURE FAX CAN ONLY BE ACCESSED BY THOSE EMPLOYEES THAT NEED THE INFORMATION AND CANNOT BE A MULTI-FUNCTIONAL DEVICE, SUCH AS COPIER, CONNECTED TO THE NETWORK).
INSPECT PAYMENT CARD TERMINALS DAILY OR BEFORE EACH USE IF NOT USED DAILY

• These inspections are completed using the Daily/Tamper Log provided by the PCI Compliance Specialist. (Requirement 9)
  • Make sure the make and model number on the terminal matches the make and model number on the Daily/Tamper Log.
  • Perform routine visual inspections of every device, looking for potential signs of tampering. Keep track of any operational difficulties that begin happening on a regular basis. If you notice these or anything out of the ordinary, stop using the device immediately and disconnect it from the POS device or network, but do not power it down. Immediately contact the campus central business office and campus central IT office. Some examples of things to look for include:
    • Damaged or altered tamper seals
    • Missing manufacturer labels
    • Missing screws or screws with damaged heads
    • Incorrect keyboard overlays
    • External wires
    • Holes in the device housing
    • An electronic serial number that does not match the number printed on the bottom of the device
    • A high number of mag-stripe read failures or debit card declines
    • Difficulty inserting a chip and PIN card into the EMV slot

• Ensure personnel is aware of indications of tampering or substitution and recognizing and reporting suspicious behavior around payment card devices to a manager or Campus Police.
**DEPARTMENTS RESPONSIBILITIES:**

<table>
<thead>
<tr>
<th>Online Payment Processing (Touchnet, U-Pay, U-Store, University Tickets, Follett, etc.)</th>
<th>Credit Card Payment Processing Terminals (FD410, Shift4 Magnetic swipe, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Complete Annual PCI Security Awareness Training</td>
<td>• Complete Annual PCI Security Awareness Training</td>
</tr>
<tr>
<td>• Sign the PCI Confidentiality Agreement Form</td>
<td>• Sign the PCI Confidentiality Agreement Form</td>
</tr>
<tr>
<td>• Follow the Departments Credit Card Processing Rules &amp; Procedures</td>
<td>• Follow the Departments Credit Card Processing Rules &amp; Procedures</td>
</tr>
<tr>
<td>• Make sure computers have latest antivirus</td>
<td>• Complete SAQ (Self Assessment Questionnaire once a year)</td>
</tr>
<tr>
<td>• Complete SAQ (Self Assessment Questionnaire once a year)</td>
<td>• PCI Compliance Specialist Quarterly Inspections</td>
</tr>
<tr>
<td></td>
<td>• Daily/Tamper Log &amp; Visitors Log</td>
</tr>
</tbody>
</table>
IF YOU ARE SELLING TAXABLE PRODUCTS OR SHIPPING MERCHANDISE...

• For all merchants, when the University sells tangible personal property, the department is responsible for collecting sales tax unless proof of tax exemption is obtained. Sales tax for the Hampton Roads Region is 6%. Sales tax exemption certificates should be kept on file by the selling department following the retention schedule.

• For taxes to be properly collected on online purchases, the TouchNet tax service must be enabled for each individual uStore.

• Each taxable product must be setup with its tax class set to “default tax rate”.

• Each uStore’s shipping class must be configured to include a mailed delivery method with “Shipping Address Required” enabled.
CONSEQUENCES OF NONCOMPLIANCE CAN INCLUDE:

• **Loss of ODU reputation** and customers.

• Significant financial fines per incident.
  • A small breach could cost up to and over $1 million in direct costs alone.
  • Direct costs include notifications, hotlines, website, credit monitoring, and fines.
  • Indirect costs include forensic investigation, system upgrades, employee time, card reissuance, fraud liability, and lawsuits.

• Litigations or sanctions.

• Termination of ability to accept credit cards.
REPORT TO SUPERVISOR, ITS PCI INCIDENT RESPONSE TEAM AND PCI COMPLIANCE SPECIALIST (OFFICE OF FINANCE) IMMEDIATELY IF:

- Lost or stolen:
  - Password,
  - ID,
  - Keys,
  - Laptop,
  - Portable storage device, or
  - Credit Card Terminal.

- Filing cabinets, credit card terminals or locks are tampered.

- Computer gets infected with virus or malicious software.

- Anything you feel is suspicious.

- If you recognize procedures/ regulations not being followed contact the Office of Finance.
Target

Year: 2013

Affected: 40 million credit and debit card accounts, as well as data on 70 million customers.

Cost: Through the end of 2014, the data breach cost Target $252 million, according to corporate filings.

What happened: The breach affected credit and debit card accounts from shoppers from Nov. 27 to Dec. 15. But personal data could have been stolen from more Target shoppers.

December 12, 2014

The University of California Berkeley has notified individuals of a data breach in their Real Estate Division that resulted in unauthorized access to servers used to support a number of Real Estate programs and work stations. The investigation of the hacking showed that these servers were breached in mid-to late September. The personal information included names, Social Security Numbers, credit card numbers and driver's license numbers.

January 10, 2013

Texas Southern University's radio station KTSU gave a volunteer position to a person with a criminal history of credit card fraud. The volunteer was later arrested for allegedly using the radio station's donation drive to steal credit card information. The dishonest volunteer faces up to 300 counts of credit card fraud for attempting to use the information on donor pledge sheets.

Home Depot

Year: 2014

Affected: 56 million credit card accounts and 53 million email addresses.

Cost: The data breach cost the company an estimated $80 million before insurance reimbursements, according to Protection Group International.

What happened: In September 2014, Home Depot revealed that hackers had gained access to the company's computer network using stolen account information from a vendor doing business with the hardware giant.
REMEMBER: YOU ARE THE FIRST LINE OF DEFENSE AGAINST FRAUD

Violations are COSTLY.

Damage to the University’s reputation would be the greatest “cost”.
CONGRATULATIONS!

YOU HAVE COMPLETED YOUR ANNUAL PCI SECURITY AWARENESS TRAINING

THIS TRAINING IS GOOD FOR **ONE CALENDAR YEAR**.

THANK YOU FOR HELPING THE UNIVERSITY PROTECT OUR CUSTOMER’S DATA.

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT THE OFFICE OF FINANCE:

PCI@ODU.EDU