PCI-DSS Compliance
Agenda

- Introduction
- New PCI-DSS Compliance Process
- CampusGuard Central Portal
- Next Steps
- Q&A

First, some administration...
History of PCI Compliance at Rutgers

2004 – PCI Standards Released

2018 – Audit & Advisory Services Review

2020 – CampusGuard engaged
- 10th anniversary year
- International Information security, privacy, and compliance firm
- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)
- Perform compliance and security assessments, vulnerability scans, penetration tests, on-going support, and training
- Focused on campus-based organizations including Higher Education, Healthcare, and State & Local Government
PCI Overview

- PCI-DSS
  Payment Card Industry Data Security Standard

- Common set of card data security measures.

- Every merchant is responsible for safeguarding cardholder data, can be held liable for security compromises, and is contractually obligated to comply with PCI-DSS.
## PCI Overview – PCI DSS Framework

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></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 Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
PCI Overview – What does PCI protect?
PCI Overview – Who needs to comply?

- **Merchant**
  - Accepts payment cards
  - Owns a Merchant ID (MID)

- **Service Provider**
  - Stores, processes, or transmit CHD on behalf of another entity
  - Provides services that control or could impact the security of CHD
    - Exception – Internet Service Providers (ISP)
PCI Overview – Defining PCI scope

- People, processes, and technologies that store, process, or transmit cardholder data, or that could affect the security of cardholder data.

- Any systems that reside in or connect to the Cardholder Data Environment (CDE).
# PCI Overview – Merchant Types

<table>
<thead>
<tr>
<th>SAQ</th>
<th>Count</th>
<th>Payment Method</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>24</td>
<td>Card-not-present merchants; all cardholder data functions fully outsourced to validated third parties</td>
<td>Green</td>
</tr>
<tr>
<td>P2PE</td>
<td>34</td>
<td>PCI Council listed P2PE solutions, only terminals approved for the solution No electronic CHD storage</td>
<td>Yellow</td>
</tr>
<tr>
<td>B</td>
<td>41</td>
<td>Merchants with only imprint machines or only standalone, dial-out terminals No electronic cardholder data storage</td>
<td>Yellow</td>
</tr>
<tr>
<td>C-VT</td>
<td>84</td>
<td>Merchants with web-based virtual terminals hosted by validated third parties No electronic CHD storage</td>
<td>Red</td>
</tr>
<tr>
<td>B-IP</td>
<td>87</td>
<td>Merchants with standalone, IP-connected PTS-approved Point-of-Interaction (POI) terminals – No electronic CHD storage</td>
<td>Red</td>
</tr>
<tr>
<td>C</td>
<td>161</td>
<td>Merchants with payment application systems connected to the Internet No electronic CHD storage</td>
<td>Red</td>
</tr>
<tr>
<td>A-EP</td>
<td>192</td>
<td>Partially outsourced ecommerce merchants using validated third party websites for payment processing</td>
<td>Red</td>
</tr>
<tr>
<td>D</td>
<td>328</td>
<td>All other SAQ-eligible merchants</td>
<td>Red</td>
</tr>
<tr>
<td>D-SP</td>
<td>370</td>
<td>All SAQ-eligible service providers</td>
<td>Red</td>
</tr>
</tbody>
</table>
Merchants have contracts with Service Providers requiring them to protect cardholder data.

The brands have contracts with banks requiring them to ensure their merchants are PCI compliant.

The banks have contracts with merchants requiring them to be PCI compliant.

Unlike regulations, PCI DSS is enforced by contract.
New PCI Compliance Process

• Developing policy and governance model

• Identification and maintenance of merchant contacts and related information

• Merchant Responsibilities:
  • Annual Security Assessment Questionnaires (SAQ’s)
  • Annual training
  • Merchant documentation
CampusGuard Central is a compliance portal that allows staff to track and document their PCI process.

The portal is user friendly and has built-in support capabilities.

There will be additional training and information provided soon.
Next Steps

CampusGuard Central
Users will be notified in March once they are set up

SAQ’s
To be completed on the portal, they are due June 30th

Training
Training will be due each year on June 30th
Requesting Training

- Due Date: June 30th of Each Year
- Currently Registered: 625
- Currently Completed: 278
  - Submit a Training Request Form for PCI Training
  - Provide Training Rosters
- Contact: Information Security Trainer - infosecurity@oit.rutgers.edu
EMAIL:
PCI-Compliance@finance.rutgers.edu