PCI-DSS Compliance

Elahe Russell

February 12, 2019
What is **PCI-DSS**?

The **Payment Card Industry Data Security Standard (PCI-DSS)** is an information security standard intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.
PCI Readiness Review

- LSU engaged CampusGuard as a Qualified Security Assessor (QSA)
- Met with PCI Team and Information Technology (IT)/Security teams
- Conducted PCI training sessions for merchants and IT
- Provided preliminary results to Executive Leadership
- Participated in 14 onsite merchant interviews
<table>
<thead>
<tr>
<th>Athletics Ticket Office</th>
<th>Pennington Biomedical Research Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary Services – Event Management</td>
<td>Residential Life</td>
</tr>
<tr>
<td>Auxiliary Services – Union Theater</td>
<td>Rural Life Museum</td>
</tr>
<tr>
<td>Bursar Operations</td>
<td>Student Health Center</td>
</tr>
<tr>
<td>Center for Computation and Technology</td>
<td>University Laboratory School</td>
</tr>
<tr>
<td>LSU Golf Course</td>
<td>University Recreation</td>
</tr>
<tr>
<td>Parking, Traffic &amp; Transportation</td>
<td>Veterinary Medicine</td>
</tr>
</tbody>
</table>
## PCI-DSS Milestones

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Goal</th>
</tr>
</thead>
</table>
| 1         | **Remove sensitive authentication data and limit data retention.**  
This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don’t need it, don’t store it! |
| 2         | **Protect systems and networks, and be prepared to respond to a system breach.**  
This milestone targets controls for points of access to most compromises, and the processes for responding. |
| 3         | **Secure payment card applications.**  
This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data. |
| 4         | **Monitor and control access to your systems.**  
Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment. |
| 5         | **Protect stored cardholder data.**  
For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data. |
| 6         | **Finalize remaining compliance efforts, and ensure all controls are in place.**  
The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment. |
Findings by Milestone

- Milestone 2: 28
- Milestone 4: 4
- Milestone 5: 4
- Milestone 6: 12
- Milestone 3: 24
- Milestone 1: 4
### Recommendations

<table>
<thead>
<tr>
<th>DO NOT</th>
<th>DO</th>
</tr>
</thead>
<tbody>
<tr>
<td>× Process or transmit cardholder data (CHD) on general use computers</td>
<td>✓ Discontinue using workstations as a method to enter payment card information</td>
</tr>
<tr>
<td>× Accept CHD via email</td>
<td>✓ Provide PCI-listed P2PE solutions or stand alone terminals to eliminate the need to enter CHD on employee workstations</td>
</tr>
<tr>
<td>× Use campus wi-fi for payment processing</td>
<td>✓ Destroy CHD in a PCI compliant manner</td>
</tr>
<tr>
<td>× Accept CHD faxed to network or multi-function printers</td>
<td>✓ Use cross-cut shredders to destroy any CHD</td>
</tr>
<tr>
<td>× Retain or store paper including CHD</td>
<td>✓ Regularly check hardware for skimming devices</td>
</tr>
</tbody>
</table>
**Action Items**

- Formalize PCI Team and charter
- Review all merchants and related payment processes
- Verify equipment and media inventory
- Eliminate storage of CHD/secure information disposal
- Cease email and unsecured fax acceptance of payment card information
- Update Incident Response Plan
- Revise and update institutional policy

- Create departmental procedures for merchants
- Formalize training of departmental merchants
- Implement procedures for inspecting devices
- Complete Self-Assessment Questionnaires (SAQs)
- Review service provider compliance
- Implement third-party service provider management program
# PCI Team

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elahe Russell</td>
<td><a href="mailto:erussell@lsu.edu">erussell@lsu.edu</a></td>
<td>Accounting Services</td>
</tr>
<tr>
<td>Beth Nettles</td>
<td><a href="mailto:studbr@lsu.edu">studbr@lsu.edu</a></td>
<td>Bursar Operations</td>
</tr>
<tr>
<td>Anthony Gonce</td>
<td><a href="mailto:agonce1@lsu.edu">agonce1@lsu.edu</a></td>
<td>Internal Audit</td>
</tr>
<tr>
<td>Sumit Jain</td>
<td><a href="mailto:sjain@lsu.edu">sjain@lsu.edu</a></td>
<td>IT Security and Policy</td>
</tr>
<tr>
<td>Daniel Butcher</td>
<td><a href="mailto:dbutch1@lsu.edu">dbutch1@lsu.edu</a></td>
<td>Bursar Operations</td>
</tr>
<tr>
<td>Sean Robbins</td>
<td><a href="mailto:sean@lsu.edu">sean@lsu.edu</a></td>
<td>Network Engineering</td>
</tr>
<tr>
<td>Jeff Deveer</td>
<td><a href="mailto:jeff@lsu.edu">jeff@lsu.edu</a></td>
<td>Athletics</td>
</tr>
<tr>
<td>Tyler French</td>
<td><a href="mailto:tfrench1@lsu.edu">tfrench1@lsu.edu</a></td>
<td>Bursar Operations</td>
</tr>
<tr>
<td>Sam Abboud</td>
<td><a href="mailto:sabbou2@lsu.edu">sabbou2@lsu.edu</a></td>
<td>College of Human Sciences and Education</td>
</tr>
<tr>
<td>Jan Bernath</td>
<td><a href="mailto:jbernath@agcenter.lsu.edu">jbernath@agcenter.lsu.edu</a></td>
<td>LSU Agricultural Center</td>
</tr>
<tr>
<td>Monica Mougeot</td>
<td><a href="mailto:monica.mougeot@pbrc.edu">monica.mougeot@pbrc.edu</a></td>
<td>Pennington Biomedical Research Center</td>
</tr>
</tbody>
</table>
Background & Timeline

- Merchant Services
  - Payment Card Industry Data Security Standards (PCI-DSS)
- Cashiering Solution
  - Workday Student Design Partner Group

- November 6, 2017
  RFP Issued for Merchant and Cashiering Services
- June 13, 2018
  CashNet Master Contract Signed
- July 25, 2018
  Project Kickoff Call
- August 31, 2018
  Start of Phase I
CashNet Modules

- eBill
- ePayment
- SmartPay
- Payment Plans
- Cashiering
- eMarket
- eRefund
Project Phases

**Phase I**
- eMarket
- Storefront
- Checkout
- SmartPay

**Phase II**
- Cashiering
- Bursar Operations
- Merchants

**Phase III**
- eBill
- ePayment
- Payment Plans
- eRefund
CashNet Advantages

- Merchant ID owned by CashNet
- Significant reduction of PCI scope
- Automated departmental deposits
- P2PE solutions for cashiering
- Customizable storefronts
Challenges

- Real-time G/L validation with Workday
- G/L segment limitation
- Student Modernization Program timeline
- Merchant adoption (eMarket)
- Third-party vendor contacts (eMarket)
Questions

Daniel Butcher
Assistant Director
Bursar Operations
dbutch1@lsu.edu