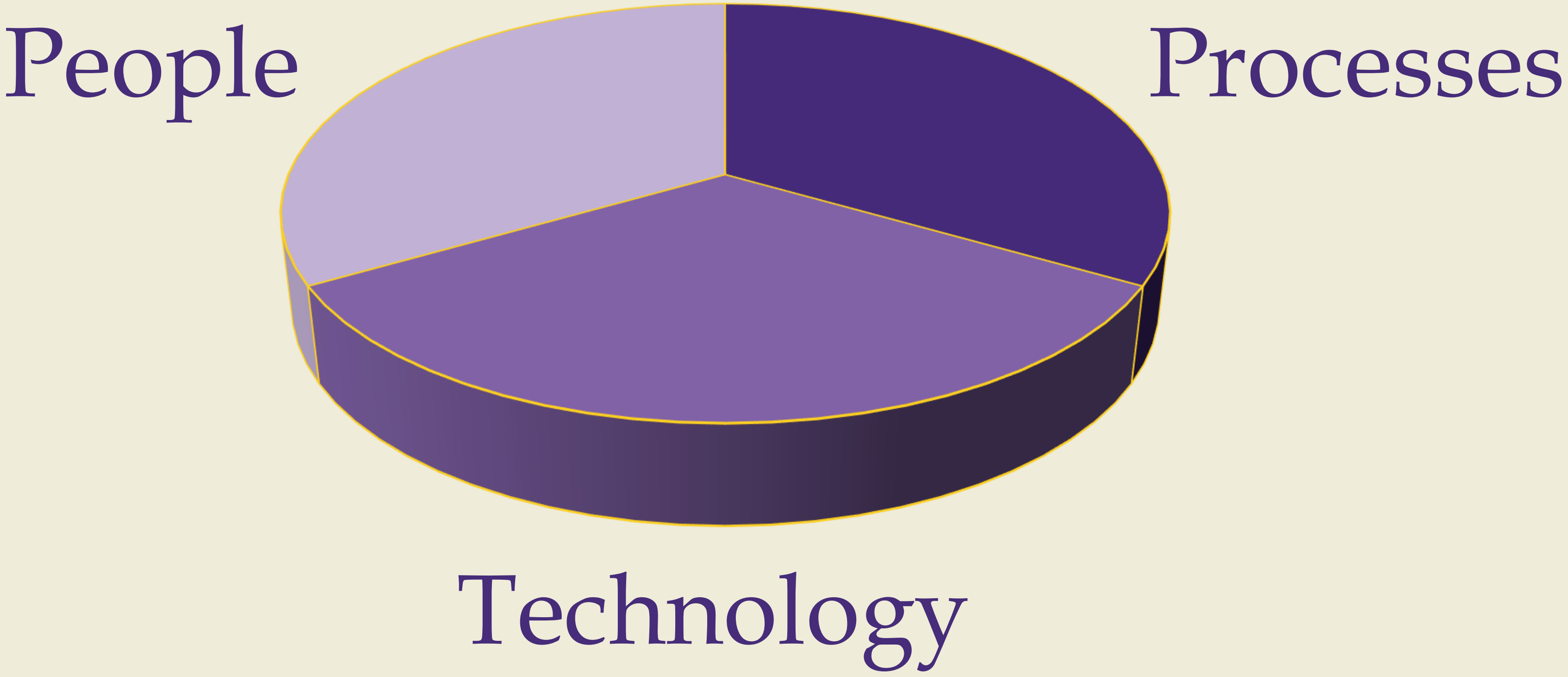
Maintaining PCI Compliance

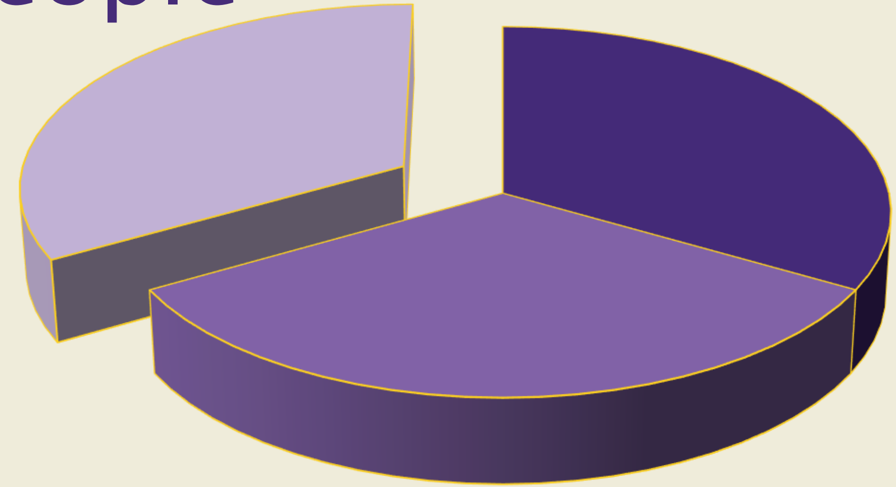
Terms Related to PCI

- PCI-DSS: Payment Card Industry - Data Security Standards
- PCI Council: Representatives from the major card brands that develop the standards
- Merchant: A department that accepts and processes payments cards, and is required to be compliant with PCI-DSS
- Sensitive data: the 16 digit payment card number, expiration date, CVV security code
- Non-sensitive data: Customer name, address, last 4 digits of the credit card number
- P2PE: Point-to-point Encryption. It is encryption software on terminals and point of sale machines that allows them to be plugged into the computer or network in a compliant way

The Pieces of PCI Compliance



People



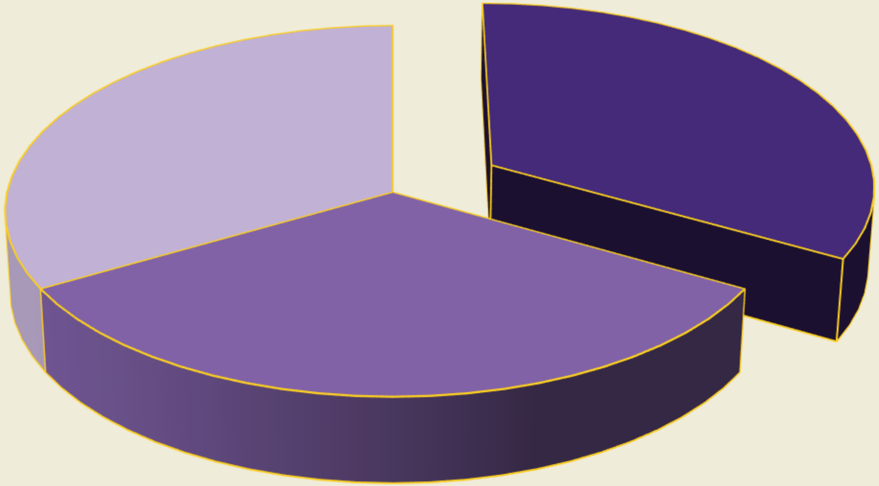
Who does it apply to?

- ➢ Any employees, including students, that are involved in, or manage, the processing of payment card transactions

What is required?

- ➢ Read the university merchant policy, FASOP: AS-22, and be familiar with the applicable policies for your processing environment.
- ➢ Sign and submit form AS539 at hire and annually thereafter
- ➢ Complete the annual online training
- ➢ Complete annual Self-Assessment Questionnaire (SAQ)

Processes

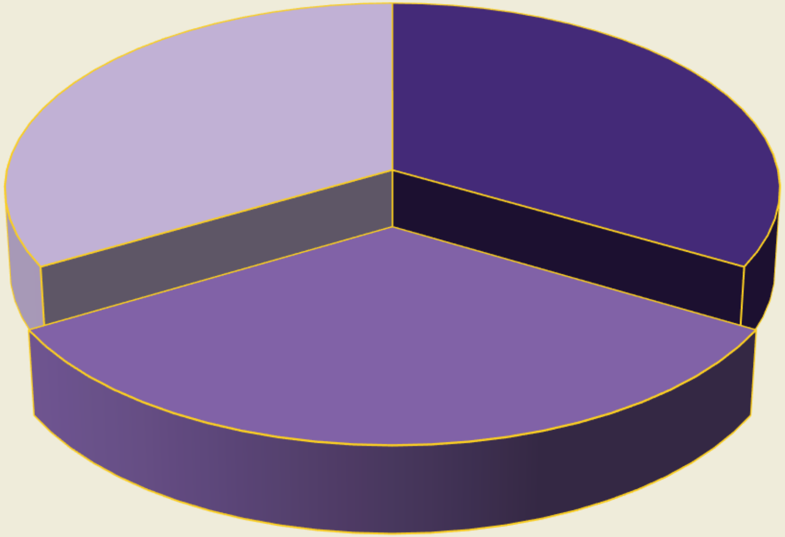


What is included?

- Business processes around receiving, storing, processing, and disposing of sensitive card data

What is required?

- Follow the applicable policies and procedures in FASOP: AS-22
- Have your own written departmental policy to fill in the gaps of the University policy
- Identify and monitor processes that have the potential to be noncompliant



Technology

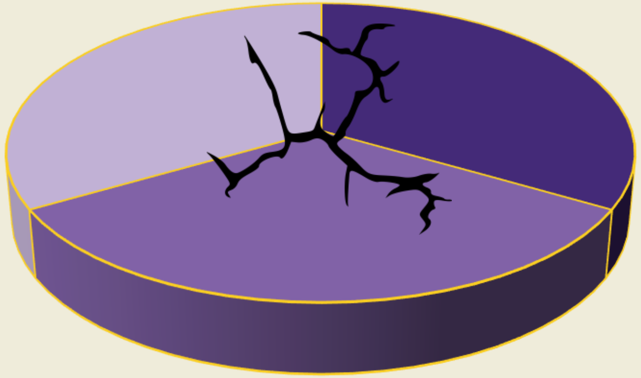
What is included?

- All hardware and software used in capturing and transmitting sensitive card data, as well as potentially anything linked to that hardware

What is required?

- Only use technology (hardware or software) that has been vetted by ITS and Bursar Operations
- Use the technology in the approved manner
- Periodically inspect hardware for tampering
- Annually request proof of compliance from 3rd party vendors

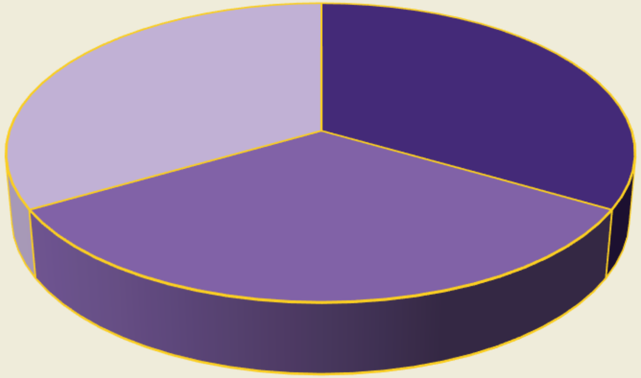
Easy Ways to Become Non-Compliant



- Using your keyboard to enter credit card information on behalf of the customer
  - **Why it is bad:** Your computer is now in scope, the university network is now in scope, and almost every computer on campus is now in scope. The university network and computers are NOT PCI compliant.
  - **What to do:** Direct your customers to your ecommerce site for them to pay, or key the data into a certified terminal if applicable.

- Processing payment data received through email, even if unsolicited
  - **Why it is bad:** Credit card information cannot be accepted by email. By processing the transaction, it is viewed by the PCI council as you accept payment information through email.
  - **What to do:** Direct the sender to a proper payment channel. If you reply to the email, remove the payment information before sending. Delete the original email from your Inbox AND Deleted folder.

Maintaining Customer Service within a Compliant Environment

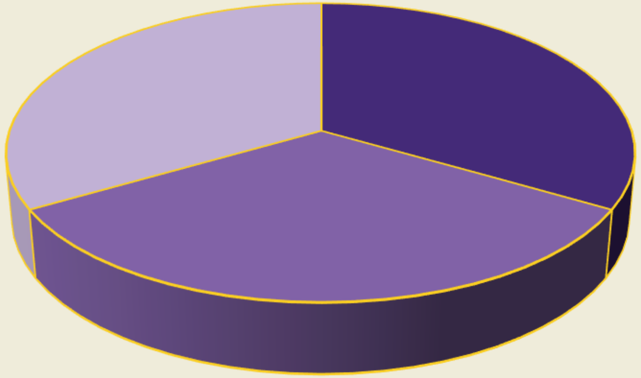


- ➢ If you have a terminal or Point of Sale system, accepting payment information by phone is allowed.
  - ➢ It is preferable to key the data directly into the approved hardware. **Writing it down is acceptable IF the steps below are followed.*
  - ➢ VOIP phones present new challenges, but ITS is aware and working to maintain compliance with the conversion of the phone systems.

* To handle written sensitive card data in a compliant manner:

- ➢ **Have a written departmental policy for your specific procedures.**
- ➢ Keep the sensitive data in a secured location for as short of a timeframe as needed. (A locked area with very limited access.)
- ➢ Immediately shred upon processing using a crosscut shredder. *Do not put into a shredding bin.

Ways to Reduce Your Scope and Make Compliance Easier



- Cashnet eMarket - eCommerce storefront hosted by Cashnet
  - Great for conference registrations, application fees, space rentals, and other non-student related items
  - Integrates with Workday and automatically posts revenue without the need for CARD entries
  - The burden of PCI Compliance is on Cashnet, not the department
    - Employees must still follow university policy regarding the handling of sensitive card data

- Choose reputable third party vendors that can readily provide their compliance status, and that use reputable companies such as Authorize.NET, PayPal, and Stripe to capture customer data

Merchant Resources

- lsu.edu/bursar > Departmental Resources > Merchant Services
- Daniel Butcher: dbutch1@lsu.edu
- Colton Corkern: coltoncorkern@lsu.edu