products to process payment card

C. IP (Internet Protocol) Address – a unique number used to represent every computer in a network. The format of an IP address is typically four sets of numbers separated by dots (e.g. 198.123.123.5), although some newer systems may use an IP address containing eight sets of numbers.

D. Merchant – a payment card merchant is a department or entity that accepts payment cards for payment. An LSU merchant is assigned a merchant account number by the merchant services provider. This number is also the merchant account number for Visa, MasterCard, and Discover transactions. A separate merchant account number is assigned for American Express.

E. PAN (Primary Account Number) – the payment card number.

F. Payment Gateway – a type of service pr (i)-3.316.2 (e p)5.t.0.9 (6.7 (r)3 d [e p)5.3 (a)13..7 ( )1.3 (c)1.1 (a)2

O. **P2PE Solution** A point-to-point encryption (P2PE) solution is provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment. A PCI P2PE solution must include all of the following:

1. Secure encryption of payment card data at the point of interaction (POI)
2. P2PE validated application(s) at the point-of-interaction
3. Secure management of encryption and decryption devices
4. Management of the decryption environment and all decrypted account data
5. Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.

P. **Qualified Security Assessor (QSA)** designation conferred by the PCI Security Standards Council to those individuals that meet specific information security education requirements, have taken the appropriate training from the PCI Security Standards Council, are employees of a Qualified Security Assessor (QSA) company approved PCI security and auditing firm, and will be performing PCI compliance assessments as they25 0cS0 (in)2.7 (p)-0.7 (r)-242e6 (y)-4.5 (p -426.141 f3 (e)-3 (d3 (e1 (o)0 (i5 (o).141 f3p (in)2r)-0.8 (,71

Case A   Redirecting customers using a link from an LSU web page to a PCI approved payment processing service provider or to another company's site.

Case B   Point of Sale (POS) software that is PCI approved and approved by Bursar Operations and Procurement Services. Approval from the LSU A&M Chief IT Security and Policy Officer or by campus-level IT unit and/or IT security personnel at other campuses will be coordinated by Bursar Operations.

Case C   Software that is PCI approved and approved by Bursar Operations and Procurement Services. Approval from the LSU A&M Chief IT Security and Policy Officer or by campus-level IT unit and/or IT security personnel at other campuses will be coordinated by Bursar Operations.

Case D   Wireless device and software that is PCI approved and approved by Bursar Operations an2

Questions	• Is the service provider PCI approved? • Is the service provider linked to another service provider? If yes, is that provider PCI approved? • Does the merchant have access to payment card number? If yes, this is not permitted.
Fiscal Requirements	• All service providers are PCI approved. • Third party contract language applies to all vendors. No access to payment card numbers.
System Requirements	• Successful external vulnerability scan by Approved Scanning Vendor • Successful internal vulnerability scan performed by campus IT. Department must coordinate with campus IT team to schedule such scans. • Implement technical controls to provide a secure computing environment, including all applicable controls required by PCI DSS. • There should be no access to payment card numbers at the redirected site.

Case B – Point of Sale (POS) Merchants
Using terminal connected to a computer to transmit or process payment card information and using PCI approved service providers. POS software must be PCI approved and approved by the university PCI Project Team. Merchants must submit a request to Bursar Operations.

Examples	• Using POS software to transmit or process payment card information. •

eMarkets, where LSU is not the merchant of record, and P2PE solutions are the preferred methods by which the university accepts payment cards.

If it is determined that LSU will be the merchant of record, in order to accept payment cards, a department must complete an AS537 "Payment Card Merchant Agreement and Request" form and return it to Bursar Operations. Upon approval, Bursar Operations will establish a new University merchant account. If at any time there is a question or concern about accepting payment cards, please contact Bursar Operations for assistance at bursar@lsu.edu or (225) 578-3357.