University of California, Riverside
Computing and Communications
Campus Requirements relating to Payment Card Industry Data Security Standard (PCI-DSS)

Which payment card method is used?

UCR purchase orders to vendors supplying Dial-out Terminals or Transaction Processing over Vendor Supplied Wireless Networks must include language stating that their systems are PCI compliant and that vendors must provide an annual attestation that their systems follow industry best practices relating to security.

UC Riverside’s Credit Card Oversight Committee must provide written, formal approval to all UCR entities that intend to process credit card transactions in any fashion (for example, via a POS system, UCR’s Secure Pay system, etc.).

What is Cardholder Data?
As defined by the Payment Card Industry. Cardholder Data includes the full track contents of the magnetic stripe or chip, verification codes and values, PIN numbers, account number, expiration date, cardholder name, and service code.

What is PCI-DSS?
The Payment Card Industry Data Security Standards are a set of requirements designed to ensure that all companies process, store, or transmit cardholder data maintain a secure environment to reduce the risk of fraud.

Who does PCI-DSS apply to?
Any department that has a Merchant ID that accepts payments via credit, debit, or gift cards with an American Express, Discover, JCB, MasterCard or Visa logo; and any individual who processes, stores, or transmits PCI protected cardholder data.

Point-of-Sale or Other Networked Devices
(Networked Processing using Private Networks)

Cardholder Data
- Is accepted by an approved UCR organization
- Uses a network connection to transmit cardholder data
- Do not store cardholder data electronically

Requirements
- POS devices and POS servers must reside on private networks
- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Assign a unique ID to each person with computer access
- Regularly test security systems and processes
- Perform quarterly external scans using an Approved Scanning Vendor (ASV)
- Maintain a policy that addresses information security for all personnel

Annual Reporting and Risk Assessment
UCR entities that process credit cards must provide Computing and Communications an annual report itemizing the devices and systems utilized to support transaction processing. This report is to be submitted as part of the annual inventory of systems that contain personal, protected data or sensitive/essential data as defined by UC security policy IS3.

Dial-out Terminals, Impact Machines, and Vendor Supplied Wireless Networks
(Offline or Standalone Processing)

Cardholder Data
- Is accepted by an approved UCR organization
- Uses a PCI certified device to send encrypted network communication directly to an approved 3rd party vendor
- Does not store cardholder data electronically

Requirements
- Protect non-electronically stored cardholder data (UCR never stores cardholder data electronically)
- Encrypt transmission of cardholder data across open, public networks (or ensure mitigating controls are in place, especially physical security controls)**
- Restrict access to cardholder data by business need to know
- Restrict physical access to cardholder data
- Maintain a policy that addresses information security for all personnel
- Perform quarterly internal scans

** Campus organizations must use compensating controls such as improved physical security if cardholder data is transmitted unencrypted.

Storefronts using SecurePay
(3rd Party Processing)

Cardholder Data
- Is processed by an approved UCR organization
- Does not use a network connection to transmit cardholder data; rather, uses SecurePay to transmit cardholder data
- Does not store cardholder data electronically

Requirements
- Restrict physical access to reports or receipts with cardholder data
- Maintain a policy that addresses information security for all personnel
- Perform quarterly internal scans

PLS