1.6. Payment Card Industry Data Security Standards Compliance Policy

1.6.1. Approval and adoption

1.6.1.1. Approved by the Chief Information Officer and Executive Vice President and adopted effective 5/29/2008.

1.6.1.2. Updated naming of ULV to La Verne, formatting and content of the document. Reviewed and approved by the Chief Information Officer and Vice President for Facilities & Technology Services and adopted effective 11/1/2017.

1.6.2. Purpose

1.6.2.1. To ensure the University complies with the Payment Card Industry Data Security Standards (PCI DSS) and properly protects its constituents' confidential credit card information. Confidential credit card information includes the Primary Account Number (PAN), credit card track data, and 3 digit Credit Card Verification (CCV) number.

1.6.3. Policy

1.6.3.1. No confidential credit card information may be collected and/or stored on University computers at any time.

1.6.3.2. No confidential credit card information may be transmitted over University of La Verne networks at any time unless the information being transmitted is [either from a University-issued credit card or the transmitter's personal credit card] **and** the transmitter is making a payment on behalf of the University using a secure (https://) website.

1.6.3.3. The only approved method for University employees to enter and/or transmit confidential credit card information is via PCI compliant Point-of-Sale (PoS) terminals with secure modem/VPN connections to the credit card authorizing services. These PoS terminals must be models identified by the University of La Verne Finance Department as capable of transmitting the confidential credit card information without storing it.

1.6.3.4. Any websites that collect confidential credit card information from external sources on behalf of the University must perform their

credit card processing through a PCI-compliant service provider validated by the credit card industry. The website that actually collects the confidential credit card information must be located directly on the PCI-compliant site to ensure the data never traverses the University of La Verne network.

1.6.4. Procedure

1.6.4.1. At the request of a functional department or the Finance Division, OIT will conduct a review of PCI compliance by working with a third-party vendor.

1.6.4.2. If necessary and required by the University's credit card merchant acquirer, OIT will arrange for external audits of our network by an approved scanning vendor and will assist with the completion of the PCI Self-Assessment Questionnaire.

1.6.5. Enforcement

1.6.5.1. Violations of any part of this policy will result in disciplinary action as prescribed by University policies and procedures up to and including termination.