Policy Title	**Original Adoption Date**	**Policy Number**
Payment Card Industry – Cardholder Data Security Policy		FS-376
Responsible College Division/Department	**Responsible College Manager Title**	
Financial Services	Director of Financial Services	

Policy Statement

LTC, as a merchant, obtains credit card information from its customers and students, and thus, must comply with PCI DSS. Third party vendors that the college contracts with to process credit card payments and/or capture credit card information must also verify compliance with the standards.

This policy requires that the college staff and contractors protect cardholder data and comply with the requirements of PCI DSS.

Reason for Policy

The Payment Card Industry Data Security Standard is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., International to help facilitate the broad adoption of consistent data security measures on a global basis.

The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any of the major card companies. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. Organizations must be compliant with these standards and must assess their compliance annually.

Historical Data, Cross References and Legal Review

Legal Counsel Review and Approval:
Board Policy:

Definitions