



<p align="center">Policy Title Payment Card Industry – Cardholder Data Security Policy</p>	<p align="center">Original Adoption Date 8/3/2018</p>	<p align="center">Policy Number FS-376</p>
<p align="center">Responsible College Division/Department Financial Services</p>	<p align="center">Responsible College Manager Title Vice President of Administration</p>	
<p align="center">Policy Statement</p> <p>Lakeshore Technical College (College) handles sensitive cardholder information daily. Sensitive information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organization. The College commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.</p>		
<p align="center">Reason for Policy</p> <p>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.</p> <p>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.</p>		
<p align="center">Historical Data, Cross References and Legal Review</p> <p>Review/Revised: 3/5/2019</p> <p>Cross Reference:</p> <p>Payment Card Industry – Cardholder Data Security Procedures www.pcisecuritystandards.org PCI DSS v3.2.1</p> <p>Protection of Sensitive and Restricted Information Policy Payment Card Industry-Cardholder Data Security Procedure</p> <p>Legal Counsel Review and Approval: Board Policy: III.F. Asset Protection</p>		
<p align="center">Definitions</p>		