SOUTHWESTERN COMMUNITY COLLEGE	BUSINESS SERVICES **PAYMENT CARD SECURITY**	Policy 7.03.09

Credit card processing at Southwestern Community College complies with the Payment Card Industry Data Security Standards (PCIDSS). The following security requirements have been established by the payment card industry and adopted by the College to ensure compliance with the payment card industry. These requirements apply to all employees, systems, and networks involved with credit card processing, including transmission, storage, or electronic and paper processing of credit card numbers.

Authorized Employees

Credit card processing for official college business is restricted to Business Office personnel only. No other College employees are authorized to process such information for any reason.

Training

College employees who process credit card information or who have access to this information will complete annual data security training.

Procedures

Each College employee who processes credit card information must strictly adhere to the following:

- Access to credit card information is restricted to Business Office personnel.
- System and desktop passwords must be changed regularly in accordance with Policy 4.05.01 - Computer Resources, Internet and Network Acceptable Use Policy.
- Accounts should be immediately terminated or disabled for employees who leave employment with the College.
- Credit card information should not be stored in any format.

Data Retention

Credit card information, including the card number, cardholder name, CVV code, and expiration date should not be retained for any reason.

Restrictions

Employees may not send or process credit card data in any insecure manner including: transmitting such data via mail, courier, email, or instant messaging. Credit card information may not be left exposed to anyone.

Network and Infrastructure

The Information Technology Department maintains additional procedures to ensure compliance with PCIDSS. These include:

- Configuration of card processing environments procedures, including segmentation of local area networks and protection through deployment of firewalls;
- Logging control procedures;
- Wireless use procedures; and
- Encryption procedures

Compliance

The College shall annually submit a PCIDSS security questionnaire maintained by Trustwave/Trustkeeper and required by the North Carolina Community College System to ensure compliance with the PCI Data Security standards.

Cross Reference: 4.05.01 – Computer Resources, Internet and Network Acceptable Use Policy;
7.03.10 – Identity Theft Red Flag Policy

Adopted: July 2014