Jamestown Community College
Policies and Procedures

Policy Title	**Payment Card Industry (PCI) Compliance Policy**	**Policy Number**	**208**
Section	**Financial Affairs and Development**	**Approval Date**	**10.15.2019**
Subsection	**General Financial Policies**	**Effective Date**	**10.15.2019**
Responsible Office	**Information Security Committee**	**Review Date**	

1.0 Purpose

1.1 The purpose of this policy is to help prevent loss or disclosure of credit card customer information, including credit card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the department and College.

1.2 Jamestown Community College's (JCC) Payment Card Industry (PCI) Compliance Policy applies to those involved with payment card handling including: faculty, staff, students, third-party vendors, individuals, systems, networks, and other parties with a relationship to the university including auxiliary service corporations, alumni associations, student associations and governments, JCC Foundation and any unit using third-party software to process credit card transactions. This includes transmission, storage, and processing of payment card data, in any form (electronic or paper.)

2.0 Policy

2.1 All card handling activities and related technologies at JCC are required to comply with the Payment Card Industry Data Security Standards (PCI DSS). No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI DSS.

2.2 The college prohibits the storage of credit card information and the transmission of credit card data through fax, email, paper forms, social media, end-user messaging, or non-certified third-party vendors for web-based credit card processing. The college prohibits the retention of complete payment card primary account numbers (PAN) or sensitive authentication data in any college system, database, network, computer, tablet, cell phone, or paper file. The storage of truncated numbers, in approved formats (first six digits OR last four digits), is permissible.

2.3 At no time will the requirements of the PCI DSS supersede local, state, and federal laws or regulations.

3.0 Procedures

3.1 All members of the college community are required to:

- Safeguard cardholder data
- Report occurrences of possible incidents and data breaches to the employee's supervisor or JCC's Information Security Officer

3.2 JCC's Information Technology Department will be responsible for:

- Maintaining security standards as required by PCI DSS
- Keeping current with PCI DSS regulations and make applicable changes to systems and processes, as appropriate
- Consulting on technical PCI DSS issues

3.3 JCC's Human Resources Office will provide mandatory, annual training sessions on PCI compliance and will monitor and enforce compliance.

3.4 JCC's Business Office will be responsible for:

- Keeping current with PCI DSS regulations and make changes to processes, as appropriate
- Maintaining an inventory of all JCC departments that process credit card transactions using an approved merchant account
- Coordinating the completion of the appropriate annual self-assessment documents (SAQs).
- Evaluating compliance to PCI regulations as part of the scheduled cash handling reviews.

3.5 Department Heads who accept credit card payments other than through approved online methods are responsible for:

- Completing the annual PCI compliance training through Human Resources
- Ensuring that applicable staff complete the annual PCI compliance training through Human Resources
- Verifying that staff understands and complies with PCI compliance policy and procedures

3.6 Credit and Debit Card Handlers and Processors are responsible for:

- Following the established cash receipts procedures for the appropriate funding source
- Completing the annual PCI compliance training through Human Resources
- Completing required annual PCI DSS training

3.7 Third Party Payment Card Processors are required to provide confirmation of compliance.

3.8 The College is required to comply with all relevant standards. However, not all of the PCI DSS requirements are relevant to JCC.

4.0 Definitions

4.1 Cardholder. Someone who owns and benefits from the use of a membership card, particularly a credit card.

4.2 Cardholder Data (CHD). Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date, and the Service Code.

4.3 Cardholder Name. The name of the Cardholder to whom the card has been issued.

4.4 CAV2, CVC2, CID, or CVV2 data. The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

4.5 Disposal. CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes and USB storage devices. The approved PCI DSS disposal methods are: crosscut shredding, incineration, or secure disposal service.

4.5 Expiration Date. The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

4.6 Magnetic Stripe (i.e., track) data. Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

4.7 Merchant. Any department or unit (can be a group of departments or a subset of a department) which has been approved to accept credit cards and has been assigned a Merchant identification number.

4.8 Payment Card Industry Data Security Standards (PCI DSS). The security requirements defined by the Payment Card Industry Security Standards Council and the major Credit Card Brands.

4.9 PIN or PIN block. Personal Identification Number entered by cardholder during a card-present transaction, or encrypted PIN block present within the transaction message.

4.10 Primary Account Number (PAN). Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

4.11 Self-Assessment Questionnaire (SAQ). The PCI DSS self-assessment questionnaires (SAQs) are validation tools to assist merchants and service providers report the results of their PCI DSS self-assessment.

4.12 Sensitive Authentication Data. Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN or PIN block.

4.13 Service Code. The service code that permits where the card is used and for what.

5.0 References

5.1 PCI Security Standards Council. https://www.pcisecuritystandards.org

5.2 Payment Card Industry Data Security Standards (PCI DSS) V3.2

5.3 Payment Card Industry Data Security Standards (PCI DSS) compliance requirements, as outlined below:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel