Rock Valley College

Credit Card Procedure

RVC Administrative Procedure (2:30.060)

Purpose

The purpose of this Procedure is to establish and define requirements for collecting, processing and transmitting credit card data to ensure proper control and integrity of data as well as to facilitate compliance with PCI DSS (defined below) requirements. These standards are designed to assist Rock Valley College (RVC) in the safekeeping of cardholder information, which in turn reduces the chances of security breaches, fraud, and potential financial losses.

Scope

This Procedure applies to all RVC employees, faculty, agents, students, contractors, vendors, guest, consultants, temporary employees, and any other users who accept donations or sell goods, services, or information, and accept credit cards as a form of payment.

All computers and electronic devices used for processing payment card data are governed by PCI DSS. This includes workstations that are used to enter payment card information, and computers or credit card swipe devices through which payment card information may be transmitted.

Definitions

1. **Payment Card Industry Data Security Standard (PCIDSS)** is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). 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 that hold, process, or pass cardholder information.

2. **Cardholder Information/Data** is any personally identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card referred to as CVV2 or CVC2), and any information which would permit access to an individual's financial account.

Department Responsibilities

Departments are responsible for knowing and complying with PCI DSS and College policies and procedures to safeguard credit card and other personally identifiable or

sensitive information. Departments must also follow established procedures to ensure that cardholder information is handled and stored securely.

This applies to all transactions regardless of the type of transaction (phone, in-person, mail, web, etc.).

Establishing Payment Card Services

Any department wishing to accept credit cards for goods or services must first contact the Vice-President of Operations/COO and Vice-President of Finance/CFO regarding their needs. Final selection of a purchasing solution requires formal approval by both the CFO (or designee) and the COO (or designee).

All transactions that involve the transfer of credit card information must be performed on systems approved by the Department of Information Technology and will include a compliance and security review; for clarity, Cardholder Information shall never be used on a personally owned device for PCI transactions or storage. Approval MUST be obtained prior to entering into any contracts or purchases of software and equipment relating to credit card processing. This requirement applies regardless of the transition method of technology used.

Security or Cardholder's Information

Cardholder Information is obtained either by the cardholder being present (credit card present) or by transmitting cardholder information (telephone, Internet, etc.). All individuals authorized to accept credit card payments must securely process and dispose of credit card data to adhere to PCIDSS.

On any materials which document a transaction made using a credit card, credit card numbers must be masked to protect account information for all users except those who have a legitimate business need. The first six or last four digits are the maximum number allowed to be displayed. If any card information is written down while performing the transaction, that information must be shredded once the transaction has been completed.

It is not permissible to transmit or obtain credit card information by email, PDAs, instant messaging, chat applications or other unsecure methods unless otherwise approved by the COO and CFO.

If an email containing cardholder data is received, immediately delete the email, and notify the sender that the College does not accept cardholder data via email and that the transaction will not be processed. In the response, give the customer a list of alternative methods of sending their card information (mail, phone, or secure fax). If you reply to the original email, you must remove any card information before sending the message. Also, be sure to delete the message from your email inbox, sent box, and deleted box.

Report any suspected exposure (to unauthorized parties) or loss of cardholder data to the Department of Information Technology immediately. This includes lost or

stolen files with credit card numbers, electronic loss of data, databases infected with viruses and any other loss or potential loss.

Allocation/Purchase Card Transactions

Rock Valley College's purchase card transactions are required to be accurately allocated no later than the fifth day of the calendar month. This is due to the College grant programs, which must conduct mandatory reporting by the tenth day of each month. Failure to meet the tenth day deadline could result in loss of the grant.

Transactions are typically available for allocation in the American Express Website two days after purchase. You can allocate those charges at any time. Best practice is to schedule yourself a reminder once a week to complete allocations.

Use of the purchase card is a privilege and non-compliance with timely allocation of purchase card activity may result in the loss of your purchase card.

Enforcement

All requests for clarifications or interpretations of this procedure should be directed to the Vice President of Operations/COO.

Implemented: March 2023