Policy

Title	**Credit Card Number Handling**		
Classification	Administrative	**Oversight & Responsibility**	Office of the VP & CFO; Finance
Category	Financial Management	**Effective Date**	2014 Oct 01
Approval	Executive	**Policy No**	1062

This policy is applied in a manner consistent with applicable statutory and legal obligations, including university collective agreements and terms of employment.

NOTE: The most up-to-date versions of our policies are posted on the policy & procedure website. If you've printed this policy, check the website to be sure you have the current version.

Policy Statement

The University must protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with the University. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.

Rationale

Credit card transactions have become the preferred method for making payments or donations to the University. Every business that accepts credit and debit card payments is required to comply with the Payment Card Industry Data Security Standards (PCI-DSS). Additionally, the University's reputation would be seriously damaged by the exposure of credit or debit card numbers. To comply with the PCI-DSS, employees who work directly with credit card processing and documentation are required to review and sign this policy on an annual basis.

Applicability of the Policy

This policy applies to any department chair or department administrator with responsibilities for managing university credit card transactions and to those employees entrusted with handling credit cards and credit card information.

Definitions

Cardholder Data - The full magnetic stripe of the card or the entire card number plus any of the following: cardholder name, expiration date, service code.

PCI DSS - The Payment Card Industry Data Security Standard was adopted to assure the protection of customer data and credit card numbers.

PCI Environment - Includes computers, network hardware and the segment of the RRU network (PCIVLAN) configured to meet the PCI standards for electronic submission, processing or storage of cardholder data.

Procedures for Access to Customer Credit Card Data

- Access is authorized only for University personnel who are responsible for processing or facilitating credit card transactions.

© Royal Roads University 2021

- Only authorized University personnel may process credit card transactions or have access to documentation related to credit card transactions.
- A copy of this policy must be read and signed by authorized personnel on initial employment and annually thereafter.

Telephone Payments
- When recording credit card information for processing via a dial-up terminal, only cardholder name, account number and expiration date may be recorded. The three-digit security code (CVV2) can be recorded for initial authorization but the record must be shredded after authorisation has been received.
- Store transaction documentation and merchant receipt in a secure (locked) area.

Fax Payments
- Collection of credit card information using an electronic fax machine is discouraged, but permitted. The fax machine should be a non-networked machine hooked up only via a phone line and accessible only to department staff. No credit card information should be received through multi-purpose machine such as a copier/scanner/printer/fax machines.

Card Present Transactions (Point of Sale)
- Picture ID is required if the card is not signed. Provide receipt to customer.
- Store transaction documentation and merchant receipt in a secure (locked) area.

Receipt of Credit Card Information in Email
- Under no circumstances will credit card numbers received in email be processed.
- The recipient of the credit card number will respond to the sender with a standard template advising that the transaction cannot be processed and offering an acceptable method for transmitting card information. Credit card numbers will be deleted from the response.

Processing Credit Card Transactions and Storage of Cardholder data on Campus Computers
- Offices that make payment card transactions on the web (that is, enter a customer's credit card number on a website in payment for a purchase at or donation to the University) must do so from a computer designated for that purpose on the campus PCI VLAN.
- Card numbers must not be entered on any computer that is not expressly designated as belonging to the PCI environment.
- Cardholder data should not be stored electronically. If there is a documented requirement for such storage, appropriate encryption must be used and data must be stored on a computer belonging to the PCI environment.
- Any documents or receipts that include a credit card Personal Account Number (PAN) must have the PAN masked in accordance with current PCI standards.

Delivery of Transaction Documents to Financial Services
- Documents/Forms containing credit card information should be delivered to Student Accounts through the security deposit bag or be personally delivered to Student Accounts.
- Never send credit card information through campus mail.

Securing Transaction Documents (for Financial Services staff)
- At work station, store securely until session materials are placed in safe at end of day.
- Any transaction documentation retrieved from the safe for review or refund purposes must be handled securely and placed back in the safe as soon as possible but no later than the end of the business day.
- Credit card transaction documents must be stored in the safe. When retention period passes it may be taken from the safe and destroyed (shredded) immediately.

Retention and Destruction of Cardholder Data

- Cardholder data should be retained in a secure location only as long as is necessary for business purposes. It is not permissible to store the three-digit security code (CVV2).
- Cardholder data will be destroyed when no longer needed. Paper will either be shredded using a cross cut shredding device, incinerated or pulped. Electronic files will be destroyed in a manner appropriate to the media on which they are stored
- Cardholder data should be retained in a secure location only as long as is necessary for business purposes. It is not permissible to store the three digit security code (CVV2).
- Cardholder data will be destroyed when no longer needed. Paper will either be shredded using a cross cut shredding device, incinerated or pulped. Electronic files Royal Roads University Page 6 of 6 21 October 2014 will be destroyed in a manner appropriate to the media on which they are stored

Contacts

Questions related to this policy can be emailed to the following address: pci@royalroads.ca

Template Response* for Credit Card Number Received in Email

Thank you for your recent communication regarding payment for item or event . For your protection, we cannot accept credit card information via email. Email is an insecure means of transmitting information and you should never use it to send your credit card number or other sensitive personal information (passwords, Social Insurance Number, etc.). Please call our office at phone number during regular business hours to complete the transaction or visit website if available. Thank you.
*Delete the cardholder data from your response and delete the original message after replying.

Related Documents and Information

Related Other Sources

- PCI DSS – The Payment Card Industry Data Security Standard

Review and Revision History

Date	Action
2014-Oct-01	Approved by Executive; current published version
2021-Oct-15	Transfer to new template – no content change
Next Review	
2017-Oct-01	For review