Treasury's Credit Card Merchant Business Practices Checklist

Precard Acceptance Business Practices Checklist – business practices that ought to be in place BEFORE a unit starts to accept card payments

(Note: each campus may have its own similar checklist.)

Yes	No	Item
		(Overall) Is the department currently employing good business practices for handling non-credit card payments?
		Do cash / deposit handling procedures conform to the campus's cash control policies and procedures? • Boulder campus (Cash Control chapter of the System Accounting Handbook): https://www.colorado.edu/gsearch/all/cash%2Bcontrol • Colorado Springs campus: (See System) • Denver campus: http://www.ucdenver.edu/faculty_staff/employees/policies/Policies%20Library/Fiscal/CashReceipts.pdf • System (Cash Control chapter of the Accounting Handbook): http://www.cu.edu/controller/cash-control
		Are all transactions and deposits processed daily?
		Are transaction, cash/deposit handling, and reconcilement duties performed with proper segregation of duties? If not, what supervisory controls are in place to ensure proper oversight?
		Are refund transactions properly controlled? That is: • Are refunds approved by a supervisor before funds are returned to the payee? (Dual controls on disbursements) • Are refund transactions properly documented and accounted for?

Yes	No	Item
		(Overall) Is the department currently employing good business practices in accounting for all payment transactions?
		Does staff understand the necessary accounting flows for transactions, and are they being properly posted?

		Are daily detail financial reports, statements, and any other applicable reports reconciled timely?
		Does the unit have the financial resources to reconcile deposit transactions daily, if it is not already being done for non-credit card deposits?
		Are the unit's speedtypes managed in a fiscally sound manner?
		Are internal records well organized, and can past transactions be readily identified and source documents quickly retrieved from the filing system (up to three years later)?
		Are document retention and destruction policies in place and followed? Do they conform to the campus and/or System record retention and destruction policies?
		Are documents securely destroyed when their retention time is completed?
Yes	No	Item
		Does the unit have **locked** file storage available for the retention of credit card payment detail on paper? (Not just storage in a locked room.) Do they actually **lock** the file drawer or cabinet when not in use?
		If paper records with cardholder information are going to be generated, is the unit's archival storage secure? (That is, if the unit sends its old records to campus storage, is that storage secure?)
		Does the unit have paper shredding capability for record destruction for paper containing cardholder information? Cross-cut shredding or outsourced, secure data destruction services are required.
		Does the unit have sufficient resources (staff, expertise, funding, etc.) to take on any more functions such as accepting and processing credit card payments and the additional account reconciliations required?
		Does the unit understand the Treasury policy that requires that only paid University staff (not volunteers) process all payments, including credit card transactions? (Paid student staff qualify.)
		Does the unit understand that they must pay for the costs of credit card merchant acceptance out of their own budget, and not charge more for payments by credit card than by other means?

Yes	No	Item
		How does the department intend to accept / process cardholder information for card payments? Check all that apply: ❒ On paper (via postal mail or in person) ❒ Via telephone (with information written on paper) ❒ Via fax ❒ Via email (strictly prohibited for security reasons) ❒ Paper forms brought to Bursar office for processing (UCCS, Denver campuses only) ❒ Using software on a PC ❒ Via a browser from their desktop PC ❒ Via the unit's web site ❒ Completely outsourced to a third party vendor / processor ❒ Other method (please describe):
		Does the unit have a physically secure fax machine available for receiving reports and chargeback notices with cardholder information on them? (Must be physically isolated from the general public.)
		Does the unit understand that it is prohibited from storing cardholder data in any electronic form whatsoever without prior approval of the campus IT Security Principal and of the Treasurer's Office?
		Does the unit understand that they must respond to and report any and all incidents that might entail cardholder data, whether that data is on paper, in electronic form, or in the possession of a third party vendor?
		Has the unit created a Data Flow Diagram showing the path of all cardholder and related data through their business processes? (This is a requirement for all units accepting card payments.)
Comments:		
Yes	No	Item
		Has the unit created an Incident Response plan that follows the Treasury's incident response plan template?
		Does the unit understand that it must understand, adopt and implement a security policy for protecting cardholder data?

		Does the unit have a training program for new staff, or staff accepting new payment processing responsibilities that include card payments?
		Is the unit aware of the security requirements for accepting payments online, if applicable?
		Does the unit have the IT staff and security knowledge to create and maintain a secure online payment web site, if applicable?
		Has the unit consulted with the campus IT Security team regarding their security obligations for processing online card payments, if applicable?

The following additional questions can be used to assess the business practices of current card-accepting merchants:

Yes	No	Item
		(Overall) Is the unit currently employing good business practices in handling card payments?
		Have there been any recent incidents that would indicate problems in processing payments, including credit cards? (Downgrades, missing deposits, delayed settlement, etc.)
		Has there been more than the normal number of chargebacks / disputed transactions?
		Are all transactions and deposits processed and accounted for daily?
		Does there continue to be proper segregation of duties, or other compensating controls in place to ensure proper oversight?
		Are refund transactions properly controlled? That is: ❒ Approval by a supervisor before funds are returned to a payee? ❒ Are refund transactions properly documented and accounted for? ❒ Are the unit's refund policies clearly disclosed to customers? ❒ Are refunds on credit cards credited only to the same card that was used for the original transaction? ❒ If the original card has expired, does the unit refund funds via the normal accounts payable process (that is, a check)?

Yes	No	Item
		Does the unit respond timely to chargebacks / disputed items? (Within 14 calendar days of notification of dispute.) Are faxed chargeback notices promptly processed or forwarded to the unit?
		Have there been significant changes in the number or dollar volume of card transactions? Are the reasons for such changes understandable?
		(Overall) Is the department continuing to employ good business practices in accounting for all payment transactions, including credit card payments?
		Have there been any recent problems that might indicate a need for review of proper accounting and/or reconciling procedures?
		Are account reconcilements completed properly and timely?
		Have there been recent personnel changes that might indicate a need for a review of good business practices with the unit?

Resources	
Treasurer's Office	https://www.cu.edu/treasurer/ Lexie Kelly 303-837-2182 Alexis.kelly@cu.edu
Payment Card Industry Data Security Standard (PCIDSS)	https://www.pcisecuritystandards.org/
CU APS #4056, Payment card compliance program	https://www.cu.edu/ope/aps/4056