Third Party Vendors [1]

Approved third party vendors and approval process

Cvent - An online platform to manage your events using Cvent, eComm's event management platform. CU departmental staff can build forms for both simple and complex events. The CU Office of the Treasurer has authorized Cvent as an approved vendor to accept secure credit card payments. You can easily customize the design of your event form and website, even if you don't know HTML. For more information about the program and instructions on how to contact your campus leadership team, go to https://www.cu.edu/ecomm [2].

Eventbrite - An online platform for event and seminar registration available to CU departments. Contact Lexie Kelly (alexis.kelly@cu.edu [3]) for more information if Cvent is not an option for your event.

Nelnet Campus Commerce - An electronic payment service provider used across the campuses for electronic student bill presentment and electronic student payment processing using Automated Clearing House (ACH) debits, credit cards and debit cards. The Commerce Manager portal within Nelnet Campus Commerce is available for departments accepting online payments tied to admission applications and program deposits.

Authorize.Net - The primary payment gateway provider integrated with a Wells Fargo merchant account for CU departments processing online payments. Authorize.net allows departments to accept credit cards and electronic checks from websites and deposit funds automatically into their merchant bank account. The solution offers fraud protection services, recurring billing subscriptions, and checkout options.

Adding new merchant accounts/vendors: If your department would like to open another merchant account, or contract with a third party vendor to accept credit card payments, start the process early by contacting the Treasurer's Office and your campus Internal Security Assessor to discuss options. If a third party vendor has already been vetted and approved by the University, the process will be easier and quicker. If a vendor is not currently under contract with the University of Colorado, please allow 3 months for Payment Card Industry review and contract negotiations after the request has been submitted to the Procurement Service Center.

If a potential third-party vendor processes payment card transactions, the vendor MUST be vetted and approved for PCI compliance, regardless of dollar amount.

University of Colorado Boulder Campus

Outsourcing agreements to third party vendors must be preapproved in writing by the Campus

Controller, Treasurer's Office and IT Security Office prior to the execution of any agreement. Departments may be required to use preapproved vendors unless there exists a legitimate business need. All third party providers must meet the standards set forth by the PCIDSS. Outsourcing agreements must also comply with Procurement Service Center (PSC) procedures. In the event that the actual processing of credit card transactions is outsourced, various training and duty requirements will differ as noted below, but the principles are the same. Any requisition that appears to be for the purchase of information communication technology (ICT) goods or services has to be reviewed and approved by the ICT program. The Boulder campus policy, available at http://www.colorado.edu/accessibility/ [4], requires that these purchases be reviewed for accessibility before proceeding. Please visit the ICT Integrity page for more information about the process and to submit a request for review: http://www.colorado.edu/ictintegrity/ [5].

The link to the Boulder ICT program: http://www.colorado.edu/ictintegrity/ict-review-process [6]

Procedural Statement can be found here:
https://www.colorado.edu/controller/sites/default/files/attached-files/P... [7]

The Boulder campus Internal Security Assessor, Lincoln Nkin, can be contacted at: OIT-DL-PCI-DSS@colorado.edu [8]

University of Colorado Denver/Anschutz Medical Campus

Third party vendors are now subject to the same Security Rule requirements as Covered Entities, and are also subject to relevant sections of the Privacy Rule and the HITECH Breach Notification Rule. In order to protect university confidential and highly confidential data, including PHI, the risk and compliance team assesses the security and practices of all third party vendor server applications and cloud services. Third party vendor applications include those that process, transmit or store PCI (Payment Card Industry) data.
Third party vendors must:

- Prevent the loss, theft, unauthorized access and/or disclosure of university data
- Destroy data when no longer needed per university data owner instructions
- Have incident response procedures and reporting requirements in case of a breach

For more information about the approved applications and assessment process go to:
https://www1.ucdenver.edu/offices/office-of-information-technology/softw... [9]

The Denver/Anschutz campus Internal Security Assessor team, Mike Adamson and Josh Hsa, can be contacted at: UCD-OIT-RAC@ucdenver.edu [10] UCD-OIT-RAC@ucdenver.edu [10].

University of Colorado Colorado Springs Campus

The UCCS Card Acceptance and Security Policy states that outsourcing agreements to third party vendors must be preapproved in writing by the Campus Controller and Treasurer's Office prior to the execution of any agreement. All Third party providers must meet the standards set forth by the Payment Card Industry Data Security Standard (PCIDSS) and be certified. This certification must be obtained before vendor is contracted and reaffirmed annually. The Treasurer's Office can assist with the vendor certification determination.

The UCCS Credit Card Acceptance and Security Policy can be found at this site: https://www.uccs.edu/Documents/vcaf/policies/2011/500-012.pdf [11]

The Colorado Springs campus Office of Information Security team contact information can be found here: https://www.uccs.edu/oit/people/security. [12] The Internal Security Assessor is Neil Kautzner.

Third Party Service Providers

A third-party service provider is a business entity directly involved in the processing, storage, or transmission of transaction data or cardholder data on behalf of the university. They also include companies or organizations that provide services that control or could impact the security of cardholder data, or manage system components – such as routers, firewalls, databases, physical security, and/or servers – in their CDE. When an entity is processing, storing or transmitting cardholder data on behalf of the university, or they have access to university's cardholder data, they are a service provider.

The use of a third party service provide does not relieve the CU merchant of ultimate responsibility for its own PCI DSS compliance, or exempt the university from accountability and obligation for ensuring that its cardholder data and Cardholder Data Environment are secure.

At this time, phone add-on devices like Square cannot be used to accept credit card payments on behalf of the University of Colorado.

Groups audience:
Treasurer

Source URL: https://www.cu.edu/treasurer/merchant-services/third-party-vendors

Links
[1] https://www.cu.edu/treasurer/merchant-services/third-party-vendors
[2] https://www.cu.edu/ecomm
[3] mailto:alexis.kelly@cu.edu
[4] http://www.colorado.edu/accessibility/
[5] http://www.colorado.edu/ictintegrity/
[6] http://www.colorado.edu/ictintegrity/ict-review-process
[7] https://www.colorado.edu/controller/sites/default/files/attached-files/Policy%20-%20Credit%20Card%20Acceptance.pdf
[8] mailto:OIT-DL-PCI-DSS@colorado.edu
[9] https://www1.ucdenver.edu/offices/office-of-information-technology/software/secure-campus/security-approved-software
[10] mailto:UCD-OIT-RAC@ucdenver.edu

[11] https://www.uccs.edu/Documents/vcaf/policies/2011/500-012.pdf
[12] https://www.uccs.edu/oit/people/security.