CSU CREDIT CARD PROCEDURE AND POLICY

1. **This policy applies to all forms of credit card processing whether existing, new or changed services on behalf of the University or by affiliates using University systems.** Credit card processing includes any payment card transaction (whether credit card, debit card, or other instrument linked to such a card) or other transmission, processing or storage of credit card data regardless of the means by which that transaction is actuated. This includes transactions initiated in-person, via the telephone or other telephonic means, in paper form, by US mail or other courier, through a terminal, kiosk, computer system, website, mobile device or any other means. This policy applies to whether the processing is performed by the University or by an outside party acting as a service provider to the University.

2. **All units that wish to process credit card transactions must establish request approval of Business and Finance** before initiating any credit card transactions, and to establish the valid business purpose of the proposed arrangements.

3. **All units that wish to process credit card transactions must obtain a University credit card merchant ID account from the Bursar's Office.** Units within the University or affiliates using the University's systems may not negotiate their own contracts with credit card companies, processors, or external services that accept credit card payments on the University's behalf. A University department accepting credit cards is deemed a credit card merchant. Only the Bursar's Office is authorized to issue University credit card merchant ID account numbers, which are required for University acceptance of credit card payments and to enable deposits through the Bursar's Office. University departments must comply with this policy and all related security policies in order to maintain their credit card merchant IDs. Credit card merchants are expected to protect cardholder data and prevent the unauthorized use of that data.

(Cardholder data refers to information printed, processed, transmitted or stored in any form from a credit card. Cardholder data elements include the primary account number (PAN), cardholder name, service code, and expiration date. Units may retain only the first six (6) digits and/or last four (4) digits of the PAN, as these data are not considered to be cardholder data under PCI DSS.)

4. **All system and service components utilized for credit card processing must be purchased through an approved University vendor for such purposes.** The University is establishing contracts, incorporating the necessary security provisions, for many system and service components needed for the acceptance and processing of credit card transactions. Where such contracts exist, all units processing credit card payments, e.g., through the World Wide Web, are required to use them. If a required service is not already covered by a University contract, the unit must work through Procurement and Accounting Services to identify and contract for approved necessary services and ensure the security of those services. Procurement and Payment Services will engage IT Services and the Bursars Office in the approval process.

5. **Credit card information is not accepted via e-mail and units may not retain any paper records with credit card information.** Any associated paper or other records or reports containing credit card customer information shall not be maintained unless absolutely necessary as determined by the unit or divisions department head or Vice President or equivalent. If absolutely necessary to maintain, the paper shall be stored in locked and secured cabinets. Access to credit card information and the processing of credit card payments should be limited to those individuals whose job requires such access, and

6. **Departments are responsible for informing the Bursar's Office of all employees in their unit who accept or process credit card transactions and requiring there employees document they have read the university's PCI compliance policy.**

7. **Departments who suspect a breach and/or fraud involving credit cards should contact the Controller or VP of Business Operations, Bursar and IT immediately.**

8. **Annual training is mandatory for any employee involved with credit card processing.** All employees involved in credit card acceptance and processing must complete an annual certification of compliance training. Additionally, new employees involved in credit card acceptance and processing must complete training before they can assume credit card acceptance and processing responsibilities in their area. Failure to complete training successfully may result in the loss of the merchant's ability to process credit card transactions.

9. **Units are responsible for timely communication with the Bursar's Office or IT Services regarding any credit card inquiries or requests for information.** All university merchants must respond to communications from the Budget and Finance, Bursar's Office or IT Services regarding credit card processing in a timely manner, including any surveys, annual questionnaires, or other inquiries. Some of these communications may be date sensitive, and failure to respond appropriately within the period indicated may result in the loss of the merchant's ability to process credit card transactions.

10. **Units are fully responsible for any and all fees associated to the merchant ID.** The University is charged fees on all credit card transactions. At month end, these fees will be charged to the unit based on that unit's activity. Additionally, some service providers may impose annual, one-time, or other fees for their services, and these are the responsibility of the merchant department. Any fines or other fees and costs resulting from non-compliance with Payment Card Industry security standards, including but not limited to those resulting from breaches of security or failure to complete annual training, will be the responsibility of the department where the failure occurred.

11. **Non-compliance with this policy may result in termination of card processing abilities for the individual and/or unit.** Units or individuals found to be acting outside of this and related policies or establishing non-approved credit card processing arrangements will have their card processing terminated, and the unit will be responsible for any costs associated with this termination.