Prepared by Treasury Office.
This amends A8.710 dated July 2001.

A8.710 Credit Card Program

1. Purpose

To provide uniform procedures for the processing of credit card transactions in accordance with University policies, banking and payment card industry requirements, the terms of the University's credit card contract and all subsequent amendments.

2. Applicability

This directive applies to all campuses of the University of Hawai‘i.

3. Definitions

a. Merchant – an entity accepting credit cards as a form of payment. A merchant number must be established by the bank before credit card processing can commence. For accounting and control reasons, only the Treasury Office will request merchant set-ups from the Contractor. Terminal identification numbers (TID) must also be established for each merchant as the mechanism to initiate credit card transactions. TID’s must be established even if software is being used to initiate credit car transactions.

b. Merchant Fee – the service fee paid to the contractor by the merchant (UH department) accepting a credit/debit card for payment

c. Contractor – the vendor contracted by the University to provide credit card processing services.

d. eCommerce – a non face to face on-line transaction using electronic media over a public or private network.

e. Payment processing service – a service that provides connectivity among merchants, customers, and financial networks to process authorizations and payments.

4. Responsibilities

a. The Treasury Office approves or disapproves requests to participate in the program. This includes requests to use a third party payment processing service to accept credit card payments over the web.

b. The campus/department will comply with all procedures specified by the University and the Contractor with respect to sales drafts and related transactions.

c. The campus/department must comply with security requirements and safeguard cardholder data as set forth by the Payment Card Industry (PCI).

d. The campus/department is responsible for the payment of the rental costs of equipment or software, dedicated telephone line, and the merchant fee.

e. The campus/department utilizing third party payment processing service to accept credit card payments over the web must ensure that they comply with all University, banking and payment card industry security requirements.

5. Procedure to Participate in Program

a. Requests to participate in the credit card program should be addressed to the Bursar and contain the following:

1) The justification for participating in the credit card program.

2) The legal authority that permits the campus/department to collect and deposit State or UH cash receipts.

b. Upon approval by the Bursar, the Treasury Office will notify the Contractor's representative to establish a merchant number and contact the department to arrange for equipment/software installation and training.

6. Procedure to Process Credit Card Sales

a. All sales drafts must be signed by the cardholder at the time of sale. Exceptions to this are purchases by mail, telephone, fax, and Internet orders. If a mail, telephone, fax, or Internet order is received, it must list the entire account number, card expiration date, cardholder's name, and amount to charge.

b. Specific instructions for credit card sales transaction processing are included in the user manual provided by the Contractor.

7. Procedure to Refund Credit Card Purchase

a. All refunds of goods and services paid for by credit card shall be made by credit vouchers. Department personnel shall sign each credit voucher. The amount of the credit voucher may not exceed the amount of the original transaction as reflected on the sales draft.

b. Specific instructions for refund processing are included in the user manual provided by the Contractor.

8. Procedure to Record Credit Card Sales in FMIS

a. All terminals must be closed and transmitted daily to the Contractor to receive credit for transactions processed. Specific instructions for deposit transaction processing are included in the user manual provided by the Contractor.

b. Contractor will credit the University's checking account no later than two (2) business days following transmission. Department must process a departmental deposit form (FMIS-5) to record the credit in FMIS. Prepare one departmental deposit form for each batch transmitted. The document number for the departmental deposit form is based on the first three digits of the fiscal officer code, followed by three digits assigned by the fiscal officer.

c. If refunds exceed sales, process a departmental deposit form (FMIS-5). To record a negative deposit in FMIS, enter a "D" in the D/C column.

d. A transaction may be charged back to the merchant when the cardholder disputes the sale or asserts that the sale was fraudulently processed. The program manager must investigate the claim and respond to the Contractor by date noted on the chargeback notice. If the chargeback is upheld, the merchant must process a journal voucher to record the chargeback in FMIS.

9. Retrieval of Credit Cards

a. As stipulated in the University's credit card contract, the department will use its best efforts to retrieve cards as requested by the Contractor.

b. Cut credit card once lengthwise through the account number and mail to the Contractor.

10. Reconciliation and Payment of Merchant Fees

a. The Contractor will submit monthly an original and two copies of invoices to each department for each merchant number.

b. Departments must reconcile the daily batch settlement report to the monthly merchant statement to ensure that the merchant was properly credited.

c. The Contractor will submit annually each July, an original and two copies of invoices to each department for the rental of equipment or software.

d. Purchase orders or departmental checks, as appropriate, shall be issued to the Contractor for payment.

11. Procedure to Withdraw from Credit Card Program

    a. Submit written request to the Bursar, with justification to withdraw from the credit card program.

    b. Upon approval, the Treasury Office will coordinate the closing procedures with department and Contractor.

12. Security Polices and Procedures for Credit Card Data

    a. It is the responsibility of all credit card merchants to safeguard cardholder data. Every effort must be made to prevent theft or inappropriate use of cardholder data.

        1) Cardholder data must be securely disposed of after meeting State of Hawai‘i records retention requirements.

        2) The full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.) in the database, log files, or point of sale products may not be stored.

        3) The card validation code (3-digit value printed on the signature panel of a card) may not be stored in any database, log file or point of sale product.

        4) All but the last 4 digits of the cardholder’s account must be masked when displaying cardholder data.

        5) Account numbers must be rendered unreadable anywhere it is stored by means of encryption or truncation.

        6) Account numbers must be sanitized before being logged in an audit log.

13. Security Policies and Procedures for Credit Card Data From eCommerce Transactions

    a. eCommerce merchants must implement data security procedures to conform to university information security policy and current PCI data security standards.

        1) Install and maintain a working firewall to protect data.

        2) Do not use vendor supplied defaults for system passwords and other security parameters.

        3) Protect stored data.

        4) Encrypt transmission of cardholder data and sensitive information across public networks.

        5) Use and regularly update antivirus software.

6) Develop and maintain secure systems and applications.

7) Restrict access to data by business need to know.

8) Assign a unique ID to each person with computer access.

9) Restrict physical access to cardholder data.

10) Track and monitor all access to network resources and cardholder data.

11) Regularly test security systems and processes.

a. eCommerce merchants must conduct a self-assessment survey and network system scan. The frequency is based on current PCI guidelines.

12) Maintain a policy that addresses information security.

14. Security Incident Response Plan

a. The department must immediately notify the University's credit card Contractor and the Treasury Office when cardholder data is breached.

1) The program manager must investigate the circumstances causing the breach and quickly resolve it. Failure to comply with security procedures and rectify the violation may result in heavy fines imposed by the credit card companies.

b. All security incidents involving eCommerce transactions must also be reported immediately to the ITS Information Security Officer and Incident Response Team.

1) Minimally, the Incident Response Team shall be comprised of the ITS Security Officer, the Application Security Administrator, the System Security Administrator, and the Credit Card Contract Administrator.

2) In the event that cardholder data from an eCommerce transaction is compromised, incident response team shall follow procedures outlined in the University's Administrative Information Systems Information Security Policy.