

CENTRAL WASHINGTON UNIVERSITY
3-50-125 PAYMENT CARD SECURITY PROCEDURES

As of June 30, 2005, VISA and Master Card Payment Card Industry Security Standards require all entities which handle or store credit cardholder data to comply with the Cardholder Information Security Program (CISP). The CISP standards are designed to protect cardholder data wherever and in whatever form it resides. Any merchant or service provider whose cardholder data is compromised, and who is not CISP compliant, may be held financially responsible for all costs up to \$500,000 per occurrence.

Overview

Central Washington University has compiled these credit card security procedures to be in compliance with the payment card industry security standards. All Central Washington University operations, units, and departments that accept payments by credit/debit card, must follow these procedures.

Central Washington University accepts the use of credit and debit cards by campus units to assist in the expansion of their customer base for products and services. The acceptance of credit cards simplifies the payment process and offers fraud protection. Visa and MasterCard are accepted. American Express, Discover and Diner's Club cards are not accepted at this time.

Departmental Responsibility

Departments are responsible to impose and follow procedures that help employees comply with the Payment Card Security Procedures. Each department is responsible to maintain internal controls that prevent payment card breaches and protect sensitive cardholder information. In accepting payment cards, departments acknowledge they are responsible to hire qualified employees, train employees on proper procedures, and ensure that their employees adhere to these procedures. ANY receipts, reports, etc., shall show only the last four digits of credit card numbers when archived. At no time shall any CWU department electronically retain cardholder data. At least annually or as part of the evaluation process, supervisors should inquire if any changes have transpired since their original background checks that would negatively affect the employee's creditworthiness or trustworthiness.

Employee Responsibilities

Selected candidates for positions (including student positions) and employees who are transferring to positions (including student positions) within CWU and who have access to MULTIPLE credit card records (as opposed to swiping single cards one at a time and returning them to the cardholder) must sign a background check authorization form (issued by Human Resources and/or Student Employment) and a form which certifies that they understand the University Procedures and their significance. (See Attachments 1 and 2 for samples of these forms.) Signed forms will be returned to Human Resources and retained in individual personnel files for all exempt and civil service employees. For student employees, departments and

supervisors are responsible to ensure that students sign the appropriate credit card security agreements. The departments and supervisors will attach the signed agreements to the Student Personnel Action Forms and forward them to Student Employment where they will be retained. Employees have the responsibility to notify their supervisors of any changes that may negatively impact the employee's creditworthiness or trustworthiness.

Employees are responsible to follow the Payment Card Security Procedures. Each employee is responsible to help establish and maintain a proper environment of internal controls that prevent credit card security breaches and protect sensitive cardholder information.

Process Overview

Acceptance and use of payment cards must be approved and coordinated with the Assistant Vice President for Financial Affairs. All CWU units and employees that receive and handle payment card information must have both an awareness of and show a commitment to strong internal controls. The Cashier's Office has primary responsibility, for the University, in accepting and processing payment cards, and for maintaining and securing cardholder data. Unless otherwise authorized, all CWU departments must direct all individuals, who pay a bill by credit or debit card, to the Cashier's Office or to its website. No card numbers shall be routed by fax, e-mail, or campus mail. Except with approved and contracted agreements with third-party processing companies, no department shall keep any payment card information in any system or computer.

Authorization Levels

Level 1 (No authority)

As these departments have no authority to receive or process payment cards, employees working in these departments must direct individuals to the Cashier's Office or to the Student Financial Services online payment process to make payments.

http://www.cwu.edu/~safari/student_financials_files/OnLine_payments.html

Level 2 (Single transaction events)

Departments authorized to utilize a credit card machine must have an authorized bank machine that is programmed to truncate credit card numbers so that printed reports and receipts show only the last four digits. Payment card transactions shall be processed immediately upon presentation and employees shall process only one card at a time.

Employees in Level 2 departments authorized to accept credit card information over the telephone may write down the information necessary to process the transaction immediately through the bank machine. Upon completion of processing the transaction, the employee shall dispose of the hand-written document containing the sensitive cardholder information following the required CISP guidelines (cross-cut shred, incinerate or pulp hardcopy materials). At no time shall the hand-written cardholder data be retained or stored. Also,

employees in this department shall not have sensitive cardholder information for more than one individual at any time.

All new employees in Level 2 departments, including student employees and CWU employees previously employed in another department, who handle or have access to cardholder data, are required to sign the Credit Card Security Agreement as a condition of employment.

Level 3 (Single transaction events and third-party vendor processing)

The Bookstore and other departments authorized to accept and process individual payment transactions or contract with a third-party vendor to process transactions for the department, shall process only one card at a time and shall follow the guidelines identified in Level 2. Any receipt or documentation related to transactions retained by the department shall contain only the last four numbers of the payment card. At no time, shall employees in the department have sensitive cardholder information for more than one individual at one time.

With assistance and support from Business Services and Contracts, Level 3 departments are authorized, following existing University policies, to contract with third-party vendors to receive and process payment on behalf of the University. These third-party vendors will be required to regularly certify and provide documentation of compliance with CISP standards.

All new employees in Level 3 departments, including student employees and CWU employees previously employed in another department, who handle or have access to cardholder data, are required to sign the Credit Card Security Agreement as a condition of employment.

Level 4 (Multiple cardholders' data)

Continuing Education and other departments that receive, record, and process hand-written cardholder data for more than one individual at a time must have written standard operating procedures, relating to the cardholder data, which are approved by the Assistant Vice President for Financial Affairs.

All new employees in Level 4 departments, including student employees and CWU employees previously employed in another department, who handle or have access to cardholder data, are required to sign the Credit Card Security Agreement and the Credit Card Security Background Check Consent forms as a condition of employment.

All cardholder information that is received shall be retained in a secure environment at all times. Any form showing a 16-digit credit card number must be kept under lock and key until being delivered to the Cashier's Office. On a timely basis, departments that receive payment card information shall hand carry, in a sealed and unmarked bag, all payments to the Cashier's Office by the end of each working day. At no time shall card numbers be routed by fax, e-mail, or campus mail. Payments received during weekends, holidays, or at evening events will be stored under lock and key until delivered to the Cashier's Office by 12 noon on the following working day. Departments will not create or retain a record that contains sensitive card holder data.

Level 5 (Multiple cardholder data and third-party vendor processing)

Student Financial Services and the Conference Center receive, process, and retain multiple cardholder data and must comply with all CISP regulations to ensure that cardholder data is protected in whatever form it resides. These departments must have written standard operating procedures, relating to the cardholder data, which are approved by the Assistant Vice President for Financial Affairs. Level 5 departments acknowledge they are responsible to train employees on proper policies and procedures, and ensure that their employees adhere to these policies and procedures.

All new employees in Level 5 departments, including student employees and CWU employees previously employed in another department, who handle or have access to cardholder data, are required to sign the Credit Card Security Agreement and the Credit Card Security Background Check Consent forms as a condition of employment.

Only Level 5 departments are authorized to retain the full 16-digit credit card account numbers (under lock and key) for a period of up to three months for purposes of refunding charges when necessary or as required by federal and state law. When payments are received, employees shall promptly record each transaction. All cardholder information showing a 16-digit credit card number shall be kept under lock and key with limited access at all times. All forms or reports containing 16-digit card numbers shall be destroyed in compliance with CISP guidelines (cross-cut shred, incinerate or pulp hardcopy materials). At no time shall these departments or any other CWU department electronically retain cardholder data.

With assistance and support from Business Services and Contracts, Level 5 departments are authorized to contract with third-party vendors to receive and process payments on behalf of the University. All third-party online payment service providers must provide secure environments for payment card information, comply with the CISP, and be able to provide CISP certified documentation upon request.

As a condition of doing business with CWU, third-party vendors will be required to sign a contract with the University regarding their adherence to industry-wide credit card security procedures and responsibilities. Level 5 departments that use online payments must always change the vendor-supplied defaults before installing a system on the network. In addition, vendor security upgrades must be installed upon release (within a reasonable time period).

Note: For more information about the CISP Standards, contact the Accounting Department or go to the following visa website: http://usa.visa.com/business/accepting Visa/ops_risk_management/cisp.html

CENTRAL WASHINGTON UNIVERSITY
PAYMENT CARD SECURITY
AGREEMENT

I, _____, certify that I have read and understand the Central Washington University Payment Card Security Procedures.

I understand my responsibilities in the prevention of payment card security breaches, and will do my utmost to comply with the CWU Payment Card Security Procedures to protect sensitive cardholder information.

I realize that violation of Central Washington University Payment Card Security Procedures may be grounds for disciplinary action up to and including termination of employment or expulsion from the University, and may lead to criminal prosecution.

X _____
Signature

Date

Original to Human Resources
C: Employee

CENTRAL WASHINGTON UNIVERSITY
PAYMENT CARD SECURITY
BACKGROUND CHECK CONSENT

As of June 30, 2005, VISA and MasterCard Payment Industry Security Standards require all merchants, members, and service providers who store, process, or transmit credit cardholder data to comply with the Cardholder Information Security Program (CISP). This program is designed to protect cardholder data wherever it resides.

Any merchants or service providers whose cardholder data is compromised, and who are not CISP compliant, may be held financially responsible for all costs up to \$500,000 per occurrence.

Central Washington University has developed Payment Card Security Procedure to be in compliance with the CISP standards. All Central Washington University operations that accept payment card (in whatever manner or form) must comply with the University's Payment Card Security Procedures.

As a new CWU employee, student employee, or a current CWU employee who is transferring to a CWU position which has access to cardholder data, I, _____, hereby give my consent for CWU to do background checks (which may include, but not be limited to, a criminal background check, a reference check, and a credit check) as prerequisites for a position which has access to multiple credit cardholders' data via systems, hard copies, and/or networks at Central Washington University. I understand that negative results obtained from these checks may be grounds to deny employment at CWU or to deny permission to transfer to a position that has access to multiple credit cardholders' data.

X _____
Signature

Date

Original to Human Resources
C: Employee