SHARED SERVICES
Financial Services

Procedure Title:	Customer Credit Card Payment Procedure				
Procedure Number:	DHS-040-013-01	**Version:**	1.0	**Effective Date:**	07/01/2010

Jim Scherzinger, Dep. Dir. of Finance
Approved By: (Authorized Signer Name)

07/01/2010
Date Approved

Procedure

Strong accountable business processes are one way to safeguard confidential information in the course of the agency's daily operations. Credit card transactions, as monetary transactions, are subject to strict management controls in order to mitigate card misuse, chargebacks and consumer identity theft.

All paperwork, records, receipts, card imprints, electronic data and other documentation containing cardholder account information is considered confidential under Public Records Law, ORS 192.501 (26).

Applicability

DHS is the custodian of personal information entrusted to the agency by clients, customers, licensees and employees. DHS is responsible for protecting these information assets from loss or misuse.

Only DHS employees or agents who are specifically authorized by the DHS Controller can accept and process credit card transactions. All such transactions must comply with Payment Card Industry (PCI) and National Automated Clearing House Association (NACHA) rules.

Compliance is not optional. Failure to comply may result in financial loss, fines, suspension of credit card processing privileges, and/or damage to the agency's reputation.

Failure to comply with any provision in the policy, associated policies, standards or procedures may result in disciplinary actions up to and including dismissal from state service or the termination of a contract. Legal action may also be taken.

Step	Responsible Party	Action
1. Protecting customer credit card information	Manager, employee	Managers shall ensure that the customer's personal credit card information is protected at all times: • Employees have read and understand the applicable statutes, rules, policies and manuals governing the protection of personal identification information. (Information referenced on the last page.)

		• Credit card processing duties and responsibilities are identified and incorporated in the appropriate section of the employee's position description, when applicable. • Access to credit card information is restricted to authorized employees only. • Credit card transactions are processed over the secure, encrypted internet connection as authorized by the DHS Information Security Office. • Credit card information shall not be retained on a personal computer in an electronic file (database, spreadsheet, word processor, images, etc.) for subsequent use. • Paper records containing full credit card information shall be redacted using a modified "manual double pass" method: o All but the last four digits of the credit card number, card-validation code, and expiration date are removed from the original form with indelible black ink marker. o A copy of the redacted original is made to document the signature of the credit card owner and the amount the owner authorized to charge to his / her credit card. The copy is retained on file in the event of a chargeback. o The original form is shredded. • Employees, contracted agents and volunteers shall not use, disclose or disseminate cardholder account number information except for the purposes of processing the authorized transaction.
2. Obtaining credit card information	Manager, employee, Information Security Office, Financial Services	**SecurePay internet transactions** Department of Administrative Services (DAS) provides a reliable and secure platform to agencies that allows customers to conduct business with the state from their home or office. Authorized agencies using SecurePay are required to follow "cardholder present" and "cardholder not present" rules. DHS provides restricted and limited access to this payment method. Requests for access must be submitted by a division or program manager and sent to the appropriate PSOB or Salem Central

Office Financial Services Receipting manager and Information Security Officer. Requests must clearly demonstrate a justifiable business reason for access. Within 30 business days, the Financial Services Receipting manager, Information Security Officer and DHS Controller will assess the documentation supporting the request to decide whether to allow access.

Cardholder not present

Telephone transactions have a substantially higher risk of chargeback. Managers must ensure that DHS 135, *Credit Card Authorization* form or DHS 0306, VISA/MasterCard/Discover Authorization form is used. Information on the forms must include, but is not limited, to:

- Name of caller / contact person;
- Date of call;
- Caller’s / contact’s telephone number;
- Cardholder’s name as it appears on the credit card;
- Cardholder’s account number;
- Card validation code (the three-digit number next to the signature panel on the back of the credit card);
- Credit card effective date (if available) and expiration date (good / valid through date) (the transaction must occur on or between the effective and expiration dates);
- Address where the credit card statement is mailed (also referred to as the billing address);
- Amount to be charged to the credit card;
- Description of the transaction that includes:
  - Provider / case number, invoice and or billing number.
  - Subject individual’s names submitted for fingerprinting.
  - Explanation for payment.

Check mark the telephone authorization box if the credit card information is obtained over the telephone.

Cardholder present

In addition to the above information that is obtained

		when the cardholder is not present, the manager must ensure that: • The credit card is examined to verify it is valid. • The signature panel on the back of the card is signed and has not been altered. o A credit card with two signatures in the signature panel or an altered signature panel is invalid. Do not accept the card. o If the signature panel is blank, the cardholder must provide government-issued identification (e.g., driver’s license), and sign the credit card in your presence. o Do not accept an unsigned card. o The cardholder verifies the information, signs and dates the completed DHS 135, *Credit Card Authorization* form. o Provide the cardholder with a copy of the signed and dated form to retain for his or her payment record. Over-the-counter credit card transactions using a manual imprinting machine to make an impression of a credit card are strictly prohibited. Use of electronic swiping devices is restricted to populating a credit card screen on a secure internet connection and must be authorized by the DHS Controller and Information Security Officer.
3. Credit Card Authorization form, DHS 135	Manager, employee	The manager must ensure that the information on the Credit Card Authorization form, DHS 135 is completed, hand-printed and legible. The form is placed in a sealed envelope and delivered or mailed to: Financial Services Receipting Unit PO Box 14006 Salem, OR 97309-5030 If a copy of the form is required to document the authorization, managers must ensure that all required credit card information is redacted.
4. Processing credit card transactions	Financial Services	All credit card transactions shall be processed by designated employees in the Financial Services Receipting unit or by an authorized third party agent under contract to DHS. Credit card transactions shall be processed using only the secure, encrypted internet connection. The authorization network sends a “declined” or “no match” response if the credit card transaction is not

		accepted. Financial Services will immediately notify the appropriate DHS office. Credit card transactions must meet State Treasurer deposit requirements in accordance with ORS 293.265. Credit card transactions submitted and accepted by the authorization network before 5 p.m. will be posted to the agency account at the State Treasurer on the next business day.
5. Recurring credit card transactions	Manager, employee, Financial Services	Recurring credit card transactions are a way for clients to make regular payments. Recurring transactions are limited to clients participating in Client Pay-In, Providence ElderPlace, and Estate Recovery programs. Manager, designated employee Because the cardholder or client will enter into a contractual agreement with DHS, the manager or designee must ensure that the cardholder or client understands the ongoing nature of the commitment he or she is undertaking. Instruct the cardholder/client that the recurring credit card payment will remain in effect until the Financial Services Receipting unit receives written notification to cancel the authorization. The written notification must be received at least seven business days before the recurring charge date in order to cancel the next payment. The Recurring Credit Card Payment Authorization, DHS 135 A form must be completed, signed and dated by the client, cardholder (if different from the client) and manager. The authorization will not be accepted if any signatures are missing. • Client’s name; • Client’s prime/case number; • Client’s phone number; • Client’s e-mail address; • Manager’s name and phone number;; • Type of credit card; e.g., Visa, Discover, MasterCard; • Cardholder’s name (exactly as it appears on the credit card); • Credit card number; • Authorization code; • Effective date (if available) and expiration date; • Cardholder’s billing address; • Amount of charge; • Frequency of charge;

		• Start and end date of charges; • Client’s signature; • Cardholder’s signature if different from client; • Manager’s signature. The manager or designated employee must sign and date the form attesting to the accuracy and completeness of the information. Provide a copy of the signed form to the client for his or her records. Seal the original form in an envelope and mail it to Financial Services Receipting unit. E-mail and facsimile networks are not sufficiently secure to protect the cardholder’s personal information. The manager shall ensure that the form is not sent via e-mail as a scanned image or faxed to the Financial Services Receipting unit. The manager’s failure to mail or deliver the form in a sealed envelope is considered an inappropriate action and subject to disciplinary action up to and including dismissal. Financial Services Receipting unit Upon receipt of the completed Recurring Credit Card Authorization form, the Financial Services Receipting unit will process the information into the encrypted system. A copy of the redacted original will be retained on file in a secure location. The original will be shredded.
6. Credit card refunds	Manager, employee	Refunds must be for the exact dollar amount of the original transaction. Refunds must be issued to the same credit card used to process the original transaction. If the original credit card has been canceled or has expired, a warrant refund may be issued upon receipt of a copy of the credit card rejection document. Cash refunds are prohibited. The manager or designated employee must provide Financial Services Receipting unit representative a completed DHS 136, Request For Credit Card Refund form to initiate a credit card refund for the cardholder. Upon receipt of the request and verification of the information, Financial Services will immediately process the refund.
7. Credit card chargebacks	Financial Services	A chargeback is the reversal of the dollar value, in whole or in part, of a transaction by the card issuer. Chargebacks generally arise from customer disputes, fraud, processing errors, authorization issues, non-compliance with the card issuer’s request for copies of

		the transaction, or customer or client non-response to requests regarding charges made to his or her credit card. The PCI Security Standards Council standards and policies must be met by all organizations that accept credit cards. Financial Services is required to respond to chargebacks and copy requests within the time frame specified by the card issuer. Additionally, PCI rules prohibit organizations from re-billing the cardholder’s credit card after a chargeback is received for the transaction, even with the cardholder’s authorization. If the chargeback is determined inappropriate and payment has not been received, Financial Services will notify the appropriate manager or designee of record and initiate the appropriate actions to create an accounts receivable for the amount owed by the cardholder. The cardholder will be required to pay by personal check or money order.
8. Reconciliation	Financial Services	The total dollar value of each day’s credit card receipts must be compared with and reconciled to the Daily General Fund Transaction Listing generated by the State Treasurer. Differences must be identified and corrected before the deposit is cleared in the statewide accounting system.
9. Breach of security	Information Security Office	Upon notification of a potential security breach the Information Security Office will initiate the appropriate actions in accordance with DHS Information Security policies and procedures, and state and federal laws.
10. Risk assessment	Financial Services, Information Security Office	Per the State Treasurer’s requirements, Financial Services and the Information Security Office will conduct and complete the annual PCI Security Standards (PCI DSS) risk assessment.
11. Record retention	Manager, employee, Financial Services	Documentation supporting credit card transactions must be retained for six years, unless otherwise specifically authorized by the State Archive policy or ORS 646A.204
12. Audit	Manager, employee, Financial Services, Information Security Office	Managers shall ensure that all documentation provided to, obtained or used by the agency to authorize, originate, receive or authenticate credit card transactions is available at all times for scheduled or unscheduled audits conducted by internal or external auditors.

Policy that applies:

DHS-040-013: Receipting of Checks and Other Negotiable Instruments
DHS-040-010: Delegated Expenditure Authority

DHS-060-002: Conflict of Interest
DHS-060-004: Discipline and Discharge-Classified, Unrepresented
DHS-060-005: Discipline and Discharge-Management Services
DHS-090-001: DHS Information Security
DHS|OHA-090-002: DHS|OHA Information System Audit and Monitoring Policy
DHS-090-003: DHS Information Access Control Security
DHS-090-004: DHS Information Security Awareness
DHS-090-005: Privacy and Information Security Incident Management

Procedure that applies:

DHS-040-010-02: Inappropriate Actions

References:

Office of the State Treasurer: 02 18 13
Oregon Accounting Manual 10.35.00
ORS 293.295, 646A.210, and 646A.214
VISA Merchant Guides: http://usa.visa.com/merchants/merchant-resources/index.jsp
Office of the State Treasurer: 02 18 13
Oregon Accounting Manual 10.35.00
ORS 293.295, 646A.210, and 646A.214
VISA Merchant Guides:

Form(s) that apply:

DHS 135, Credit Card Authorization
DHS 135 A, Recurring Credit Card Payment Authorization
DHS 136, Request for Credit Card Refund

Contact(s):

Name: Jeff Aldridge; **Phone:** 503-947-5007; **Email:** jeff.aldridge@state.or.us

Procedure History:

- **Version 1.0:**
  07/01/2010 Initial Release

Keywords:

(List keywords here that might be used by someone to search for this policy on the internet)