



**DEPARTMENT OF CORRECTIONS
Business & Finance**



Title:	Customer Credit Card Payment	DOC Policy: 30.1.5
Effective:	3/1/12	Supersedes: N/A
Applicability:	All DOC employees who are specifically authorized by the DOC Appointing Authority to accept and process or approve credit card transactions.	
Directives Cross-Reference:	Policy: Acceptable Use of Electronic Information Systems – 60.1.1 Information Security – 60.1.4 Information Security Awareness – 60.1.5 Information Security Incident Response – 60.1.6 Oregon Accounting Manual – 10.35.00	
Attachments:	None	

I. PURPOSE

The purpose of this policy is to protect credit card data, the cardholder, and the Department. This policy provides direction and support for information security in accordance with business requirements and relevant laws and regulations including but not limited to the Department of Corrections (DOC) Information Security Plan and the Payment Card Industry Data Security Standards (PCI DSS).

II. DEFINITIONS

- A. **Availability:** The reliability and accessibility of data and resources to authorized individuals in a timely manner.
- B. **Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects.
- C. **Controls:** Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
- D. **Electronic Data Interchange (EDI):** The computer-to-computer exchange of structured information, by agreed message standards, from one computer application to another by electronic means and with a minimum of human intervention.
- E. **Electronic Commerce:** Electronic commerce, commonly known as e-commerce or e-Commerce; conducting business activities - buying, selling and other transactions - via communications and computer technologies. It includes transactions done by telephone, fax, credit card, debit card, television shopping, EDI and the Internet.
- F. **Encryption:** Process of converting information into an unintelligible form except to holders of a specific cryptographic key.

- G. Information Security: Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.
- H. Information Owner: Administrative designee for a division or functional unit that has been assigned responsibility for final decisions regarding classification, retention and information security policy associated with their designated programs.
- I. Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.
- J. PCI DSS: Payment Card Industry Data Security Standard - A set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.
- K. Personally Identifiable Information (PII): A consumer's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired:
 - 1. Social Security number
 - 2. Driver license number or state identification card number issued by the Department of Transportation
 - 3. Passport number or other United States issued identification number
 - 4. Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account.
- L. Point of Sale (POS): A location where credit card transactions are performed with the cardholder present. The card is read magnetically, and the cardholder's signature is obtained as insurance against the transaction. This is the most secure form of credit card commerce.
- M. Redaction: The process of editing a publication or document by deleting, blacking out or otherwise removing protected or confidential information prior to release or distribution.
- N. Risk: The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.
- O. Sensitive Information: Any information where the loss, misuse, or unauthorized access to or modification, could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.
- P. Sensitivity: A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

III. POLICY

A. Standards

1. All DOC systems associated with payment cards will be developed and maintained in accordance with, but not limited to current PCI DSS standards.
2. All transactions associated with payment cards will be conducted in accordance with, but not limited to current PCI DSS standards.
3. All documentation relating to payment cards containing personally identifiable information will be handled, stored and transmitted in accordance with current DOC Information Security Plan standards.

B. Electronic Commerce

1. Information involved in electronic commerce must be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
2. DOC will not accept credit card payments via email, instant messaging or chat technology.

C. Control Requirements

1. Telephone Transactions

When accepting and processing credit cards in payment of products, services, licenses, or other fees in transactions that are conducted by telephone the responsible employee(s) shall include the following controls into their operations.

- a. Name of caller, telephone number, and date of call.
- b. Cardholder's name as it appears on the credit card, and cardholder's account number.
- c. Credit card effective date.
- d. Address where the credit card statement is mailed (billing address).
- e. Amount to be charged to the credit card.
- f. Description of the transaction that includes the customer number and invoice number along with explanation for the payment.
- g. Card validation code, and credit card number obtained to complete the card authorization of the transaction shall be immediately destroyed/shredded appropriately when authorization is received.

2. On-Line Transactions

Information involved in on-line transactions must be protected to prevent unauthorized access, incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

3. **Point of Sale (POS) Transactions**

Information involved in point of sale transactions must be protected to prevent incomplete transmission, unauthorized disclosure, or unauthorized access. The following procedures shall be used.

Procedures:

- a. Before swiping the customer's credit card through the POS terminal, verify that the card expiration date has not passed. Expired credit cards shall not be accepted for payment.
- b. Ensure that the dollar amount charged to the card is fixed by the transaction. No cash refund or credit may be issued in conjunction with the purchase transaction.
- c. If the authorization network approves the transaction, ask the customer to sign the sales receipt and then compare the customer's signature with the signature on the back panel of the credit card. Unsigned cards shall not be accepted.
- d. Compare the name and account number on the credit card with the name and last four digits of the account number on the printed receipt. Refer to the US Bank Merchant Terms of Service (MTOS) or Discover Business Services Merchant Operating Regulations (MOR) guidelines if the name or digits do not match.

NOTE: The MTOS/MOR requirement that all POS devices must suppress all but the last four digits of the credit card account number and the entire expiration date on the cardholder's copy of the transaction receipt is consistent with Oregon law. The Oregon Identity Theft Prevention Act (Oregon Laws 2007, Chapter 759) states that data shall be redacted so that no more than the last four digits of a customer's credit or debit card number are accessible.

- e. If the credit card's magnetic stripe cannot be read, and the cardholder's information is key-entered, you must:
 - (1) Request Address Verification Services (AVS).
 - (2) Make a physical imprint of the card using a manual imprinter.
 - (3) Obtain the cardholder's signature on the imprinted transaction receipt and compare it to the signature on the back panel of the card. Unsigned cards must not be accepted.
 - (4) Black-out all but the last four digits of the credit card number on the cardholder's copy of the receipt.
- f. To complete the transaction, information necessary for the delivery of purchased goods or services may be requested and recorded as long as the information is provided voluntarily by the credit cardholder (ORS 646A.214).

- g. If a “declined” or “no match” response is received from the authorization network, the credit card cannot be accepted. The employee should offer to process a different, valid credit card or another acceptable form of payment, such as a personal check or cash.

D. Deposit / Settlement

1. All credit card transactions must meet the deposit requirements of ORS 293.265.
2. Credit card terminals: The daily receipts totals from all credit card processing devices must be printed and used to settle transactions at the end of each business day. Transactions settled before 5:00 p.m. will be posted to the DOC’s account at the Office of State Treasurer (OST) at midnight.
3. Transactions settled before 5 p.m. will be posted to DOC accounts the next business day if there are no changes/errors in the normal daily processes.

E. Reconciliations

1. Daily Reconciliation: The total dollar value of each day’s credit card receipts shall be compared with and reconciled to the underlying transaction records of goods, licenses, etc., sold or issued.
 - a. Total credit card receipts from all systems must be reconciled to the total dollar value of the underlying transaction records (i.e., the number of products sold or licenses issued multiplied by applicable unit prices).
 - b. If the total credit card receipts do not agree to the total dollar value of the underlying transaction records, a transaction-by-transaction analysis must be performed to locate the difference.
 - c. Differences must be identified and corrected prior to clearing the deposit.
2. Bank Reconciliation: The total for credit card receipts must be reconciled to the treasury statement received from OST, and daily treasury statement must be reconciled to the Statewide Financial Management Application (SFMA) or the DOC’s cash management system. Small volume transactions may be reconciled on a less frequent basis, such as weekly, but not less than once a month.

F. Merchant Fees

Merchant fees for all transactions are deducted monthly from DOC accounts at OST. A review shall be performed on the US Bank Merchant Statements to ensure that the amounts charged for merchant fees are appropriate.

G. Refunds

1. No cash refund shall be processed as the result of a credit card transaction including, but not limited to cash back requests, returned or undeliverable product, or an otherwise cancelled transaction.
 - a. The amount charged to the card must be fixed by the amount of the transaction.

- b. Credits (refunds) must be issued to the same credit card used to process the original purchase transaction.
- c. If the original credit card has been cancelled or has expired, a warrant or check refund may be issued upon receipt of a copy of the credit card reject document.
- d. The agency's credit (refund) policy should be clearly communicated at the time of the initial transaction.

H. Chargebacks

A chargeback is the reversal of the dollar value, in whole or in part, of a particular transaction by the card issuer to the state agency that originally processed the transaction. Chargebacks generally arise from customer disputes, fraud, processing errors, authorization issues and non-compliance with copy requests. DOC shall respond as soon as possible to chargebacks and copy requests. Refer to the MTOS/MOR for further information and appropriate actions.

I. Protecting Confidential Credit Card Records

1. DOC has implemented an Information Security program that has appropriate Administrative, Technical and Physical safeguards in place complying with the Oregon Identity Theft Prevention Act.
2. DOC Information Security Policies:
 - **Information Security** 60.1.4
 - **Information Security Awareness** 60.1.5
 - **Information Security Incident Response** 60.1.6
 - **Acceptable Use of Electronic Information Systems** 60.1.1
3. DOC shall protect any media (paper, electronic, or other) containing confidential cardholder information from unauthorized access and/or disclosure at all times. Backup media shall be securely stored. Information Security is the responsibility of every employee, contractor, group or individual. **Information Security** policy 60.1.4 ensures all information, specifically cardholder data, is appropriately classified and secure.
4. DOC shall keep secure networks or other devices, including point-of-sale terminals, used to store, process or transmit confidential credit card information collected from customers.

J. Security Breach and Notification Requirements

1. The Oregon Identity Theft Prevention Act requires any agency that maintains personal information, including credit card information, of Oregon consumers must notify its customers if files containing that personal information have been subject to a security breach.
2. Information security breaches, if they occur at DOC are covered under Policy 60.1.6 **Information Security Incident Response**. Policy 60.1.6 stipulates that a breach of credit card information results in a notification to the Oregon State Treasurer.

K. Payment Card Industry Compliance

1. The DOC must comply with applicable industry data security standards in order to store, process or transmit cardholder information associated with credit card transactions. Visa, MasterCard, American Express, and Discover card brands require compliance with the Payment Card Industry Data Security Standard (PCI-DSS). Failure to comply with industry standards may result in fines and /or revocation of credit card acceptance.
2. DOC shall not store the following sensitive authentication data subsequent to authorization of a transaction in DOC credit card processing system.
 - a. The full contents of the magnetic stripe on the back side of the credit card.
 - b. The card validation code or value (the three-digit or four-digit number printed on either the front or back of the credit card).
 - c. The personal identification number (PIN) or the encrypted PIN block.
3. Sensitive credit card information shall be stored in a secure area such as a locked file or safe at all times.
4. Virtual terminals or card terminals shall be locked in a file or safe when not in use.

L. Segregation of Duties

1. Adequate segregation of duties increases the likelihood that unintentional and intentional errors, including fraud, will be prevented or detected in a timely fashion.
2. DOC, whenever possible, will assign credit card function tasks to separate individuals. Access will be limited to staff whose job requires access.

M. Credit Card Records Exempt from Public Disclosure

All paperwork, records, receipts, card imprints, electronic data, etc., containing information provided to, obtained by or used by a DOC to authorize, originate, receive or authenticate a transfer of funds, including but not limited to a credit card number, payment card expiration date, password, financial institution account number and financial institution routing number are exempt from disclosure under ORS 192.410 to 192.505 unless the public interest requires disclosure in the particular instance. ORS 192.501(27) – Public Records Law

N. Record Retention Requirements

In general, copies of credit card receipts and supporting documentation must be retained by DOC for 6 years (or in accordance with current archive requirements). However, copies of credit card receipts containing more information about a customer than the customer's name and five digits of the customer's card number must be destroyed on or before the sooner of:

1. The date the image of the copy is transferred onto microfilm or microfiche; or
2. Thirty-six (36) months after the date of the transaction that created the copy (ORS 646A.204).

IV. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: _____
Birdie Worley, Rules Coordinator

Approved: _____
Mitch Morrow, Deputy Director