**Payment Cards**

Effective: February 9, 2015

**Purpose**

To comply with Payment Card Industry (PCI) Data Security Standards (DSS) and establish protocol for good payment card handling practices by the Utah Department of Transportation (Department).

**Policy**

The Department will operate in accordance with current PCI DSS requirements. Compliance will be evaluated annually.

The Comptroller’s Office General Ledger (G/L) Manager will coordinate all Department divisions’ acceptance of payment cards. The G/L Manager will coordinate with the Department of Technology Services (DTS) to initiate acceptance of payment cards.

Divisions will specify locations, personnel, and equipment used in the acceptance of payment cards. Divisions will not make changes or additions without the consent of the G/L Manager once approved.

Only those employees authorized by the Comptroller’s Office may accept payment card information. Divisions will verify that all employees accepting payment card information complete DTS PCI DSS training. Divisions will provide any other training necessary to guarantee PCI DSS compliance. Other employees may not accept or transmit payment card information, and must instead refer the customer to an employee authorized and trained to do so.

Department employees will not record or store, in electronic or hardcopy format, any payment card information. The Department will not accept any payment card information transmitted by email or fax; electronic media will be deleted and hardcopies will be cross-shredded immediately.

Complete payment card numbers will not be transmitted by or stored by Department business systems. Payment card numbers will be masked except for the last four digits on all receipts and reports.

The card security code will never be recorded in electronic or hardcopy format. It will only be entered into the terminal.

Physical payment cards will remain in the cardholder’s line of sight at all times.
Terminals will be situated in secure locations that allow for control of physical access and that are in clear view while in use. Terminals will be stored in secure locations out of sight when not in use. Terminals and cords will be inspected for evidence of tampering at the beginning and end of each shift.

Potential breaches and irregularities will be reported immediately to the G/L Manager. The G/L Manager will work with the DTS Compliance Auditor and the Division of Administrative Service Division of Finance (DAS/Finance) Payment Card Specialist to determine the potential extent of the breach, the response to the breach, and the investigation of the breach.

The G/L Manager will authorize all maintenance to and replacement of payment card equipment. Employees will validate this authorization, as well as credentials, before allowing any person, entity, or organization physical or electronic access to equipment used in payment card processing.

Each location accepting payment cards will settle batches nightly. Region offices will transmit batch information to the Comptroller’s Office Payables Supervisor. The Motor Carrier Division will aggregate batch information from the Ports of Entry and will transmit the information to the Comptroller’s Office Payables Supervisor.

Default user names and passwords will be changed prior to deployment for all equipment and systems. All equipment involved in credit card processing will be maintained properly, including physical cleaning and maintenance, anti-virus and anti-malware scans, encryption protocols, firmware patches, and software updates.

Payment card payments will be accepted via secure online portals administered by PCI DSS compliant third party vendors or via bank-issued payment card terminals either in person or by phone. The Department employee will enter the cardholder information into the terminal and will not record or divulge the information in any other manner if a customer pays by phone.

Access rights to Department systems and applications involved in payment card processing will be restricted to the least privileges necessary to perform job duties, and will be based on job classification and function.
Responsibility: Division Business Analyst

Actions

1. Identify opportunity and need to accept payment cards.
2. Draft proposal to accept payment cards.
3. Present proposal to Comptroller’s Office General Ledger Manager.

Responsibility: Comptroller’s Office General Ledger Manager

4. Review the proposal, consulting with DTS Compliance Auditor and DAS/Finance PCI Specialist.
5. Determine course of action to guarantee PCI DSS compliance.

Responsibility: Division Business Analyst

6. Implement General Ledger Manager’s recommendations.
7. Report all personnel, equipment, and internal processes to General Ledger Manager.
8. Provide training for all division employees involved in the payment card acceptance process.
Custody of Payment Card Terminal

**Responsibility:** Comptroller’s Office General Ledger Manager

### Actions

1. Maintain inventory list of terminals with locations, list of employees accepting payment cards, internal handling guidelines, and network diagrams.

**Responsibility:** Division Business Analyst

2. Provide the General Ledger Manager with any location updates.

3. Provide division employees with all necessary PCI DSS compliance training.

**Responsibility:** Department of Technology Services

4. Provide the General Ledger Manager with network diagram updates.

**Responsibility:** Employees Accepting Payment Card Payments

5. Complete all applicable training.

6. Maintain the terminal in a secure but visible location during shift.

7. Store the terminal in a secure, out of sight location at the end of a shift.

8. Inspect the terminal and cords at the beginning and end of each shift for tampering.

9. Inspect the premises for unauthorized surveillance and access irregularities.

10. Validate credentials of any person, entity, or organization that requests physical or electronic access to the terminal.

11. Contact the General Ledger Manager to verify that the access is authorized.
Responsibility: Department Employee Designated to Process Payment Cards

Actions

1. Complete all applicable training.
2. Be familiar with PCI DSS.
3. Inspect terminal and cords for tampering at beginning of shift.
4. Survey building for irregularities and potential access hazards.
5. Maintain terminal in secure location throughout shift.
6. Keep payment card in view of customer at all times.
7. Return payment card to customer after swipe and verification.
8. Guarantee that the card number, security code, expiration date, and any other card information is not recorded outside of the terminal or displayed without being masked.
9. Inspect terminal and cords for tampering at end of shift.
10. Store terminal in a secure location out of view.
Responsibility: Department Employee Designated to Process Payment Cards

Actions

1. Complete all applicable training.
2. Be familiar with PCI DSS.
3. Inspect terminal and cords for tampering at beginning of shift.
4. Survey building for irregularities and potential access hazards.
5. Maintain terminal in secure location throughout shift.
6. Accept payments only by phone.
7. Immediately delete emails with payment card information, and immediately cross-shred faxes and letters with payment card information.
8. Guarantee that the card number, security code, expiration date, and any other card information is not recorded outside of the terminal or displayed without being masked.
9. Inspect terminal and cords for tampering at end of shift.
10. Store terminal in a secure location out of view.
Incident Response UDOT 02-65.5

Responsibility: All Employees

Actions

1. Report potential system and policy breaches to General Ledger Manager.

Responsibility: General Ledger Manager

2. Assess the potential effects and estimate the scope.

3. Determine if the breach has occurred.

4. Immediately notify the DTS Compliance Auditor and the DAS/Finance PCI Specialist if a breach has occurred.

5. Notify affected parties and law enforcement as appropriate.

6. Implement the appropriate response action, based on the scope and effects.

7. Assemble and lead an investigation to determine the cause of the breach and to recommend a future course of action.