
DTS PAYMENT CARD (PCI) SECURITY STANDARDS

Status: **Approved**
Effective Date: March 2009 through March 2010
Revised Date: N/A
Approved By: Michael J. Casey
Authority: *UCA §63F-1-206; Governor's Executive Order: Directing the Chief Information Officer to Develop and Implement Policy Promoting Security of State Information and Information Systems*

S7.1 Purpose

The purpose of this policy is to establish a standard for protection of payment card information of individuals and businesses that conduct business with the State of Utah as required by Finance Policy FIACCT 07-09.00 Revenue - Credit Cards and the Payment Card Industry (PCI) Data Security Standard (PCI DSS) requirements.

S7.1.1 Background

The Payment Card Industry has implemented a series of data security standards which require all entities storing, processing or transmitting cardholder data be compliant. There are stiff financial and operational penalties for non-compliance.

S7.1.2 Scope

This Standard applies to all Executive Branch State Agencies which process or makes use of payment card transactions as required by section A 4 of Finance's policy.

S7.1.3 Exceptions

Exceptions to this standard must be approved in writing by both the director of the Utah Division of Finance (Finance) and the executive director of the Utah Department of Technology Services (DTS).

S7.2 Definitions

Cardholder Data

All personally identifiable data about the cardholder and relationship to the member (i.e., account number, expiration date, data provided by the member, other electronic data gathered by the merchant/agent, and so on). This term also accounts for other personal insights gathered.

Card Validation Number

The three or four digit value printed on the signature panel of a card or front of the card on American Express.

External Connection

A connection originating from a device located on an external network and terminating on a device located on an internal network.

External Network

Any network which is not under the direct control of a state agency. The Internet is a prime example of an external network. Other external networks may include other state or federal WANs.

Media

Any physical item which contains information. Such items may include paper (printed or handwritten); back-up tapes, storage devices (e.g., floppy disks, USB drives, hard drives), etc. Within the context of this policy, media shall refer to all media which contains Cardholder Data.

Payment Card

Payment cards are all credit and debit cards and their associated account numbers and other personally identifiable information.

Payment Card Industry (PCI)

A consortium of payment card companies including Visa, Mastercard, and Discover.

Sensitive Authentication Data

Sensitive Authentication Data can be:

- The contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.)
- The card-validate code (three or four-digit value printed on the front or back of a payment card), otherwise known as CVC2 or CVV2 data.
- The PIN Verification Value (PVV).

Sensitive Cardholder Data

Data stored on the card whose unauthorized disclosure may be used in fraudulent transactions. It includes, the account number, magnetic stripe data, CVC2/CVV2 and expiration date.

System Component

System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment.

S7.3 Standards

S7.3.1 PCI- DSS authorized tools will be used to ensure agencies accepting credit cards comply with State policy and PCI-DSS requirements. This will include:

- Agencies annually filling out the appropriate PCI self-assessment

questionnaire

- Annually validating, where applicable, PCI compliance of third-party application and gateways.
- Conducting quarterly vulnerability security scans for all merchant card solutions having outward facing IP addresses.
- Reporting issues, detected in the self-assessment or the quarterly vulnerability scans, to Chief Information Security Officer (CISO), the Director of the Division of Finance, and the appropriate Agency Services IT Director.
- Developing and executing a required remediation plan for each detected PCI non-compliance issue.

S7.3.2 Merchant card payment solutions will incorporate requirements defined within the PCI-DSS.

S7.3.2.1 Network Security

- DTS managed networks transmitting or storing credit card data adhere to DTS 5000-1760 Firewall Management Policy.
- Wireless network access points are not installed without prior approval of DTS.
- Wireless networks are segmented from all networks transmitting or storing cardholder data.
- Direct public access is prohibited between external networks and any system components that stores cardholder data.

S7.3.2.2 System Settings

- All vendor default security settings are changed-prior to installing the system on the network.
- Default accounts and passwords are disabled or changed prior to installing systems on the network.
- Production systems are hardened by removing all unnecessary services and protocols
- Secure encrypted communications are used for remote administrative access.

S7.3.2.3 Protect Stored Cardholder Data

- Sensitive cardholder data is disposed when no longer needed.
- The full contents of any track from the magnetic card stripe is not stored in any manner.
- The card-validation code is not stored in any manner.
- The Primary Account Number (PAN) is masked when displayed. The

first six and last four digits are the maximum number of digits displayed

- In cases where a PAN must be stored, it is rendered unreadable via encryption, truncation or a one way hash.
- Account numbers are sanitized (encrypted, truncated or hashed) before logging them in the audit trail.
- Access to card account numbers is restricted-on a need-to-know basis.
- Employees having access to systems containing bulk merchant card data are required to successfully complete a background check.

S7.3.2.4 Encrypted Transmission of Cardholder Data

- Transmissions of sensitive cardholder data is encrypted using strong and secure protocols, such as secure sockets layer (SSL)/ transport layer security (TLS) and Internet protocol security (IPSEC).
- Card holder data is transmitted over any wireless network
- Credit card numbers are NOT transmitted via email unless encrypted.

S7.3.2.5 Anti-Virus, Anti-Spyware Protection

- All workstations and servers have installed and run appropriate anti-virus and anti-spyware software and definitions are updated regularly.

S7.3.2.6 Applications and Systems Security

- All networks and systems transmitting or storing credit card data are in accordance with the firewall configurations as specified by requirement 1: Build and Maintain a Secure Network of the PCI DSS.
- All systems are updated with the latest security patches within a reasonable time of their release.
- The software and development process are based on industry best practice and information security is included throughout the process.
- Sensitive cardholder data is sanitized before being used for testing and development.
- All changes to production systems are formally authorized, planned and logged.
- Sensitive cardholder data stored in browser cookies are secured or encrypted.
- Where possible computer system that store, process or transmit cardholder data are segmented off from all other systems within an agency network.

S7.3.2.7 Strong Access Control Measures

All computer systems that store, process or transmit cardholder data ~~must~~ comply with 5000-1404-S1 DTS Password Standard. Additionally:

- First-time passwords are set to a unique value for each user and

require the user to change the password immediately after first use.

- All remote and administrative access is via a secure connection.
- All user accounts are regularly reviewed to ensure that malicious, out-of-date and unknown accounts do not exist.
- All inactive accounts are automatically disabled after a pre-defined period.
- Vendor accounts used for remote maintenance are disabled when not needed

S7.3.2.8 Physical Access

- Multiple physical security controls prevent unauthorized access to the facility.
- Equipment and media containing cardholder data is physically protected against unauthorized access.
- Cardholder data printed on paper or received by fax is protected against unauthorized access.
- Proper procedures for the distribution and disposal of any media containing cardholder data are followed.
- All media devices that store cardholder data are inventoried and properly secured. The merchant copy of receipts is kept according to State Records retention policy.
- Cardholder data is deleted or destroyed before it is physically disposed of according DTS Policy 5000-0001 - Removal of Data from Decommissioned Storage Devices.
- All cache memory containing merchant card data is cleared at least daily.

S7.3.2.9 Track and Monitor Access

- All access to cardholder data is logged.
- Logs contain successful and unsuccessful login attempts and all access to the audit logs.
- Critical system clocks are synchronized with the agency's time server, and logs include date and time stamps.
- Logs are secured, regularly backed up and retained for three months online and one year offline.

S7.3.2.10 Test and Auditing of Security Controls and Systems

- The DTS Enterprise Information Security Office (EISO) tests, at least annually, security controls, limitations, and network connections.
- The EISO contracts with an approved security vendor to perform quarterly external scans and assessments.
 - Agencies accepting credit cards submit to the EISO a list of all

IP address for inclusion in the quarterly scans.

- DTS performs ongoing internal and external scans and evaluation of security controls to identify and stop possible unauthorized access.
- Systems containing card holder data deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files.

S7.3.2.11 Training and Awareness

- A Security awareness and training program is established for all employees with access to credit card data.
- Employees with access to payment card data are required to acknowledge in writing that they have read and understand identified security policies, standards and associated procedures.

S7.3.2.12 Security Incident Plan

- Agencies adhere to all requirements pertaining to the establishment of a security incident plan as required by the PCI DSS and other applicable policies, including:
 - All actions necessary to secure any exposed data,
 - Reporting incidents to appropriate agency management, and
 - Reporting incidents to the DTS Enterprise Information security Office.
- Agencies-report all possible credit card breaches as described in the DTS 5000-1250 Computer Incident Reporting Policy.

S7.4 Related Documents

Payment Card Industry Data Security Standards	https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
DTS Policies and Standards	5000-1760 Firewall Management Policy 5000-1404-S1 DTS Password Standard 5000-0001 - Removal of Data from Decommissioned Storage Devices
Finance Policy	FIACCT 07-09.00 Revenue - Credit Cards

S7.5 Document History

Originator: Michael Allred
Next Review: March 2010
Reviewed Date: N/A
Reviewed By: N/A

S7.5.1 Document Information

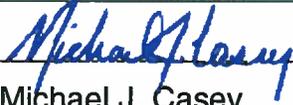
Property/Name	Value
Classification	For Official Use Only

S7.5.2 Revision History

Author	Description	Date Modified	Vers. #
Michael Allred	Cleanup from suggestions. comments	18.Jan-2008	.94
Michael Allred	Review and better line up with PCI Standard	25-Apr-08	.95
Michael Allred	Updated from comments and added additional content related to the PCI 1.1 standard	11-Jun-08	.96
Mike Casey	Final Draft	10/2/2008	.99
Mike Casey	Document approved	2/26/2009	1.0

S7.6 Appendices

None

DTS Representative			
Signature:		Date:	3/2/2009
Name (Printed):	Michael J. Casey	Title (Printed):	CISO/ DTS Director of Information Security