Texas Department
of Motor Vehicles

Workstation Modification Form

Submit questions related to this form to TAC-WMF@TxDMV.gov.

All modifications to or connectivity from an RTS workstation must be reviewed and approved by TxDMV. This includes credit card readers, keyboard, video and mouse (KVM) switches, automatic security cash drawer openers, peripherals, linking to databases, access to websites, firewall access, etc. To request any such modifications, please complete this form and submit to TAC-WMF@TxDMV.gov. Approval or denial will be communicated by return of this form via email to the email address listed below. Please allow 15 business days for processing.

Contact Information

County	County Contact Name	
Email Address	Phone Number	Cell Phone Number

Type of Request

Website Access □	**Device/Peripheral Connected to RTS Workstation** □	**Connection to County System** □

Website Information

URL	Type of Website	Business Justification for Website Access from RTS Workstation

Device/Peripheral Information

Type of Device/Peripheral (e.g., credit card reader, auto security cash drawer openers, etc.)	**Model Name**	**Model Number**	**Type of Connection** (e.g., USB, serial port, etc.)	Does connection of device require software (including device drivers) installed on RTS workstation? □Yes □No

Vendor Information	Vendor Name	Vendor Contact	Phone Number	Email Address

Description of how the device will be used:

Additional technical information for Credit Card Readers only

Website URL(s) (max of 5)	Does the payment process utilize more than five (5) external URSs?	Is the vendor certified PCI compliant?	Is the vendor PA-DSS compliant and/or is the system on the PABP list?
	□Yes □No	□Yes □No	□Yes □No

Attach the following technical documentation:

1) Vendor contract(s)
2) Appropriate PCI SAQ (self-assessment questionnaire)*

Click to download form

*The most recent PCI-DSS form version found on the PCI website should be used.

NOTE: Vendors must not accept charges using the RTS Network until they have been approved to do so.

County System Information

Description of County System:	Does the access to this County System require connection of the RTS Workstation to the county network? □ Yes □ No
Business justification for connection of County System to RTS Workstation:	

Additional Information (use this section to provide additional information or details about the requested modification(s))

Requested By

Name	Title
Signature	Date

For credit card readers, my signature above confirms that all impacted personnel have read the validation policy RTS Vendor Request for Credit Card Processing and agree to adhere to it.

TxDMV Use Only

Website Access	□ Approved	□ Denied	If denied, reason:
Device/Peripheral	□ Approved	□ Denied	If denied, reason:
County System	□ Approved	□ Denied	If denied, reason:

Comments:

Reviewed by	Title
Signature	Date

Texas Department *of* Motor Vehicles
HELPING TEXANS GO. HELPING TEXAS GROW.

TxDMV Information Security Manual
Section 3.9, *RTS Vendor Request for Credit Card Processing*

Authority
As a convenience to our customers, the Texas Department of Motor Vehicles (TxDMV) may authorize third party merchants to provide payment card processing through the RTS network. Any activity involving the acceptance of payments for goods or services by means of credit or debit cards over the RTS network requires authorization from TxDMV. The agency has a fiduciary responsibility to its constituents and payment card processors to comply with the Payment Card Industry Data Security Standard (PCI DSS) when providing a conduit for payment card transactions. Failure to comply with this standard can result in serious consequences including: damage to reputation, litigation, and financial liability.

Credit and debit card merchants are required to follow strict procedures to protect customers' credit card data. These directives apply to all types of credit card activity including the: storage, processing, and transmission of card information. PCI DSS compliance is required of all merchants that store, process, and transmit cardholder data as well as the payment channels used in the procedure.

Purpose
The purpose of this policy is to establish the standard for the outsourcing of payment card processing by authorized third party merchants and to:

a) Ensure compliance with PCI DSS and other applicable policies & standards
b) Establish the governance structure for payment card processing & compliance activities via the TxDMV network
c) Define responsibilities for payment card services to vendors
d) Provide general guidelines regarding the handling of cardholder data

General Requirements
Merchants utilizing the Texas Department of Motor Vehicles' (TxDMV) network as a gateway for card payment processing must adhere to the following:

1. Payment Card Industry Data Security Standard (PCI DSS)- High Level Overview
    a. Build and Maintain a Secure Network and Systems
        - *Requirement 1*: Install and maintain a firewall configuration to protect cardholder data.
        - *Requirement 2*: Do not use vendor-supplied defaults for system passwords and other security parameters.
    b. Protect Cardholder Data
        - *Requirement 3*: Protect stored cardholder data.
        - *Requirement 4*: Encrypt transmission of cardholder data across open, public networks.

c. Maintain a Vulnerability Management Program
   - *Requirement 5*: Protect all systems against malware and regularly update anti-virus software or programs.
   - *Requirement 6*: Develop and maintain secure systems and applications.

ci. Implement Strong Access Control Measures
   - *Requirement 7*: Restrict access to cardholder data by business need to know.
   - *Requirement 8*: Identify and authenticate access to system components.
   - *Requirement 9*: Restrict physical access to cardholder data.

cii. Regularly Monitor and Test Networks
   - *Requirement 10*: Track and monitor all access to network resources and cardholder data.
   - *Requirement 11*: Regularly test security systems and processes.

ciii. Maintain an Information Security Policy
   - *Requirement 12*: Maintain a policy that addresses information security for all personnel.

RTS workstations should not be modified without written approval from TxDMV. Please refer to Section 5.1 in the County Equipment Guide for more details.

Merchants must perform an annual self-assessment in partnership with TxDMV. The PCI C-VT Questionnaire is a validation tool intended to assist merchants in self-evaluating their compliance with PCI DSS.

Credit card brand compliance validation levels and enforcement – Merchants should be familiar with all of the individual brand standards (VISA, MasterCard, Discover, Am Ex) and refer to them periodically.

Hardware used for payment card processing activities must not participate in regularly scheduled driver updates.

No more than five (5) external URLs may be used in the procedure for payment card processing.

Violations

Violation of this policy may result in revocation of payment card acceptance services. Additionally, merchants are subject to loss of TxDMV information resources access privileges, civil, and criminal prosecution.