PCI DSS Solution Overview and Implementation Guide

Toast, Inc.

Date: June 30, 2015

PCI DSS Overview

Toast, Inc. (Toast) is a PCI DSS approved service provider offering the Toast POS solution. As a service provider, Toast has overall responsibility for the design and implementation of our solutions, and we manage the solutions for our customers.

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. Four major credit-card companies created the PCI DSS jointly in 2004: Visa, MasterCard, Discover and American Express. The PCI DSS specifies and elaborates on twelve (12) major requirements that address six major objectives:

1. A secure network must be maintained in which transactions can be conducted.
2. Cardholder information must be protected wherever it is stored.
3. Systems should be protected against the activities of malicious hackers by using frequently updated anti-virus software, anti-spyware programs, and other anti-malware solutions. All applications should be free of bugs and vulnerabilities that might open the door to exploits in which cardholder data could be stolen or altered.
4. Access to system information and operations should be restricted and controlled.
5. Networks must be constantly monitored and regularly tested to ensure that all security measures and processes are in place, are functioning properly, and are kept up-do-date.
6. A formal information security policy must be defined, maintained, and followed at all times and by all participating entities.

Toast has taken steps to address the PCI DSS requirements in regards to the Toast POS through our own validation efforts. Understand that utilizing our Toast solutions does not remove you from the scope of your own PCI DSS requirements. In addition, if you capture cardholder data in other manners beyond the offered solution, the systems and environment utilized by these secondary methods are fully within scope of PCI DSS and are solely your responsibility.

It is critical that you never store cardholder information in an insecure manner. Toast recommends that you store information as securely as possible and as little as possible. Under no circumstances should Track data, pin blocks, or CVV values EVER be stored.

It is the user's responsibility to comply with any PCI requirements. Please see https://www.pcisecuritystandards.org/ for more information. We recommend that you use a PCI qualified Assessor to be sure that your environment is compliant.

Table of Contents

Introduction

The purpose of this manual is to provide you instruction to ensure your deployment of the Toast POS solution is performed in manner to enable you to achieve PCI DSS compliance as it relates to the Toast solution. In addition, this manual will provide you guidelines governing:

- Inventory Control and Monitoring Procedures
- Installation and Connecting POI Devices
- Physical Security of Devices
- Detection of Unauthorized Alterations or Replacement of Devices
- Appropriate Deployment Locations for POI Devices
- Monitoring of Third-Party Personnel access to POI Devices
- Securing of Devices Removed from Service
- Disposal of Devices
- Guidance for Managing Device Failure
- Troubleshooting
- Detection of Tampering

Finally, an appendix is provided that details what PCI DSS requirements are directly addressed by Toast as it pertains to the Toast POS solution.

It is of utmost importance that you adhere to the guidelines detailed within this guide. Failure to do will impact your PCI DSS compliance and may impact the security of the deployed solution implemented within your environment.

Installation and Connecting of Point-of-Interaction (POI) Devices

It is imperative that you follow the guidelines detailed below for the deployment of the Toast solution. Failure to do so may impact your PCI DSS compliance and the protections afforded to you.

Prior to deployment, you must understand that any modification to the deployment can and will impact your compliance. Such modifications may include:

- Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the POI device
- Attempting to alter security configurations or authentication controls
- Physically opening the device
- Attempting to install applications onto the device

Based on your hardware selection, the Toast POS solution may consist of cash drawers, receipt printer, et al. However, at a minimum the solution will consist of at least one (1) Android OS tablet and one (1) card reader. Our tablets come from various manufacturers and are standard consumer based tablets or tablets designed for enterprise use. The card reader you receive may come from one of two manufacturers: IDTech or MagTek. Each of these card readers are unique in that they come to you pre-injected with a PIN that enables encryption of cardholder data upon swipe. This encryption upon swipe provides you a higher level of security and can reduce the impact of PCI DSS to you.

The specific type of readers you may received are detailed in the table below:

Manufacturer	Device Make	Device Model	Encryption
MAGTEK	Dynamag		AES & 3DES using DUKPT
MAGTEK	uDynamo	SCRA	AES & 3DES using DUKPT
MAGTEK	BulleT		AES & 3DES using DUKPT
ID TECH	Shuttle	ID-80110010-XXX	AES & 3DES using DUKPT

For deployment, the devices are shipped directly to you. You will need to power on the tablets and connect them to your deployed wireless or ethernet network. The tablets provided will come pre-installed with the Toast solution. This software will communicate with our hosted solution to meet your needs.

For a payment card transaction, you will initiate payment through the Table POS solution. When prompted, you will swipe the patron's payment card through the card reader attached to the tablet. The card reader will encrypt the patron's card data with a pre-injected encryption key and transmit the captured data to Toast's PCI DSS validated payment gateway for authorization and payment capture over an 128-Bit TLS 1.1+ (AES) connection. If you are required to manually enter the patron's card data, the application will automatically encrypt the data with a pre-loaded RSA2048 public key. As with the swiped data, this data is transmitted to

Toast's PCI DSS validated payment gateway for authorization and payment capture over an 128-Bit TLS 1.1+ (AES) connection. Toast's payment gateway will return the results of the transaction attempt to the tablet. A receipt will be generated and printed if you have a receipt printer deployed. All transaction activity is recorded within our cloud solution for you to review as needed.

Protected (Credit Card Number) and sensitive cardholder data (track1/track2 data) is securely wiped from all devices upon authorization. Furthermore, the components deployed in your locations have no access to the cryptographic keys needed to decrypt the captured cardholder data. This greatly reduces the impact of PCI DSS to you.

To ensure the Toast POS can communicate with the Toast payment gateway, you must enable outbound HTTPS (TCP/443) connectivity from the tablets to the Toast payment gateway through your Internet firewall. No inbound access is required for the solution to operate. **Note: It is imperative that you do not allow unrestricted inbound access from outside networks to the Toast solution. Doing so will imperil your PCI DSS compliance.**

Wireless Networks

If using Toast handhelds or using WiFi with Toast Terminals, a wireless network is required to operate the system. Therefore, for you own PCI DSS compliance and overall protection, you must ensure your wireless network is deployed in a manner consistent with PCI DSS requirements. The secure deployment of a wireless network is solely your responsibility. In order for you to achieve PCI DSS compliance, the following guidelines must be followed for deployment of a wireless network:

- wireless encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions;
- default SNMP community strings on wireless devices must be changed;
- default passwords/passphrases on access points must be changed;
- firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks;
- other security-related wireless vendor defaults must be changed, if applicable; and
- wireless networks transmitting cardholder data or connected to the cardholder environment must use industry best practices to implement strong encryption for authentication and transmission.

If you have wireless network deployed within your environment and it is not part of your cardholder network, a firewall is required between any wireless networks and the cardholder data environment. The firewall must be configured to deny or control any traffic from the wireless environment into the cardholder data environment.

Remote Access

The solution does not support remote access capabilities. You, as a merchant, may choose to utilize these remote access capabilities, but in order to maintain PCI DSS compliance only remote access technology supporting two-factor authentication may be used. Two-factor authentication consisting of something you have, know, or are is required for remote access in order for you to maintain your PCI DSS compliance. In addition to the use of two-factor authentication, it is important to remember that the remote access capability should only be enabled when needed and disabled when no longer required. Furthermore, your remote access software must provide for the following features or configuration settings:

- You must ensure changes are made to the default setting in the remote access software;
- Remotes access software must be configured to only allow access from specific IP addresses;
- Encrypted data transmissions such as IPSEC VPN, SSH, 128-Bit TLS or must enforced;
- Access to customer passwords must be restricted to authorized personnel;
- Logging of remote access must be enabled;
- Systems must be configured so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed;
- Unique user IDs must be used for each user account;
- Authentication composed of passwords and two-factor authentication must be used for remote access;
- Remote access must not require or use any group, shared, or generic accounts or passwords;
- Passwords must change every ninety (90) days or less;
- Passwords must be a minimum of seven (7) characters;
- Passwords must contain both numeric and alphabetic characters;
- Password history of the last four (4) passwords must be kept and new passwords must be different than any of the last four (4) passwords;
- Account lockout must occur after six (6) invalid logon attempts;
- Remote access accounts must be locked out for no less than thirty (30) minutes or until reset by a system administrator; and
- Remote access sessions must timeout after no more than fifteen (15) minutes of inactivity.

Data Capture and Removal

The solution will capture the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere) within volatile system memory of the provided devices. The solution does not store, and may not be configured to store, sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)), card verification values or codes (the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data)), PIN, Encrypted PIN Block, or the Primary Account Number (PAN) after authorization.

The application automatically deletes the full contents of any track from the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere), card verification values or codes (the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data)), PIN, Encrypted PIN Bock and PAN

upon authorization from volatile memory, per DOD 5220.22-M guidelines, in which storage areas are overwritten with a random bit pattern five (5) times.

Cryptographic Materials

There is no stored cardholder data (sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)), card verification values or codes (the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data)), PIN, Encrypted PIN Block, or the Primary Account Number (PAN)) post-authorization by the solution. For offline and manually entered transactions, the application will encrypt the captured data with a RSA2048 public key. This key cannot be used to decrypt any captured cardholder data. As you the merchant have no ability to decrypt the cardholder data, key management requirements do not apply. Toast handles all key management requirements for keys involved with the deployed solution. If you, as the merchant, decide to retain cardholder data in an electronic means outside of the application using third party methods, you must ensure that you meet PCI DSS requirements for the secure storage of this data and adhere to the cryptographic key management guidelines identified in the latest PCI DSS standard.

Data Purging

As previously stated, the solution does not store and may not be configured to store cardholder data (sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)), card verification values or codes (the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data)), PIN, Encrypted PIN Block, or the Primary Account Number (PAN)) after authorization within your environment. As such, there is no need for you, as the merchant, to purge cardholder data from the solution provided to you onsite. However, as you may decide to retain cardholder data outside of the solution using third party means (Secondary payment method, Excel spread sheet, written hardcopy, etc.), you must understand that any cardholder data collected by the you exceeding the defined retention period must be purged based upon business, legal, and/or regulatory requirements in order for you to achieve and meet your own PCI DSS compliance requirements.

Required Services, Protocol, and Dependent Software

The solution does not require any additional software beyond that delivered to you as part of the overall solution.

The solution communicates over the TCP/IP protocol suite and does not rely on any other communication protocol for functionality. The application utilizes HTTPS (TCP port 443) to communicate with the Toast PCI DSS validated payment gateway over the Internet for authorization and payment capture.

Note: Communication with the payment gateway only requires Internet outbound HTTPS (TCP port 443) access. No Internet inbound access of any type is required for functionality. It is recommended that you disallow all Internet inbound access to the environment supporting the solution. You are required by PCI DSS to disallow all Internet inbound access to the device supporting the solution. Failure to do so will jeopardize your PCI DSS compliance.

The aforementioned protocols and services are the only protocols and services enabled by default "out-of-the-box". No unnecessary or insecure services, daemons, protocols or components are enabled by default by the solution on supporting systems, nor are any required by the solution to function properly.

Transmitting Cardholder Data

The solution transmits cardholder data over the Internet using 128-Bit TLS (AES) for encryption to the Toast payment gateway. This is done by default and cannot be disabled. This secure, encrypted transmission is required for you to maintain PCI DSS compliance. This is the only means of transmitting cardholder data supported by the solution; the application does not support and/or facilitate sending of PANs by end-user messaging technologies.

Note: Understand that the transfer of cardholder data across public networks must be encrypted in order for you to maintain your PCI DSS compliance.

Inventory Control and Monitoring

In order for you to maintain your compliance you must maintain an inventory of the provided Point-of-Interaction (POI) devices. You must track which devices are deployed, which are awaiting deployment, those that have been removed from service for repair or otherwise not in use, and those in transit for deployment or return for repair. It is recommended that you designate a Job Role or personnel responsible for maintaining the POI inventory and for inspection of devices.

For each area identified the following information must be recorded. It is recommended that you record this information upon receipt of your POI device and then update the location of each device as it transitions from storage, transit, deployment, and repair or return.

- Manufacturer of device;
- Make and Model of device;
- Serial Number of Device;
- Internal Inventory Number; (if applicable);
- General Description of Device (Color, Secure Seals, Labels, Hidden Marking, etc.);
- Number and type of physical connections (Network, Serial, etc)
- Device Location (Storage, Where Deployed, In Transit, Awaiting Repairs or Returned);
- Date of Location Inspection (Last Date device location was confirmed);
- Date of Last Inspection (last date device was inspected for tampering);
- Name of Job Role of personnel performing inspection; and
- Date inventory was last updated

Device inventories are to be performed no less than annually to confirm that inventory of devices is being catalogued and performed correctly; however, inventory must be updated as device transition in and out of service and from one location to another. This inventory must also be completed to confirm that all devices identified as being within your environment are currently within your possession and not missing.

Access to device inventory and to the devices themselves must be restricted to authorized personnel. The method for maintaining a device inventory is determined by you; however the method utilized must enable you to restrict access to the inventory tracking information and allow you to record who has had access to the inventory tracking information. Failure to do so will impact your PCI DSS compliance. In addition, you must be able to restrict access to stored devices and record who has accessed said devices and when access occurred.

During your inventory process, you must investigate the POI devices to identify unauthorized removal, tampering, or substitution of devices. Detection of these events may be an indication of a compromise of your environment. Inspection of device should compare information located on the device itself with the inventory information previously recorded. In addition, the inspection should look for indications that the device has been tampered with. Indications of tampering may include, but is not limited to, attachment of

unauthorized devices to the POI device, breakage of security seals, cracks within the seal of the device itself, or insertion of a “skimmer” device within the Magnetic Stripe Reader (MSR) of the device. Skimmers are devices used by attackers to capture cardholder data prior to the POI device reading the card. Skimmers may be inserted in the MSR of the device or overlaid on the device itself. It is recommended that you training personnel interfacing with the POI devices on a regular basis to inspect deployed POI devices daily.

Should you detect a compromised device or find that your inventory indicated a missing or substituted device, you must report this information to Toast immediately. Contact information may be found in the Support section of this manual.

Device Physical Security

Maintain proper physical security of POI devices is required for you to maintain your own PCI DSS compliance and for you to ensure that devices have not been tampered with. Physical security of devices must be addressed in four key areas prior to receiving, during storage, and while in transit.

Receiving

Toast takes all necessary precautions to ensure devices are not tampered with or compromised prior to be shipped to you. However, there are steps that you must undertake to ensure that devices have not been tampered with during transit.

First you must confirm that shipment of devices originated from one of the following locations:

Toast, 100 Cambridge Park Drive, **Cambridge MA 02140**

DCRS Solutions, 2605 Metro Boulevard, Maryland Heights, MO 63043

If using devices purchased from Toast, Inc., in order to remain compliant, you may only deploy POI devices that are shipped from one of the aforementioned locations. Confirmation that devices were shipped from an authorized source may be performed by comparing the shipping information with the information listed above.

If you cannot confirm the device was shipped from an authorized source, DO NOT deploy the device.

In addition to confirm shipping origination, you must confirm that neither the packaging nor the device has been tampered with. All POI devices will be shipped using tamper-evident packaging. This packing will be evident on the shipping package itself and internally. Examples of said packaging include:

- Sealed Tamper Evident Bags: like Tamper Evident Deposit Bags
- Tamper Evident Tape used on all seams of the box

You must also inspect the device. You should look for broken security seals and cracks around device's seals to determine if the POI device itself has been compromised. If you believe the packaging or the device has been tampered with, DO NOT deploy the device.

For device confirmation or reporting of tampering, please contact us immediately. If it is determined that a device or package has been tampered with, we will provide you an address for the return of the POI device so we may conduct a further investigation.

Storage, **including periods of NON-USE (even END of SHIFT)**

For device being stored be it prior to deployment, shipment, or awaiting repairs, they must be stored in a secure area with restricted access to ensure they are not tampered with. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

- Device must be stored in locked room or container;
- Storage location must support restricted access;
- Must restrict access to authorized personnel.

Example include:

- Door/Container requiring key access in which defined personnel have access to the key; or
- Door/Container required knowledge of cipherlock code in which defined personnel have knowledge of the cipherlock code.
- Access to room or container storing device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access);
- Access to room must be monitored (Cameras or physical sight).

Transit

When you are shipping devices to your location for deployment or for return, devices must be shipped securely. They must be packed in tamper-evident packaging and shipped in a secure manner. All devices either being shipped to a location for deployment or for return, must be shipped using a secure transport method such as a secure courier or bonded carrier (e.g. UPS, FedEx). For deployment to sites, it is permissible to use employees for transport; however, they must be authorized to delivery the devices and the recipient must be notified of who will be delivering the devices to them. Be it a bonded carrier, secure courier, or internal employee, you must log the following information:

1) Personnel providing shipping (if employee, record name and job role);
2) Date of pickup
3) Device being shipped
4) Confirmation Date of Site delivery

When packaging devices for transit, they must be packed in tamper-evident packaging. You determine the type of packaging; however the recipient must be notified as to how to determine if the package has been tampered with during transit. As with your inspection of POI device received from us, your deployment sites must perform the same inspection on device shipped from your storage location. They must be notified of

authorized shipping locations, notified of how the device will be shipped, and trained in how to inspect the packaging and device for tampering. For example, they must be trained to investigate for breakage of tamper-evident seals on the external packaging and to investigate the device itself for cracks or breakage of security seals. Finally, they must be instructed that if they receive devices without prior confirmation from the shipping location or they are delivered in a manner unexpected, they must confirm prior to deployment of the devices.

Special Note: If using internal employees for device shipment, they must be instructed to not leave devices in public areas unattended, for example, in the front or back seat of a car. This may lead to unauthorized access or theft of the device.

Detection of Unauthorized Alterations or Replacement of Devices

You must implement procedures for the detection of unauthorized alterations or replacement of devices prior to use and once deployed. This is imperative to maintaining the security of the solution and in enabling you to maintain your PCI DSS compliance.

Prior to Deployment

While awaiting deployment, the device must be deployed in a secure storage location with restricted access. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

1) Device must be stored in locked room or container;
2) Device must remain in its original, tamper-evident packaging or in a physically secure storage until ready for use;
3) Storage location must support restricted access;
4) Must restrict access to authorized personnel. Example include:
    a. Door/Container requiring key access in which defined personnel have access to the key; or
    b. Door/Container required knowledge of cipherlock code in which defined personnel have knowledge of the cipherlock code.
5) Access to room or container storing device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access);
6) Access to room must be monitored (Cameras or physical sight).

Once the device is removed from storage and is being prepped for deployment, the following steps must be implemented:

1) The serial number on the devices must be matched with the recorded serial number of the device removed from storage and shipped to the location. This information must be recorded within inventory tracking at the deployment location and at the shipping location at the time of deployment;
2) A pre-installation of the device must be performed to ensure the device has not been tampered with. This must include physical inspection of the device to search for breakage of seal and security tampering seals; and
3) Prior to finally deployment into production, functionality must be tested to ensure that the device communicates and captures data properly.

Special Note: It is recommended that a list of device and serial numbers approved for a defined location be delivered to the location separate from the devices themselves. This will circumvent an individual from being able to substitute devices with differing serial numbers and updating the inventory list to reflect the compromised devices.

Post Deployment

Once devices have been deployed, periodic inspection must be made at deployment locations to ensure devices have not been tampered with or substituted. The type of location for deployment will drive the frequency for inspections. For high traffic, visible areas, it is recommended inspections occur twice a year. For locations that are remote or unattended, it is recommended that inspections occur every ninety (90) days.

When inspecting devices the first step should be to compare the serial number of the device with the serial number recorded for the location. If the serial numbers do not match, this could be the result of an unauthorized substitution. The individual should contact the personnel responsible for the storage, shipping, and installation of the POI device to confirm if the documentation is incorrect or if indeed a device has been substituted. Once the serial number has been confirmed, the device should undergo a physical inspection for tampering. Tamper and security seals should be examined to see if the seals are broken. The connection to the device should be inspected to ensure no extraneous devices are attached. The device should be inspected for missing screws, holes, or the addition of labels or covering that could be used to mask damage. Finally, the card DIP or magnetic stripe reader of the POI device should be investigated to ensure a "skimmer" or other type of device as not been inserted. If tampering is suspected, one should contact the personnel responsible for the storage, shipping, and installation of the POI device to report the tampering. The device should be taken offline. You should contact us (Toast) to report the tampering and we will provide remote assistance regarding the removal and return of the device for further investigation.

Appropriate Deployment Locations

When deploying a POI device, you must deploy them in the most secure manner possible. The following recommendations for deployment are provided:

1) Public access (non-employee) to devices must be limited such that they only have access to portion of the device needed to complete the transaction. For example, they should only have access to the card reader.
2) If the devices are stationary, they should be physically secure to prevent theft. For example, they should be bolted down.
3) Finally, they should be place in an area the easily viewable by employees and management. This will reduce the chances that a device is tampered with.

If the devices are deployed in a remote location or unattended, it is recommended that the devices be monitored with a camera so that one may review footage to determine if someone has attempted to tamper with the device. In addition, during off-hours, the device should be move to a secure location to reduce chance of theft and/or tampering.

Third-Party Access Monitoring

Access to POI devices by third-party personnel for repair/maintenance must be monitored. This monitoring is required to ensure there is no unauthorized access to device that could result in tampering, theft, or substitution of the device. To ensure proper third-party access monitoring, you should have a policy in place that requires the following steps:

1) Maintenance/repair of the device must be pre-arranged with date and timeframe of third-party personnel defined. Unexpected visits for repair/maintenance must be verified. If they cannot be verified, access to the device must be denied;
2) Prior to granting access to a device, personnel must be identified and authorized to access the device;
3) Third-party personnel access must be recorded and include personnel name, company, time of access, and purpose of access. Log must be maintained for no less than one year;
4) Personnel must be escorted and observed at all times; and
5) Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried.

Securing Devices Removed From Service

When devices are removed from service either for repair, being returned, being replaced, or being returned to storage, this must be done in a manner that allows for the tracking and security of the device. The following initial steps are required regardless of the reason a device is removed from service:

1) Removal of device must be pre-arranged prior to removal;
2) Location of device removal must confirm personnel removing device are authorized;
3) Personnel performing removal must be documented to include name, company, and time of removal; and
4) Inventory must be updated to indicate that the device was removed and reason for removal.

If the device is to remain at the deployment location for future deployment, the device must be securely stored at the location in a manner as described earlier within this manual.

If the device is to be returned to your shipping location, the device must be packed in a tamper-evident package and shipped using an authorized source that can be tracked. Methods for shipping and tracking are described in previous sections of this manual.

If the device is to be returned to us for repair or replacement, you must take the following steps:

1) Perform the Steps provided to you via the support contact below or the documentation you received with the device to wipe the device of all sensitive data.
2) Pack the device within a tamper-evident packaging; and
3) Notify us that the device is being returned. You will need to provide us the serial number of the device and a tracking number of the package as provided by the carrier.

Disposal of Devices

Disposal of devices will be handled by Toast or our authorized parties. If you have device for disposal, please follow the instruction regarding the removal of device for repair and return the device to us.

Troubleshooting

In the event of an issue, we will work with you to troubleshoot the issue. Prior to any troubleshooting, we will confirm that the individual contacting us is an authorized individual within your organization for troubleshooting purposes as defined to us during the initial deployment of the solution.

During our troubleshooting process:

1) Primary Account Number or Sensitive Authentication Data will never be outputted to your systems;
2) We will only collect the Primary Account Number or Sensitive Authentication Data as need to resolve the issue;
3) Data collected will be encrypted upon storage;
4) Data will be stored in specific, known locations with access restricted to those individuals charged with resolving your issue;
5) We will only collect limited amounts of data needed to solve the issue; and
6) All data will be securely removed from storage immediately after use and the issue is resolved.

Contact and Support Information

Customers may contact **DCRS** (**not** Toast) for support in troubleshooting the provided solution. Toast support consists of phone and, when needed, remote access support. Toast support may be contacted at:

Phone: **DCRS 314-739-6666 ... do not call Toast unless instructed by DCRS** 1-617-682-0225

Email: **support@DCRS.com ... do not email Toast unless instructed** support@toasttab.com

Note: Toast will not collect sensitive authentication data (magnetic stripe data, card validation codes or values, and PINs or PIN block data) or Primary Account Numbers (PAN) for any reason, even upon customer request. To do so may compromise Toast own PCI DSS validation and, in return, your PCI DSS compliance.

If you, as a customer, decide to collect sensitive authentication data as part of your own troubleshooting process, you must adhere to the following guidelines or risk compromising your PCI DSS compliance:

- You must only perform the collection of sensitive authentication data when needed to solve a specific problem;
- You store such data in a specific, known location with limited access;
- You must perform collection of only the limited amount of data needed to solve a specific problem;
- You must provide for the encryption of sensitive authentication data as required upon storage; and
- You must perform secure deletion of such data immediately after use, using tools which utilize the DoD 5220.22-M military grade secure deletion process.

PCI DSS Requirements Addressed by Toast for the Toast POS

Toast addresses the following requirements for the Toast POS only. Full adherence to PCI DSS is solely your responsibility for all payment acceptance methods.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 1 addresses the security of your network environment. The security of your network is solely your responsibility.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirements	Comments
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.	For the Toast provided devices, all vendor-supplied defaults have been removed or disabled.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	For the wireless network connectivity, all vendor defaults have been changed and are unique to your environment.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	Toast has developed configuration standards for the devices to be deployed in your environment. These standards are based on SANS and NIST guidelines.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	Toast has designed the solution so that each device performs a single purpose function.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	The Toast solution only supports those services, protocols, daemon, etc. that are necessary for functioning system.

2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	Non-console access to devices is permissible through the use of SSH or over HTTPS.

Protect Stored Cardholder Data

Requirement 3: Protect stored cardholder data

The access solution does not retain cardholder data (protected or sensitive post-authorization) and all captured cardholder data is securely wiped upon authorization. Protection of cardholder data outside the Toast solution through secondary payment measures are your sole responsibility.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements	Comments
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS) • Satellite communications	The Toast Solution encrypts cardholder data upon swipe and transmits the cardholder data to our payment gateway through an 128-Bit TLS tunnel.

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control is prohibited.	The Toast Solution encrypts cardholder data upon swipe and transmits the cardholder data to our payment gateway through an 128-Bit TLS tunnel.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Toast has validated our adherence to PCI DSS requirement 5 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 5 for your systems and application outside of the Toast environment is solely your responsibility.

Requirement 6: Develop and maintain secure systems and applications

Toast has validated our adherence to PCI DSS requirement 6 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 6 for your systems and application outside of the Toast environment is solely your responsibility.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

Toast has validated our adherence to PCI DSS requirement 7 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 7 for your systems and applications outside of the Toast environment is solely your responsibility.

Requirement 8: Identify and authenticate access to system components

Toast has validated our adherence to PCI DSS requirement 8 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 8 for your systems and applications outside of the Toast environment is solely your responsibility.

Requirement 9: Restrict physical access to cardholder data

Toast has validated our adherence to PCI DSS requirement 9 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 9 for your systems and applications outside of the Toast environment is solely your responsibility.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and CHD

PCI DSS Requirements	Comments
10.1 Implement audit trails to link all access to system components to each individual user.	The Toast solution supports proper audit capabilities to link access to individual user.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.
10.2.1 All individual user accesses to cardholder data.	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.
10.2.2 All actions taken by any individual with root or administrative privileges.	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.
10.2.3 Access to all audit trails.	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.
10.2.4 Invalid logical access attempts.	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.

10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.
10.2.6 Initialization, stopping, or pausing of the audit logs.	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.
10.2.7 Creation and deletion of system-level objects.	The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.
10.3 Record at least the following audit trail entries for all system components for each event:	
10.3.1 User identification	The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.
10.3.2 Type of event	The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.
10.3.3 Date and time	The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.
10.3.4 Success or failure indication	The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.
10.3.5 Origination of event	The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.
10.3.6 Identity or name of affected data, system component, or resource	The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.

10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	The Toast solution has been designed to utilize proper time-synchronization technology.
10.5 Secure audit trails so they cannot be altered.	
10.5.1 Limit viewing of audit trails to those with a job-related need.	The Toast solution has been designed to limit access and viewing of audit trails to authorized individuals.
10.5.2 Protect audit trail files from unauthorized modifications.	The Toast solution has been designed to protect audit trail files from unauthorized modifications.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	The Toast solution has been designed to detect unauthorized changes to log files.

Requirement 11: Regularly test security systems and processes

Toast has validated our adherence to PCI DSS requirement 11 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 11 for your systems and applications outside of the Toast environment is solely your responsibility.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Toast has validated our adherence to PCI DSS requirement 12 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 12 for your environment outside of the Toast environment is solely your responsibility.