toast

Toast PCI Instruction Guide

Table of Contents

Purpose

Toast, Inc. (Toast) is a PCI DSS approved level 1 service provider offering the Toast POS solution. As a service provider, Toast manages the payment processing environment and has taken steps to address certain PCI DSS requirements through our own validation efforts and by providing guidance to our customers.

Partnering with a PCI DSS compliant POS provider does not make you compliant with PCI regulations. Toast was built, configured, and installed in such a manner as to assist you in meeting applicable requirements, but you as the merchant remain solely responsible for ensuring your business is compliant with all current legal and regulatory requirements to include those imposed by PCI SSC and the Card Brands. We recommend that you use a PCI qualified Assessor to be sure your environment is compliant. Please see https://www.pcisecuritystandards.org/ for more information.

Toast POS is a PA-DSS validated application when utilized with a Toast-issued Elo device[1]. Confirmation of Toast's PCI DSS and PA-DSS status can be verified at the following sites:

- https://www.visa.com/splisting/searchGrsp.do
- https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html
- https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications

The purpose of the guide is to:

1. Help you identify your appropriate PCI DSS reporting requirements and responsibilities as it applies to the Toast POS solution;
2. Provide guidance on how the Toast POS solution impacts a requirement and, whether said requirement is addressed directly or in part by the Toast; and
3. Provide a Deployment checklist for you or your Qualified Security Assessor's references on how the Toast POS solution is deployed by Toast integrators or should be deployed if you the merchant have selected to self-deploy the solution.

The scope of this guide is limited to the Toast POS solution, its supported hardware and is intended for merchants who have elected to utiliz+e Toast's implementation services.

[1] Hardware restrictions apply. Please check the PCI SSC website for a current list of validated hardware.

What are PCI DSS & PA-DSS

About PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitates the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI DSS comprises a minimum set of requirements for protecting account data and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with applicable PCI DSS requirements. PCI DSS requirements apply to organizations where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted.

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the third party per the applicable PCI DSS requirements protects the account data.

PCI DSS requires that merchants utilize PCI DSS compliant service providers or receive contractual agreement that a service provider will meet PCI DSS requirements for card data shared with them.

About PA-DSS

The Payment Application Data Security Standard (PA-DSS), formerly referred to as the Payment Application Best Practices (PABP), is a standard developed by the card brands and the PCI SSC. PA-DSS is a standard designed to work hand-in-hand with PCI DSS. PA-DSS was implemented in an effort to provide the definitive data standard for software vendors that develop payment applications. The standard aims to prevent payment applications developed for third parties from storing prohibited secure data including magnetic stripe, CVV2, or PIN. In that process, the standard also dictates that software vendors develop payment applications that are compliant

with PCI DSS.

For a payment application to be deemed PA-DSS compliant, software vendors must ensure that their software includes the following fourteen protections:

1. Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data.
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Log payment application activity.
5. Develop secure payment applications.
6. Protect wireless transmissions.
7. Test payment applications to address vulnerabilities and maintain payment application updates.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote access to payment application.
11. Encrypt sensitive traffic over public networks.
12. Secure all non-console administrative access.
13. Maintain a PA-DSS Implementation Guide for customers, resellers, and integrators.
14. Assign PA-DSS responsibilities for personnel, and maintain training programs for personnel, customers, resellers, and integrators.

Toast has pursued PA-DSS validation for our POS application when hosted on a Toast-issued Elo device. At this time, use of application with hardware not listed on validation report has not be tested or evaluated under the PA-DSS framework.

Merchant Reporting Requirements

Merchant Levels

Merchant reporting requirements are dependent upon a merchant defined merchant level. Merchant levels are defined by the individual card brands and are based on the number of payment card transactions a merchant does each year. Merchant levels and reporting requirements are identified in the table below.

Merchant Level	Transaction Volume	Reporting Requirements
1	6 Million+	Every Year: • Report of Compliance completed by a QSA or ISA certified internal auditor Quarterly: • Conduct quarterly ASV scans
2	1 to 6 Million	Every Year: • Report of Compliance completed by a QSA or ISA certified internal auditor; or • Self-Assessment Questionnaire completed by a QSA or ISA certified internal auditor Quarterly: • Conduct quarterly ASV scans
3	20,000 to 1 Million E-Commerce only	Every Year: • Self-Assessment Questionnaire completed by merchant or QSA Quarterly: • Conduct quarterly ASV scans
4	All other merchants	Every Year: • Self-Assessment Questionnaire completed by merchant or QSA Quarterly: • Conduct quarterly ASV scans

Note: Please review processing statements for the previous fiscal year to estimate your transaction volume per Card Brand.

Self-Assessment Questionnaire Types

Level 1 merchants are required to have a Report on Compliance (ROC) completed by an approved QSA. If you have an ISA certified internal auditor on staff, this individual may complete the ROC as well.

Only level 2 – level 4 merchants are eligible to complete a Self-Assessment Questionnaire (SAQ). The SAQ type you are eligible to complete is based on how you accept payment cards.

Merchants who deploy and use Toast POS as recommended are eligible for one of two types of SAQs: SAQ-C or SAQ-D for Merchant.

SAQ-C Eligibility

If you only process payment cards through Toast POS, you are eligible to complete SAQ-C. However, you must also meet the following requirements:

Requirement	Do I qualify?
Toast POS is deployed in an isolated network segment not connected to other non-payment related devices in your environment.	If Toast installed your POS to include company-approved networking equipment, our standard deployment process ensures this requirement is met. If you deploy the Toast POS solution yourself or use a secondary third-party, you will need to ensure they adhere to the Deployment Checklist in Appendix A to assure requirement one (1) above is being addressed.
You do not store cardholder data in an electronic form.	Toast POS does not store electronic copies of cardholder data; therefore, if you only process payments through Toast POS you will meet this requirement.
If cardholder data is retained, it is only in paper reports or copies of paper receipts.	Ensuring you only retain paper copies of reports or receipts displaying full account numbers is solely your responsibility.
You do not support an e-Commerce site, even if said site is fully outsourced to a third-party hosting provider.	If you utilize Online Ordering, SAQ D is most likely the appropriate SAQ. However, please consult a PCI Qualified Security Assessor to determine your options.

If you do not meet all of the SAQ-C requirements, or if you process payments through additional means such as a secondary POS vendor, we recommend you contact a Qualified Security Assessor for help in determining the appropriate SAQ.

SAQ-D for Merchants Eligibility

SAQ-D is the 'catch-all' questionnaire appropriate for merchants that do not meet the eligibility requirements for the other SAQs. Please refer to the PCI SSC website for information on the other SAQs. https://www.pcisecuritystandards.org/

Toast POS Solution

Based on your hardware selection, the Toast POS solution will consist of at least one (1) Android OS tablet and one (1) card reader, cash drawer and receipt printer. The card reader may be integrated with the tablet or a stand-alone device connected to the tablet. The picture below is an example of the solution:

Figure 1: Toast POS Solution Example

POI Device Detail

The following information lists the details of the PCI-approved POI devices available for use with Toast POS.

Note all POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transactio

n_security .php

POI Device Vendor	**Ingenico**
POS Device Model and Number	iCMP
PCI PTS Approval #	4-20235
POI Device Vendor	**Magtek**
POS Device Model and Number	eDynamo
POI Device Vendor	**Magtek**
POS Device Model and Number	Dynamag
POI Device Vendor	**Elo**
POS Device Model and Number	MSR E1001002

In addition to the Toast POS hardware, Toast recommends merchants purchase a Meraki router and Ubiquiti Access points which will be used to setup an isolated network for the Toast POS solution.

Figure 2: Meraki Router

Figure 3: Ubiquiti Access Point

To use Toast POS solution, you must have an Internet connection already in place prior to the solution's deployment.

Merchant General Responsibilities

Wireless Networks

If using Toast handhelds or using WiFi with Toast Terminals, a wireless network is required. Wireless networks must deployed in a manner consistent with PCI DSS requirements.

PCI DSS guidelines require:

- Wireless encryption keys must be changed from default at installation, and must be changed anytime someone 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 a wireless network or guest Wifi deployed on the same network as your Toast POS, a firewall is required between the wireless network and the cardholder data environment.

- The firewall must be configured to deny or control all traffic (only authorized business purposes) from the wireless environment into the cardholder data environment.

Remote Access

Your Toast-issued hardware may support remote access capabilities, depending on device make and model. Where available, remote access enables Toast to assist with support calls and similar troubleshooting requests. The software utilized by Toast to perform remote access has been configured to ensure compliance with PCI DSS.

Prior to use, we will confirm the individual contacting Toast is an authorized individual within your organization as provided during the initial deployment of the POS. We will then walk your authorized agent through the process to initiate the remote connection. Upon conclusion of the

call, directions will be provided to terminate the remote connection.

If you choose to utilize your device's remote access feature or other third-party software, note the requirements in order to maintain PCI DSS compliance:

- Unique user IDs and passwords must be used for each user account. Group, shared, or generic accounts or passwords are not permitted;
- Only remote access technology supporting two-factor authentication may be used for non-console and remote access;
- Set unique passwords for first-time use/password reset and require immediate change upon login;
- Passwords must:
    - change every ninety (90) days or less;
    - be a minimum of seven (7) characters;
    - contain 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;
- You must change default settings 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 be enforced;
- Access to 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;
- 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

Toast POS will capture the magnetic stripe data (located on the back of the card, contained in the chip, or elsewhere) within volatile system memory of the provided devices to perform authorization.Upon authorization, the application automatically deletes the full contents of any track data, card verification codes, PIN, Encrypted PIN Block and PAN from volatile memory per DOD 5220.22-M guidelines, in which storage areas are overwritten with a random bit pattern five (5) times.

The solution does not store, and may not be configured to store Sensitive authentication data, card verification values or codes, PIN, Encrypted PIN Block, or the Primary Account Number (PAN) after authorization.

Cryptographic Materials

Toast handles all cryptographic key management requirements for the Toast POS solution in accordance with PCI-DSS. As you the merchant have no ability to decrypt cardholder data, key management requirements do not apply you (Requirements 3.5-3.6, 8.2.1).
If you, as the merchant, decide to retain cardholder data outside of the application, 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, where applicable.

Transmitting Cardholder Data

The transfer of cardholder data across public networks (to include the Internet) must be encrypted to comply with PCI DSS compliance.

Cardholder data is transmitted over the internet from your POS to Toast's payment gateway using TLS 1.2. This secure connection is done by default and cannot be disabled. The application does not support and/or facilitate the sending of PANs by end-user messaging technologies.

Data Purging

As the solution does not store and may not be configured to store cardholder data, there is no need for you to purge cardholder data from your onsite hardware.

If you retain cardholder data outside of Toast POS (secondary payment method, historical records in hardcopy or server, etc.), you must monitor to and purge cardholder data in accordance with applicable business, legal, and/or regulatory requirements once your defined retention period has exceeded.

Required Services, Protocol, and Dependent Software

Toast POS does not require any additional software beyond what was delivered to you as part of the overall solution.

Toast POS 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 over the Internet with Toast's PCI DSS validated payment gateway for payment authorization and 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. PCI DSS requires you to deny all Internet inbound traffic. As Toast POS is installed on a physically segregated network and cardholder data is encrypted at the Point of Interaction (POI), it is not necessary to filter outbound traffic.

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.

Inventory Control and Monitoring

You must regularly perform an inventory of POI devices and maintain a record of the inventory in a secure location to prevent unauthorized access. Any variances in inventory, such as missing or substituted POI devices, must be reported to Toast immediately. At least annually, the inventory record(s) must be reviewed by management to ensure the inventory is being maintained and all devices are being catalogued.

The following information must be recorded on the inventory. Please find a sample in Appendix A.

- Make and model of device
- Device status (deployed, in storage, in transit, undergoing repair, or otherwise not in use)
- Location of device (for example, restaurant address or other site where the device is located)
- Device serial number or other method of unique identification.
- Hardware/Firmware versions
- Date of inspection and name of person(s) performing inspection
- Date inventory was last updated and name of person(s) performing update

POI Inventory and Monitoring - Recommendations

- Begin recording inventory information upon receipt of your POS solution and update the location of each device as it transitions from storage, transit, restaurant use, and repair or return.
- Designate a specific job role or group of personnel responsibility for maintaining the POI inventory and for periodic inspection of devices to identify unauthorized:
    - Removal – missing devices, devices not located where previously recorded on the device inventory, etc.
    - Tampering – indications a device has been tampered with may include, but are not limited to, attachment of unauthorized devices, broken security seals, cracks within the seal of the device itself, or insertion of a "skimmer" device within the Magnetic Stripe Reader (MSR).[2]
    - Substitution – Devices who serial or other identifying numbers do not match those listed on the inventory or where such numbers have been partially or fully scratched out.
- Provide basic inspection training to all employees using Toast POS so that they may inspect equipment for obvious signs of compromise before their shift.

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:

- Maintenance/repair of the device must be pre-arranged with date and time frame 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;
- Prior to granting access to a device, personnel must be identified and authorized to access the device;
- 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;
- Personnel must be escorted and observed at all times;
- Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried;
- Personnel should provide you with a Qualified Implementor or Reseller certification evidencing they comply with the PCI QIR program.

[2] 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.

Installation and Removal of Devices

If Toast performs installation, we will take appropriate steps to ensure the security of the device(s) before deployment. If you elect to self-install or hire a third-party, the following steps must be performed before installation:

- The serial number on the device(s) must be matched against the serial number recorded for the device at the time it was shipped to your location and/or removed from storage.
- The device should be inspected for signs of tampering such as broken security seal, loose casing, screw holes, or the addition of labels or coverings, etc.

The following steps are required whenever a device is removed from service:

- Management should provide written instruction or memorialize verbal instructions for the device removal, to include the name and company of the person authorized to perform the removal as well as the date and time of removal.
- If management is not present, on-site personnel must confirm the identity of the individual(s) removing device are authorized;
- The device Inventory must be updated to indicate that the device was removed.
- The device must be securely stored until it is returned to Toast or securely disposed of.

Device Physical Security

To ensure tampered devices are not introduced into your POS environment, PCI DSS requires devices be physically secured while in transit (to/from), storage, and when in use.

Toast securely configures, stores, and packages devices to ensure devices are not tampered with or compromised while in our possession. However, there are steps you must undertake before using your device and while it remains in your possession.

Transit

Toast securely configures, stores, and packages devices to ensure devices are not tampered with or compromised while in our possession. However, there are steps you must undertake before using your device to ensure they were not tampered with during transit.

1. Inspect the shipping slip to confirm your shipment of devices originated from Toast's Configuration Center location:

   Toast, Inc. 5 Commonwealth Ave, Woburn MA 01801

2. Inspect the packaging for signs of tampering such as openings, tears, or different tape. All POI devices will be shipped using tamper-evident tape on all seams of the box.

3. Upon opening the packaging, inspect the device(s) for broken security seals and cracks around the device seals which may indicate tampering.

If the shipment arrived from an unauthorized source or you suspect the packaging or device has been tampered with, DO NOT deploy the device. Please contact Toast immediately to report your suspicions. We will provide you an address for the return of the POI device so we may conduct a further investigation.

Storage

All devices must be securely stored when not in use (prior to deployment, while awaiting repairs, etc). Device must be stored in accordance with the following measures:

- Stored in a locked room or container;
- Storage location supports restricted access;
- Access is restricted to authorized personnel;
- Access to room or container storing device is logged, can be a written access log or system log (i.e.proximity card system that records access; and
- Access to room must be monitored (cameras or within physical sight).

Shipping

If you must ship or transport devices (to another restaurant location or to Toast for service/return), additional steps must be taken to ensure device security. This includes:

- Devices must be shipped in tamper-evident packaging. (i.e. tamper-proof bags or use of tamper-proof tape along all seams)
- Devices must be shipped using a secure transport method
    - A secure courier or bonded carrier (e.g. UPS, FedEx); or
    - Employee authorized by management to rransport the device;
- Recipient must be notified in advance of who will be deliver the device, how to inspect the device dor signs of tampering, and the serial number of the device being transported
- Recipient validates the identity of the employee delivering the device and the device serial number, then confirms delivery with restaurant management.
- Recipient inspects device for signs of tampering before deploying the device in their environment.

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

Be it a bonded carrier, secure courier, or internal employee, be sure to log the following information in the device inventory:

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

As with your inspection of the device received from Toast, shipping recipients must inspect the device before use. They must be notified of the shipping origination address, how the device will be shipped, and trained in how to inspect the packaging and device for tampering. Finally, they

must be instructed that if they receive devices without prior confirmation from the shipping location, devices delivered in an unexpected manner or devices evidencing signs of tampering, they should contact Toast immediately and not deploy the device.

In Use

You are responsible for physically securing your device(s) to prevent unauthorized tampering, removal, or substitution while they are deployed for use. Select an install location appropriate to the device and with protection measures in mind:

- Control public access to devices. Customers should only have access to those components of device needed to complete a transaction (screen, card reader/EMV)
- Locate devices in area where they can be observed/monitored by authorized personnel. Remember, fraud can be perpetrated by both customers and employees.
- Position the device in such a way as to make it difficult for unauthorized person to observe a PIN entry or a keyed-in card transaction.

Wireless and handheld devices can be challenging to secure:

- Utilize holsters to minimize the risk of employees setting the device down and leaving
- Secure the devices in a locked room after hours or when otherwise not in use.
- Use sign in-sign out sheets to track who has the device at all times

If you suspect a device has been tampered with while in transit, storage, or use:

- Do not deploy the device or remove it from use
- Contact Toast Support immediately to report your suspicions, which can include:
    - Physical device breach
    - Logical alterations to device (configuration, access controls)
    - Disconnection or reconnection of device
    - Connection of unrecognized device
    - Failure of encryption mechanism
    - Failure failure of any device security control

Disposal

Toast will securely dispose of Toast-issued devices upon request. If you have a device for disposal, please follow the instructions regarding removal/transit and sent the device to us.

Contact and Support Information

Customers may contact Toast Support for assistance troubleshooting the POS solution as well as to report security concerns. Prior to ay troubleshooting, we will confirm that the individual contacting us is authorized to provide instruction on behalf of your organization. Toast Support may be contacted at:

Phone: 1-617-682-0225

Email: 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) 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 Controls Impact & Toast Responsibilities

The following table is meant to assist in completing SAQ or ROC templates. The table details those PCI DSS v3.2.1 requirements that most commonly apply to our customer base, how the use of Toast assists you in satisfying a given requirement, and actions most merchants must perform to fully satisfy the requirement. It should be noted, that by using only the Toast POS solution, cardholder data is not electronically retained in your environment. If a requirement is not identified below, it is your responsibility to research and determine its applicability in your use case.

NOTE: You are fully responsible for understanding how the PCI requirements apply to your business and ensuring compliance with PCI DSS at all times. The following table is intended for guidance purposes only and should not be relied upon as an authoritative source of information. Please consult with your IT team or a QSA for information specific to your business operations.

Keyed to PCI DSS SAQ v3.2.1		
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	**Toast Notes**	**What you will need to do**
1.1 Establish and implement firewall and router configuration standards that include the following:		
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	Toast will confirm requestor's identity before executing change instructions. Toast performs periodic reviews of firewall and router configurations to ensure no unauthorized changes were performed.	You are responsible for approving all network connections and instructions to change firewall and router configurations.You are responsible for testing all network connections.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	If Toast performs your installation, a network diagram can be provided upon request that identifies all connections between the CDE and other networks as well as the flow of cardholder data.	You are responsible for maintaining and updating the network diagram.
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	If Toast performs your installation, a network diagram can be provided upon request that identifies all connections between the CDE and other networks as well as the flow of cardholder data.	You are responsible for maintaining and updating the network diagram.
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	When deployed per the Deployment Checklist, the Toast POS solution is setup on an isolated network segment. Connectivity between untrusted	You are responsible for ensuring proper segmentation for any additional services

	networks and the Card Data Environment (CDE) is controlled via firewall.	connected to the Toast POS network.
1.1.5 Description of groups, roles, and responsibilities for management of network components		You are responsible for management of network components.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	,	You are responsible for management of network components.
1.1.7 Requirement to review firewall and router rule sets at least every six months.	Toast will confirm requestor's identity before executing change instructions. Toast performs periodic reviews of firewall and router configurations to ensure no unauthorized changes were performed.	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*		
1.2.1 Restrict inbound and outbound traffic for the cardholder data environment to that which is necessary (i.e. valid business purpose) and deny all other traffic.	When deployed per the Deployment Checklist, the Toast POS solution is setup in an isolated network with firewall(s) in place to secure against Wifi networks and systems outside the CDE. By default, All inbound traffic not required for normal operation of the POS solution is denied. It is not necessary to deny outbound traffic as cardholder data in encrypted at POI and the POS solution is setup in an isolated network.	.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	When deployed per the Deployment Checklist, the Toast POS solution is setup in an isolated network with firewall(s) in place to secure against Wifi networks and systems outside the CDE. By default, All inbound traffic not required for normal operation of the POS solution is denied. It is not necessary to deny outbound traffic as cardholder data in encrypted at POI and the POS solution is setup in an isolated network.	

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.		
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	The Toast POS is deployed within a network segment internal to your network. The deployment prevents any direct public access to the CDE from the Internet.	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	If Toast performs your installation, firewall rules will be created to include deny all inbound traffic not required for operation of the services.	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	If Toast performs your installation, firewall rules will be created to include deny all inbound traffic not required for operation of the services.	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	It is not necessary to deny outbound traffic as cardholder data in encrypted at POI and the POS solution is setup in an isolated network.	
1.3.5 Permit only "established" connections into the network.	When deployed per the Deployment Checklist, only established connections are permitted. Note: No connections initiated from outside the CDE are permitted by default.	
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	The Toast POS is deployed within a network segment internal to your network. Note: As cardholder data is encrypted at the POI and your POI device is not capable of decryption, cardholder data is never stored within Toast POS.	
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls, • Removal or filtering of route advertisements for private networks that employ registered addressing,	Toast utilizes NAT to obscure IP addresses. Toast will only disclose private IP addresses and routing information to authorized parties upon request. IP information can also be found on the device(s).	You are responsible for securing private IP addresses and routing information from unauthorized parties.

• Internal use of RFC1918 address space instead of registered addresses.		
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.		You are responsible for ensuring handheld devices (e.g. ToastGo) if utilized are connected to the isolated and/or properly segmented POS network.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.		You are responsible for maintaining appropriate policies and processes.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	**Toast Notes**	**What you will need to do**
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, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	Toast will change any default password or accounts prior to or during the deployment.	If you elect to self-deploy the POS solution, you are responsible for making said changes as outlined in the Deployment Checklist.
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.	Toast will change all wireless defaults at installation and implement appropriate Wifi security controls.	If you elect to self-deploy the POS solution, you are responsible for making said changes as outlined in the Deployment Checklist.
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).*		
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from coexisting 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.*	The Toast POS workstations are to provide payment functionality only.	
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	The Toast POS solution is delivered with all unnecessary services, protocols, daemons, etc. disabled.	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	The Toast POS solution is delivered with no unsecure services enabled. The solution only supports TLS 1.2 connectivity and all cardholder data is encrypted prior to transmission by the hardware or application.	
2.2.4 Configure system security parameters to prevent misuse.	The Toast POS solution is delivered with security parameters enabled to prevent misuse.	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	The Toast POS solution is delivered with all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers removed.	
2.3 Encrypt all non-console administrative access using strong cryptography. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	The Toast POS solution as delivered only supports console-based access.	
2.4 Maintain an inventory of system components that are in scope for PCI DSS.		You are responsible for maintaining an inventory of system components that are in scope for PCI DSS.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are		You are responsible for maintaining appropriate policies and processes.

documented, in use, and known to all affected parties.		
Requirement 3: Protect stored cardholder data	**Toast Notes**	**What you will need to do**
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: ● Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements ● Specific retention requirements for cardholder data ● Processes for secure deletion of data when no longer needed ● A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Toast POS does not retain cardholder data in electronic form.	This requirement only applies if cardholder data (PAN and/or SAD) is written down in hardcopy or received via mail.
3.2 Do not store sensitive authentication data (SAD) after authorization of the transaction even if encrypted. If SAD is received, render all data unrecoverable upon completion of the authorization process. SAD includes the data as cited in the following Requirements 3.2.1 through 3.2.3:		
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ● *The cardholder's name* ● *Primary account number (PAN)* ● *Expiration date* ● *Service code* *To minimize risk, only store this information as needed for business.*	Toast POS solution securely deletes full track data upon authorization. The solution cannot be configured to store this data.	
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment	Toast POS solution securely deletes card validation code/value upon authorization.	

card used to verify card-not-present transactions) after authorization.	The solution cannot be configured to store this data.	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	Toast POS solution securely deletes PIN or Encrypted PIN block upon authorization. The solution cannot be configured to store this data.	
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	Toast POS only displays truncated PAN.	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	Toast POS only displays truncated PAN. During Offline Mode, credit card information is temporarily stored on your device in an encrypted form.	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.		You are responsible for maintaining appropriate policies and processes.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	**Toast Notes**	**What you will need to do**

4.1 Use strong cryptography and security protocols 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		
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Toast POS encrypts data at the POI or upon manual entry into the solution. All data is transmitted to the payment gateway using a TLS 1.2 connection. In addition, if a wireless network is deployed by Toast, industry best practices are used to ensure strong encryption and transmission.	If you elect to self-deploy the POS solution, you are responsible for ensuring industry best practices are utilized to secure the wireless network(s).
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	Not applicable to your deployed Toast POS solution.	
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	As you the merchant do not have access to the Toast POS cryptographic keys, you are not responsible for this requirement.	
Requirement 5: Use and regularly update anti-virus software or programs	**Toast Notes**	**What you will need to do**
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	The Toast POS solution runs customized firmware deployed on an AndroidOS system. Toast is of the opinion our devices as configured are not "commonly affected by malicious software."	You are responsible for determining whether to deploy anti-virus software on your Toast device(s). Toast hardware permits users deployment of anti-virus software.
5.1.1 Ensure that antivirus programs are capable of detecting, removing, and	.	If you elect to deploy anti-virus software on your Toast device(s), you are

protecting against all known types of malicious software.		responsible for ensuring the software meets PCI requirements.
5.1.2 For systems considered to not be commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Toast monitors for security vulnerabilities that affect the POS solution and underlying systems to determine hardware susceptibility..	If you elect to deploy anti-virus software on your Toast device(s), you are responsible for ensuring the software meets PCI requirements.
5.2 Ensure that all anti-virus mechanisms are maintained as follows: ● Are kept current, ● Perform periodic scans ● Generate audit logs which are retained per PCI DSS Requirement 10.7.		If you elect to deploy anti-virus software on your Toast device(s), you are responsible for ensuring the software meets PCI requirements.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	.	If you elect to deploy anti-virus software on your Toast device(s), you are responsible for ensuring the software meets PCI requirements.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.		You are responsible for maintaining appropriate policies and processes.
Requirement 6: Develop and maintain secure systems and applications	**Toast Notes**	**What you will need to do**
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	Toast monitors for security vulnerabilities and has risk-rating processes in place. Toast monitors for security vulnerabilities that affect the POS solution and underlying systems. Toast has implemented a risk-rating process to assist in understanding and prioritizing remediations.	You are responsible for the devices within your environment, to include developing processes to stay abreast of security vulnerabilities and notifying Toast in the event you encounter a product vulnerability. .

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:*** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	Toast monitors for security vulnerabilities that affect the POS solution and underlying systems and issues updates and/or guidance as needed. Toast-issued devices are preconfigured to download security updates as they become available.	You are responsible for ensuring security updates are installed on your hardware as they become available. You are responsible for replacing your hardware once the support warranty has ended and manufacturer security updates are no longer provided.
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Toast ensures any significant changes to the solution comply with PCI DSS requirements.	You are responsible for ensuring any configuration changes you make to Toast POS solution or changes in how the solution is used are compliant with PCI DSS requirements.
Requirement 7: Restrict access to cardholder data by business need to know	**Toast Notes**	**What you will need to do**
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.		
7.1.1 Define access needs for each role, including: ● System components and data resources that each role needs to access for their job function ● Level of privilege required (for example, user, administrator, etc.) for accessing resources.	During deployment, Toast personnel will create a user account with administrative access for the restaurant point of contact. Users with Administrator access can invite or delete other account users and modify access and system privileges for all users. Note: Toast POS limits user access to a truncated PAN.	It is your responsibility to ensure access and system privileges are appropriate for each user.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Users with Administrator access can invite or delete other account users and modify access and system privileges for all users.	It is your responsibility to ensure access and system privileges are appropriate for each user.
7.1.3 Assign access based on individual personnel's job classification and function.	Users with Administrator access can invite or delete other account users and modify access and system privileges for all users.	It is your responsibility to ensure access and system privileges are appropriate for each user.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	.	

7.2.2 Assignment of privileges to individuals based on job classification and function.	Users with Administrator access can invite or delete other account users and modify access and system privileges for all users.	It is your responsibility to ensure access and system privileges are appropriate for each user.
7.2.3 Default "deny-all" setting.	The Toast POS access control feature supports a 'deny-all' setting by default.	
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.		You are also responsible for maintaining appropriate policies and processes. Note: additional policies or procedures may be required if employees hande physical payment cards or cardholder data is received via telephone or other electronic means and manually entered.
Requirement 8: Assign a unique ID to each person with computer access	**Toast Notes**	**What you will need to do**
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:		
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	During install, Toast will invite you via the email on record to create a unique administrator account.	You are responsible for the setup of any new accounts for your employee and administrator users.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Users with Administrator access can invite or delete other account users and modify access and system privileges for all users.	It is your responsibility to ensure access and system privileges are appropriate for each user.
8.1.3 Immediately revoke access for any terminated users.	Users with Administrator access can invite or delete other account users and modify access and system privileges for all users.	It is your responsibility to ensure user access is revoked when no longer required.
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: ● Enabled only during the time period needed and disabled when not in use. ● Monitored when in use.	Occasionally, it is necessary for Toast Support to remotely access the POS device. Toast Support will only do so with your permission and you must take affirmative steps to enable such access. The system will log all access and activity performed. Prior to concluding the remote session, Toast will instruct you on how to securely terminate the remote session.	You are responsible for enabling/disabling the remote access and monitoring remote users during active sessions.

8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	The Toast POS solution is setup by default to lock out user accounts after 6 failed attempts.	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	The Toast POS solution is setup by default to a lockout duration of 60 minutes.	
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	The Toast POS solution is setup by default to disconnect after 15 minutes of idle activity.	
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: ● Something you know, such as a password or passphrase ● Something you have, such as a token device or smart card ● Something you are, such as a biometric.		
8.2.3 Passwords/passphrases must meet the following: ● Require a minimum length of at least seven characters. ● Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	Toast POS is setup to require complex passwords by default.	
8.2.4 Change user passwords/passphrases at least once every 90 days.	Toast POS solution supports on-demand password changes.	You are also responsible for maintaining appropriate policies and processes.
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	Toast POS solution supports on-demand password changes.	You are also responsible for maintaining appropriate policies and processes.
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	Toast POS solution supports user created passwords. Added users will receive an email link which directs them to create a user profile and password.	You are also responsible for maintaining appropriate policies and processes.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Toast POS does not support administrative non-console access.	

8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	Toast POS supports multi-factor authentication. This feature is not enabled by default. Toast Customer Support accounts require users to perform multi-factor authentication before a remote support session can be established.	You are responsible for ensuring multi-factor authentication is enabled for all employee or third-party users accessing the system from outside of the your network.
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.		You are responsible for maintaining user access policies or processes.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: ● Generic user IDs are disabled or removed. ● Shared user IDs do not exist for system administration and other critical functions. ● Shared and generic user IDs are not used to administer any system components.	Toast POS supports unique accounts for each user.	You are responsible for maintaining user access policies or processes.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.		You are responsible for maintaining user access policies or processes.
Requirement 9: Restrict physical access to cardholder data	**Toast Notes**	**What you will need to do**
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.		
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.		It is your responsibility to ensure the security of your physical environment.

Note: *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*		
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	Toast will restrict access to unused network ports on networking equipment during install (plugs or tape).	It is your responsibility to ensure the security of your physical environment.
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.		It is your responsibility to ensure the security of your physical environment.
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)**.**		You are responsible for maintaining appropriate policies and processes.
9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.		You are responsible for maintaining appropriate policies and processes.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:		
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.		You are responsible for maintaining appropriate policies and processes.
9.4.2 Visitors are identified and given a badge or other identification that expires and that		You are responsible for maintaining appropriate policies and processes.

visibly distinguishes the visitors from onsite personnel.		
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.		You are responsible for maintaining appropriate policies and processes.
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months,		You are responsible for maintaining appropriate policies and processes.
9.5 Physically secure all media.		
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.		It is your responsibility to ensure the security of your physical environment.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:		
9.6.1 Classify media so the sensitivity of the data can be determined.		You are responsible for maintaining appropriate policies and processes.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.		You are responsible for maintaining appropriate policies and processes.
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).		You are responsible for maintaining appropriate policies and processes.
9.7 Maintain strict control over the storage and accessibility of media.		
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.		You are responsible for maintaining appropriate policies and processes.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:		

9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.		You are responsible for maintaining appropriate policies and processes.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note**: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*		
9.9.1 Maintain an up-to-date list of devices. The list should include the following: ● Make, model of device ● Location of device (for example, the address of the site or facility where the device is located) ● Device serial number or other method of unique identification.		You are responsible for maintain an up-to-date device inventory.
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	Toast ships all hardware in tamper-proof packaging. Delivery is handled by a secured courier and subject to delivery tracking.	You are responsible for ensuring devices are regularly inspected for evidence of tampering or substitution.
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: ● Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. ● Do not install, replace, or return devices without verification. ● Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). ● Report suspicious behavior and indications of device tampering or substitution to appropriate personnel		You are responsible for ensuring employees are trained on best practices for detecting attempted tampering or replacement of devices.

(for example, to a manager or security officer).		
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.		You are also responsible for maintaining appropriate policies and processes. Note: additional policies or procedures may be required if employees hande physical payment cards or cardholder data is received via telephone or other electronic means and manually entered.
Requirement 10: Track and monitor all access to network resources and cardholder data	**Toast Notes**	**What you will need to do**
10.1 Implement audit trails to link all access to system components to each individual user.	The Toast POS solution is setup by default to implement PCI DSS compliant logging.	
10.2 Implement automated audit trails for all system components to reconstruct the following events:		
10.2.2 All actions taken by any individual with root or administrative privileges	The Toast POS solution is setup by default to implement PCI DSS compliant logging.	
10.2.4 Invalid logical access attempts	The Toast POS solution is setup by default to implement PCI DSS compliant logging.	
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 POS solution is setup by default to implement PCI DSS compliant logging.	
10.3 Record at least the following audit trail entries for all system components for each event:		
10.3.1 User identification	The Toast POS solution is setup by default implement PCI DSS compliant logging.	
10.3.2 Type of event	The Toast POS solution is setup by default implement PCI DSS compliant logging.	
10.3.3 Date and time	The Toast POS solution is setup by default implement PCI DSS compliant logging.	
10.3.4 Success or failure indication	The Toast POS solution is setup by default implement PCI DSS compliant logging.	

10.3.5 Origination of event	The Toast POS solution is setup by default implement PCI DSS compliant logging.	
10.3.6 Identity or name of affected data, system component, or resource.	The Toast POS solution is setup by default implement PCI DSS compliant logging.	
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*		
10.6.1 Review the following at least daily: ● All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/ intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Toast has implemented internal security controls to monitor logs, detect anomalies and suspicious activity, and alert Toast staff for investigation.	
10.6.3 Follow up exceptions and anomalies identified during the review process.	Toast has implemented internal security controls to monitor logs, detect anomalies and suspicious activity, and alert Toast staff for investigation.	
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	The Toast POS solution retains audit trail history in accordance with PCI DSS requirements.	
Requirement 11: Regularly test security systems and processes	**Toast Notes**	**What you will need to do**
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to*		You are responsible for performing quarterly inspections of your location(s) to identify any additional access points (authorized or unauthorized).

detect and identify both authorized and unauthorized devices.		
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	At the time of installation, Toast will provide you a list of the devices setup as part of your deployment, to include wireless access points and SSID.	You must maintain this record and perform quarterly physical inspections of your location(s) to identify any additional access points (authorized or unauthorized).
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.		You are responsible for maintaining appropriate policies and processes. If an unauthorized access point is discovered during a quarterly inspection, it should be removed to comply with PCI DSS.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). **Note:** Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.		You are responsible for performing external and internal vulnerability scans Scans should be carried out as detailed in 11.2.1 and 11.2.2 below.
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.		You are responsible for maintaining appropriate policies and processes.

11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.		Every quarter, you must perform a scan of the internet connections(s) associated with your locations. Scanning services are offered by a number of third-party vendors. Please refer to the PCI SSC website for a list of approved scanning vendors. You are responsible for hiring and coordinating the scans with your vendor of choice.
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.		You are responsible for maintaining appropriate policies and processes.
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		You are responsible for performing external and internal vulnerability penetration tests.
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		You are responsible for performing external and internal vulnerability penetration tests.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.		You are responsible for maintaining appropriate policies and processes.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		You are responsible for maintaining appropriate policies and processes.

11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Toast has implemented security controls designed to detect and prevent intrusions to infrastructure under our control in accordance with PCI DSS.	You are responsible for security of networking devices and other infrastructure installed at your location(s).
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. **Note:** For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	Toast has implemented security controls designed to monitor for changes per PCI DSS and PA-DSS requirements and alert the appropriate personnel for investigation.	You are responsible for security of networking devices and other infrastructure installed at your location(s).
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	Toast has implemented security control configured to monitor for changes per PCI DSS and PA-DSS requirements and alert the appropriate personnel for investigation.	You are responsible for security of networking devices and other infrastructure installed at your location(s).
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.		You are responsible for maintaining appropriate policies and processes.
Requirement 12: Maintain a policy that addresses information security for all personnel	**Toast Notes**	**What you will need to do**
12.1 Establish, publish, maintain, and disseminate a security policy.		
12.1.1 Review the security policy at least annually and update the policy when the environment changes.		You are responsible for maintaining appropriate policies and processes.
12.2 Implement a risk-assessment process that:		You are responsible for maintaining appropriate policies and processes.

• Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.		
12.3 Develop usage policies for critical technologies and define proper use of these technologies. **Note:** Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage. Ensure these usage policies require the following:		
12.3.1 Explicit approval by authorized parties		You are responsible for maintaining appropriate policies and processes.
12.3.2 Authentication for use of the technology		You are responsible for maintaining appropriate policies and processes.
12.3.3 A list of all such devices and personnel with access		You are responsible for maintaining appropriate policies and processes.
12.3.5 Acceptable uses of the technology		You are responsible for maintaining appropriate policies and processes.
12.3.6 Acceptable network locations for the technologies		You are responsible for maintaining appropriate policies and processes.
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	In the event our support personnel require remote access for troubleshooting, you will be provided with instruction on secure connection and disconnection.	You are responsible for maintaining appropriate policies and processes.
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and	In the event our support personnel require remote access for troubleshooting, you will be provided with	You are responsible for maintaining appropriate policies and processes.

business partners, with immediate deactivation after use	instruction on secure connection and disconnection.	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.		You are responsible for maintaining appropriate policies and processes.
12.5 Assign to an individual or team the following information security management responsibilities:		
12.5.1 Establish, document, and distribute security policies and procedures.		You are responsible for maintaining appropriate policies and processes.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.		You are responsible for maintaining appropriate policies and processes.
12.5.4 Administer user accounts, including additions, deletions, and modifications.		You are responsible for maintaining appropriate policies and processes.
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.		
12.6.1 Educate personnel upon hire and at least annually.		You are responsible for maintaining appropriate policies and processes.
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.		You are responsible for maintaining appropriate policies and processes.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.		You are responsible for maintaining appropriate policies and processes.
12.8 Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows		

12.8.1 Maintain a list of service providers including a description of the service provided.		You are responsible for maintaining appropriate policies and processes.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	The merchant agreement you entered into with Toast, Inc satisfies this requirement.	You are responsible for ensuring any agreements with third-party service providers comply with PCI DSS.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.		You are responsible for maintaining appropriate policies and processes.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	As a service provider, Toast is required to maintain PCI DSS compliance and validate annually. You may validate our compliance by requesting a copy of our AoC or reviewing the following websites. PCI SSC : https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true Visa: https://www.visa.com/splisting/searchGrsp.do Mastercard: :https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html .	You are responsible for maintaining appropriate policies and processes.
12.8.5 Maintain information about which PCI DSS requirements are managed by each	This table provides a list of PCI DSS requirements that the Toast POS solution impacts.	You are responsible for maintaining appropriate policies and processes.

service provider, and which are managed by the entity.		
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.		
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ● Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ● Specific incident response procedures ● Business recovery and continuity procedures ● Data backup processes ● Analysis of legal requirements for reporting compromises ● Coverage and responses of all critical system components ● Reference or inclusion of incident response procedures from the payment brands.		You are responsible for maintaining appropriate policies and processes.
Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS	**Toast Notes**	**What you will need to do**
A2.1 For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS: ● Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are **not** susceptible to any known exploits for SSL/early TLS.	Toast POS does not use SSL or early TLS. Solution utilizes TLS 1.2 for all communication over the internet.	

Appendix A: Sample Inventory Record

Device model name(s) and number	**Device Serial number or other Unique Identifier**	**Device Status**	**Device Location**	**Hardware/ Firmware version(s)**
Magtek eDynamo	123456789	Storage - not in use	Location 101 Manager's office	N/A
Inventory Updated by	Jane Doe	Inventory updated on:	02/01/2018	
	Jane Doe		08/2018	
Annual Inspection Performed by:	John Smith	Annual Inspection Performed on:	6/01/2017	No issues
	John Smith		06/01/2018	No issues