PCI Checklist for Merchants using Restaurant Manager

This checklist is intended only as an overview of key data security standards. To fully verify PCI Compliance, merchants must refer to Self Assessment Questionnaire published by the PCI Security Standards Council and undergo a compliance audit using a certified PCI compliance auditor

RM Configuration Settings

- ❑ ENABLE: ***Enhanced Password Control***
- ❑ DISABLE or reset <***Master Password***> to non-default value
- ❑ CONFIGURE All Administrator Passwords with <***Password Expiration Days***> of "90" or to a lesser value that is greater than "0
- ❑ DISABLE: <**Save CC info in payment file**> (*unless there is proven business need*)
- ❑ SET <**Number of days to store CC Info**> to minimum required for business need
- ❑ DISABLE <**Save/Restore frequent diner credit card info**> (*unless there is proven business need*)
- ❑ SET <**Number of days to keep unused card info**> to minimum required for business need

Store Installation and Infrastructure

- ❑ RUN MD5 Hash Verification on PA-DSS certified POS software prior to installation
- ❑ INSTALL PA-DSS certified POS software on a Dedicated File Server
- ❑ GENERATE Encryption Key for PA-DSS certified software
- ❑ SECURE POS File Server by two (2) independent means (i.e. behind locked door or in locked cabinet, and also in area restricted to authorized personnel only or protected by other security system such as recording video cameras).
- ❑ CONFIGURE remote access with two factor authentication
- ❑ CHANGE default user and passwords on ***all*** hardware (i.e. fileserver, router, AP, Station computers)
- ❑ If Wireless Network Is Present
    - ❑ No open ports allowed from the WAN (Internet) directly to the server machine.
    - ❑ Firewall (with stateful packet inspection capability) installed between WAN/Internet and the store server machine / network, configured to disallow all incoming communication, and only allow POS required ports and protocols.
- ❑ If RM Handheld/RM Tablet wireless is in use:
    - ❑ INSTALL Firewall (with stateful packet inspection capability) between wireless network and the POS File Server / network, configured to only allow port 80, 53, and ICMP services through
    - ❑ . CONFIGURE wireless network for POS devices with WPA2 encryption, key rotation enabled, MAC address filtering enabled, non-default SSID, SSID broadcast disabled.
    - ❑ Any non RM Handheld/RM Tablet wireless network is isolated on separate subnet.

Store Procedures

- ❑ RESTRICT use of the POS File Server to POS functions only (e.g. no web browsing, email access, etc.)
- ❑ ESTABLISH protocols for managing passwords across the network (*e.g. do not allow common or shared passwords, verify identity before password reset, disable passwords of terminated users, do not use group/shared user accounts etc.*)
- ❑ DISABLE Remote Access applications except during specified service periods. (*Exception for applications that offer two factor authentication with single use authentication token.*)
- ❑ NEVER SEND or solicit credit card numbers or personal data via email or any other non-secure means
- ❑ ENSURE no credit card numbers or personal data are saved in any files stored on any system computers
- ❑ ENABLE automatic updates for all anti-virus, malware, and OS security applications
- ❑ GENERATE New Encryption Key and sign updated Key Custodian Agreement for POS software at least once a year
- ❑ SECURE all system backup media
- ❑ MAINTAIN an accurate inventory list of all system components has been created with the understanding it is to be kept current by the end user.

Merchant Responsibility

The attached checklist details software settings and business procedures that help merchants meet the Data Security Standards (DSS) imposed by the Payment Card Industry (PCI). These procedures include the requirements of Payment Application Best Practices (PABP). It is the responsibility of the merchant to ensure that their store infrastructure, business procedures, and POS System are compliant with these best practices.

Please note that the attached checklist is not a complete guideline for meeting PCI-DSS requirements. To fully verify PCI compliance, merchants are advised to refer to the PCI DSS publication - https://www.pcisecuritystandards.org/documents/SAQ_InstrGuidelines_v3-1.pdf , and to undergo a compliance audit using a certified PCI compliance auditor.

Dealer: _____ does not offer these auditing services and the installation of a PCI Compliant software application does not necessarily mean a merchant is compliant with PCI-DSS.

Responsibility for full PCI Compliance lies solely with the merchant. Please sign below to verify you have read and understood your responsibility as a merchant to ensure that your operations meet the Data Security Standards of the Payment Card Industry.

Company Name: _____

Merchant Signature: _____

Date: _____