Qualified Integrators and Resellers (QIR)™ Implementation Statement

The QIR Professional must complete this document for each Qualified Installation performed. This *QIR Implementation Statement* confirms what the QIR Professional did, what they observed and what they informed the customer of at the conclusion of the QIR Installation. The QIR Professional is not performing a PCI DSS assessment—compliance with PCI DSS remains the responsibility of the customer.

A copy of this *QIR Implementation Statement* must be delivered to the customer no later than ten (10) business days after completion of the Qualified Installation, and a copy must be retained by the QIR Professional.

Note: *A Qualified Installation may involve the installation of or upgrade to a payment application, or activities concerning the deployment, configuration, or access to other services in the customer's cardholder data environment.*

1. *If an application being installed or configured is PA-DSS validated, Part 2b of this statement should be completed.*
2. *The customer may request the QIR Professional to complete work beyond the scope of the QIR Program. This work should not be documented as part of the Qualified Installation.*
3. *This document is written as if Engagements and Qualified Installations are carried out by one QIR Professional. In the event that a larger project involves more than one QIR Professional, one of those individuals should be nominated as the primary or lead.*

The QIR Professional must adhere to the requirements defined in the *QIR Qualification Requirements* and *QIR Program Guide* for all Qualified Installations.

Part 1: Implementation Statement Summary

Customer Details					
Company Name:					
Contact Name:			Job Title:		
E-mail:			Telephone:		
Business Address:			City:		
State/Province:		Country:		Postal Code:	
URL:					

QIR Details					
QIR Professional Name:					
QIR Professional – Company Name:			Job Title:		
E-mail:			Telephone:		
Business Address:			City:		
State/Province:		Country:		Postal Code:	
URL:					

Details of Qualified Installation	
Address of impacted customer location(s)	Services performed under Qualified Installation

QIR Acknowledgement of Implementation Statement			
By accepting this Implementation Statement, *QIR Professional Name* acknowledges the following:			
☐	The QIR Professional performed this Qualified Installation in accordance with the requirements defined in the *QIR Qualification Requirements, QIR Program Guide,* and *QIR Implementation Instructions*.		
☐	All information within this Implementation Statement represents the results of the Qualified Installation fairly and accurately in all material respects.		
☐	The QIR Professional has advised *Customer Company Name* of any potential security risks observed, or other relevant observations identified during the Qualified installation, as documented in Part 3 of this Implementation Statement.		
QIR Professional Signature:			
QIR Professional Name:	QIR Professional Name	*Date:*	

Customer Acknowledgement of Implementation Statement			
Based on this Implementation Statement, *Customer Company Name* acknowledges the following:			
☐	The *QIR Implementation Statement* is an accurate record of the work completed by the QIR Professional.		
☐	The Customer Company has read and understands the potential security risks identified in Part 3 of the *QIR Implementation Statement*.		
☐	The Customer Company understands they are responsible for maintaining their PCI DSS compliance and that that any changes to their systems or environment should be made in accordance with PCI DSS Requirements.		
Customer Contact Signature:			
Customer Contact Name:		*Date:*	

Part 2: Implementation Statement Details

Part 2a: Critical Controls

This part is applicable to all Qualified Installations.

Remote Access		
1.	Is the customer aware that any remote access into their network must be configured as follows:	
	• Remote access to the payment application requires multi-factor authentication?	Choose an item.
	• Remote access must be activated only when needed, monitored when in use, and immediately deactivated after use?	Choose an item.
	• Remote access must be implemented securely?	Choose an item.
2.	Will any QIR personnel access the customer site remotely or configure remote access on behalf of the customer?	
☐	**Yes.** QIR personnel are using and/or configuring remote access to the customer site:	
	• Is remote access implemented to require multi-factor authentication?	Choose an item.
	• Does the customer have a process to ensure that remote access to the customer network is activated only when needed, is monitored while in use, and is immediately deactivated after use?	Choose an item.
	• Is remote access to the customer network implemented securely?	Choose an item.
☐	**No.** The QIR will not access the customer site remotely and will not configure remote access on behalf of the customer.	

Accounts and Passwords		
3.	Have all passwords been changed for all payment application default accounts, and have unnecessary default accounts been removed or disabled (including all user and administrative accounts used by operating systems, software that provides security services, application and system accounts, POS terminals, etc. installed by the QIR Company)?	Choose an item.
4.	Is strong authentication and multi-factor authentication configured for all payment application administrative accounts and strong authentication configured for all application accounts with access to cardholder data?	Choose an item.
5.	Is the customer aware that all access to systems containing cardholder data (such as PCs, servers, and databases) should use unique user IDs and strong authentication?	Choose an item.
6.	Is the customer aware that, for all accounts used by operating systems (such as security software, application systems, POS terminals): a. All vendor-supplied defaults should be changed, and b. All unnecessary default accounts should be removed or disabled?	Choose an item.
7.	Are all QIR personnel using unique accounts and passwords for each customer location?	Choose an item.
8.	Is the customer aware of all accounts set up by or used for QIR personnel access, and have instructions been provided on how to change the passwords and disable or remove those accounts?	Choose an item.

Patching	
9. Have the latest vendor-supplied security patches and updates been applied to all software installed by the QIR Employee, including the payment application?	Choose an item.
10. Is the customer aware that vendor-supplied security patches and updates must be applied to the payment application and any underlying software or systems?	Choose an item.

Part 2b: PA-DSS Validated Payment Applications

This part is applicable only to PA-DSS Validated Payment Application installations.

PA-DSS Validated Payment Application and Implementation Guide Used	
If a PA-DSS Validated Application was installed the following information should be provided:	
PCI SSC Listing Number:	
Payment Application Vendor:	
Payment Application Name:	
Application Version Number:	
The validated payment application was installed in accordance with the ***PA-DSS Implementation Guide.*** *(Yes/No)* *If "No," please provide a brief explanation:*	Choose an item.
Date and version of the *PA-DSS Implementation Guide* used during the installation of the payment application:	

Part 3: QIR Professional Additional Observations

The QIR Professional must use this section to:

- Explain all items identified in Part 2 as *"No – Details provided in Part 3";* and
- Document any observations or details they feel the customer should be aware of, including any potential security risks the QIR Professional is aware of in the customer environment.

Note: *Observations included in this section in no way imply that an assessment of PCI DSS compliance has been completed.*

Observation #	Observation Details	Applicable Subject and Question Number from Part 2	Potential security risks?		PCI DSS Reference (if applicable)
			Yes	No	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	