Personify-Client Shared PCI DSS Responsibility – ThreeSixty

Version: 2.0

December 2024

Personify

Table of Contents

Purpose and Overview 2

Requirements of Payment Card Industry Data Security Standard 2

Table 1 - PCI DSS Requirements 2

Payment Card Industry Data Security Standard, v4.0.1 – Requirement Details 3

1. Install and Maintain Network Security Controls. 3
2. Apply Secure Configurations to All System Components. 3
3. Protect Stored Account Data. 3
4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks. 3
5. Protect All Systems and Networks from Malicious Software. 3
6. Develop and Maintain Secure Systems and Software. 3
7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 3
8. Identify Users and Authenticate Access to System Components. 4
9. Restrict Physical Access to Cardholder Data. 4
10. Log and Monitor All Access to System Components and Cardholder Data. 4
11. Test Security of Systems and Networks Regularly. 4
12. Support Information Security with Organizational Policies and Programs. 4

Appendix A: Additional PCI DSS Requirements. 4

Appendix A1: Additional Requirements for Shared Hosting Providers. 4

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections. 4

Appendix A3: Designated Entities Supplemental Validation. 4

Purpose and Overview

Maintaining Payment Card Industry Data Security Standards (PCI DSS) is a shared responsibility between Personify and our Clients. The purpose of this document is to delineate responsibilities belonging to Personify from those belonging our Clients and provide Clients a brief summary of how Personify meets the requirements we are responsible for.

Requirements of Payment Card Industry Data Security Standard

The table below indicates the requirements set forth by the PCI Council in the Payment Card Industry Data Security Standards, v4.0.1 and which organization (Personify, Client, or both) is responsible for each.

Table 1 - PCI DSS Requirements

PCI DSS v4.0.1 Requirement	Personify	Client
1. Install and Maintain Network Security Controls.	✓	
2. Apply Secure Configurations to All System Components.	✓	✓
3. Protect Stored Account Data.	—	✓
4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	✓	✓
5. Protect All Systems and Networks from Malicious Software.	✓	
6. Develop and Maintain Secure Systems and Software.	✓	✓
7. Restrict Access to System Components and Cardholder Data by Business Need to Know.	✓	
8. Identify Users and Authenticate Access to System Components.	✓	
9. Restrict Physical Access to Cardholder Data.	✓	✓
10. Log and Monitor All Access to System Components and Cardholder Data.	✓	
11. Test Security of Systems and Networks Regularly.	✓	
12. Support Information Security with Organizational Policies and Programs.	✓	
A1. Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers.	—	
A2. Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections.	—	✓
A3. Appendix A3: Designated Entities Supplemental Validation (DESV)	—	—

Payment Card Industry Data Security Standard, v4.0.1 – Requirement Details

1. Install and Maintain Network Security Controls.

Servers hosted in Personify's private cloud and public cloud environment(s) are maintained by Personify. The network supporting these servers is also maintained by Personify. These separate network environments have stateful firewalls at Internet border ingress/egress and utilize micro segmentation, also known as Distributed Firewall, technologies to control connectivity inside the network and restrict access in and out of the Cardholder Data Environment.

2. Apply Secure Configurations to All System Components.

Personify follows this guidance when deploying systems and applications. Personify is responsible for account security and passwords on devices and applications owned and operated by Personify. The ThreeSixty application is installed and configured by Personify as a service for Customers. Clients are able to access and manage default accounts, namely the 'Admin' account, within the ThreeSixty application and have the responsibility of creating and maintaining any related passwords for those accounts. Other applications developed by Clients, or third-party vendors contracted by Clients, and deployed to Personify hosted servers will be the responsibility of the Client.

3. Protect Stored Account Data.

The ThreeSixty application is not designed to store cardholder data as defined by the PCI council. Other applications developed by Clients or third-party vendors contracted by Clients and deployed to Personify hosted servers will be the responsibility of the Client. Client is responsible for security of cardholder data at the end user workstation.

4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.

Personify is responsible for configuring servers and websites to use secure encryption technologies. Personify is responsible for configuring the ThreeSixty application to use secure encryption technologies. Where requested and agreed, Personify may offer advice or assistance to Clients with Client, or third party vendors contracted by Clients, developed applications deployed to Personify hosted servers.

5. Protect All Systems and Networks from Malicious Software.

Personify is responsible for maintaining and updating anti-virus and/or antimalware on the hosted servers, performing regular antimalware scanning, receiving, and responding to alerts, and resolving incidents.

6. Develop and Maintain Secure Systems and Software.

Personify is responsible for secure development and deployment of the ThreeSixty application and any enhancements or customizations developed by Personify for a Client. Clients are responsible for secure development of Client, or third party vendors contracted by Clients, developed applications deployed to Personify hosted servers. Where requested and agreed, Personify may offer advice or assistance to Clients with Client, or third party vendors contracted by Clients, developed applications deployed to Personify hosting servers. If a Client has been granted server access to perform deployments, the Client is responsible for change management procedures regarding their deployments.

7. Restrict Access to System Components and Cardholder Data by Business Need to Know.

Personify is responsible for controlling access to all servers hosted within the Personify cloud environments including those in the Cardholder Data Environment, the authorization of access requests and granting an appropriate level of access based on level of need.

8. Identify Users and Authenticate Access to System Components.

Personify is responsible for identification and authentication procedures and protocols for servers hosted within the Personify cloud environments.

9. Restrict Physical Access to Cardholder Data.

Personify is responsible for ensuring protection of physical access to Cardholder Data Environment network servers. This responsibility is formally delegated to our hosting facility providers. Personify is responsible for monitoring PCI compliance of hosting providers and documenting that they acknowledge that they are providing coverage for PCI DSS Requirement 9. Wherever Client takes in-person card payments from their constituents, Client is responsible for ensuring secure handling of cardholder data.

10. Log and Monitor All Access to System Components and Cardholder Data.

Personify is responsible for logging and monitoring usage of the Cardholder Data Environment network and servers. Personify is responsible for alert monitoring, log review, and incident response to log events.

11. Test Security of Systems and Networks Regularly.

Personify is responsible for regular system and process testing. This includes penetration testing, vulnerability scans, and segmentation verification. Personify contracts with a PCI Council Approved Scanning Vendor to perform regular network scans and, when necessary, works with Clients to remediate scan issues. Personify regularly performs additional tests such as incident response testing. Personify monitors network activity and file changes in the Cardholder Data Environment.

12. Support Information Security with Organizational Policies and Programs.

Personify maintains an internal Policies and Procedures document guiding our implementation of PCI DSS requirements and addresses information security for all personnel granted access to the Cardholder Data Environment network and servers.

Appendix A: Additional PCI DSS Requirements.

Appendix A1: Additional Requirements for Shared Hosting Providers.

Not Applicable to Personify. Personify is not a shared hosting provider. Personify's ThreeSixty Web Client application is hosted in a shared-server environment. Personify is responsible for ensuring that each entity can access only their own data, that audit trails are unique to each entity in the shared environment, and that processes and documentation enable timely investigations when needed.

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections.

Not Applicable to Personify. Personify does not use any POS/POI devices with SSL and/or early TLS. If a Client, or a third-party vendor contracted by the Client, takes in-person card payments using a POS/POI device with SSL and/or early TLS, the Client shall be responsible for meeting all requirements under Appendix A2 and the associated security of cardholder data.

Appendix A3: Designated Entities Supplemental Validation.

Not Applicable to Personify. Personify is not a 'Designated Entity' by any payment brand(s) or acquirer.