PCI Compliance Information

Document Overview

The purpose of this document is to ensure that customers and prospective customers of the Donation Station by GWD are fully informed about PCI Compliance and how it affects them as an organisation that accepts card payments.

Your responsibilities as a merchant

In order to use the Donation Station your organisation needs to apply for an account with one of GWD's selected payment providers. Having this account and accepting card donations means that you are a merchant. **As a merchant, you are required by the card schemes (VISA, Mastercard and others) to adhere to the Payment Card Industry Data Security Standards (PCI DSS).**

The need to be PCI compliant applies to all merchants, no matter what payment solution or acquirer you use, however it is down to the acquirer to decide how this should be monitored or enforced, there is variation between each acquirer.

GWD's current acquirer is AIB and this guide focuses on helping Donation Station customers understand what AIB expects of them and how to comply with their rules.

Annual declaration & assessment

AIB provide merchants with a tool to help them ensure they are compliance with PCI DSS.

As an AIB merchant you will receive an email from the AIB Merchant Services PCI DSS programme giving you access to the portal that they have set up to help merchants adhere to the requirements.

This process can however be confusing, so GWD has prepared prepopulated documentation and a step-by-step guide to complete your annual return for AIB.

AIB will send email reminders to the person listed as the data security contact on your merchant account. If you fail to complete the annual return AIB will start charging you a £25 per month non-compliance fee in accordance with their Terms & Conditions.

Costs

AIB may charge merchants £3.90 per month to be part of their PCI DSS programme. This charge will appear on your monthly invoice from AIB. If you find this to be the case, then GWD will pay this fee for you and you can therefore claim a rebate via your quarterly GWD invoice. To do this please send a copy of your AIB invoice to accounts@gwd.team and they will provide a rebate on your next quarterly invoice.

Is the card data secure?

The scope for breach of card data connected to ownership or use of the Donation Station is extremely limited.

By far the most common cause of a card data security breach is if merchants write down card numbers and store them in some way. This is both unnecessary and bad practice. With the Donation Station, the cardholder data is instantly encrypted as soon as the card touches the card reader, and it then starts its journey through the gateways and banks in order to be authorised. Neither you as a merchant, nor GWD as a solution provider have any opportunity to access the cardholder data and even if we did, it is protected by four layers of highly secure encryption.

Given the relatively low volume of donation transactions compared to retail transactions the risk of a hacker targeting your Donation Station for its cardholder data is low. However should a hacker wish to target this and succeed in breaking into your network they too would only have access to encrypted data.

In order to ensure the solution is as secure as it can possibly be, we only work with payment vendors who can provide us evidence of compliance with the relevant PCI standards.

All Donation Stations will therefore be boarded to a gateway offered by one of the following providers. They are both registered providers with the PCI Standards Council: https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions?agree=true

- NMI Creditcall payment gateway (Search "Network Merchants" as the company)
- Kinetic Smart Solutions

A copy of their Attestation of Compliance is available upon request.

PCI Housekeeping

Whilst the solution is designed to protect cardholder data without the need for merchants to also do so, there are a few things you should consider:

1. *Secured network*. Don't used your Donation Station on a network that untrusted people can also use (e.g. guest WiFi).
2. *Device tampering*. If you see evidence of someone having broken into the enclosure, contact GWD for advice.

3. *Device inspection*. If you have a Chip & PIN variant (where the card reader is exposed), periodically inspect your Donation Station for signs of tampering: unusual wires, something inserted into the reader or ports, card reader securely in place.

Semi-attended usage

Different card readers are designed for different purposes. Some are designed to be used by a retailer face-to-face (attended) and some are designed to be used in a location where staff are never present (unattended). The solution we provide is rated as semi-attended, which means that it is suitable for using in locations where staff are often present, but with periods of absence when the device is still available for use. Based on the advice we have received from our payment supply chain, we have determined that Donation Station customers we sell to fall within the semi-attended category. If you have any questions or concerns about this, please email support@gwd.team to discuss further.

The term "periods of absence" is vague, but as an example, if you are a church and you open the doors on a daily basis, but don't always necessarily have someone in the building at all times we would still consider this device to be suitable and our payment partners agree.

Disclaimer

Any information provided by GWD to assist you with your PCI DSS compliance (including in this document) does not constitute formal advice and GWD does not accept any liability relating to your obligations as a merchant to comply with PCI DSS. The information and assistance provided is intended to help signpost you to what you need to know, however if you are unsure you should seek advice from a qualified security assessor (QSA) who will be able to offer further assistance.