

# Cardholder Data Policy Statement

Reference: PCI POL 4.1

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 29/06/2020

Organisation Issue Date:

## 1. Scope

"If your organisation stores, processes, or transmits cardholder data in any way use the following scope: This policy applies to all cardholder data of any description that Organisation Name is responsible for, receives or processes; or that can affect the security of the storage, processing or transmission of the cardholder data.

If your organisation doesn't store, process, or transmit cardholder data use the following scope: Organisation Name does not in the course of normal operations store, transmit, or handle cardholder data in any form. This policy applies should Organisation Name for any reason become responsible for any cardholder data."

## 2. Responsibilities

2.1 All Employees/Staff involved in receiving, processing, storing or in any way using cardholder data are responsible for ensuring that these policy requirements are met.

## 3. Requirements

3.1 The PCI DSS must be followed in all respects.

3.2 All appropriate steps (as mandated by the PCI DSS) will be taken to protect cardholder data, whether in storage or in transmission.

3.3 Access to cardholder data is restricted on a need-to-know basis.

3.4 Physical access to cardholder data is restricted.

3.5 Cardholder data must be securely disposed of when no longer needed as per data retention standards.

3.6 The full contents of any track (track 1 or track 2) from the magnetic stripe (on the back of the card, in a chip, etc.) must not be stored.

3.7 The card-validation code (CVV) or value must not be stored.

3.8 The personal identification number (PIN) or the PIN block from the smart chip must not be stored.

3.9 Mask PAN when displayed (the first six or last four digits are the maximum number of digits to be displayed).

3.10 The PAN must be rendered unreadable anywhere it is stored, using strong cryptography, truncation, strong one-way hash functions, or index tokens and pads. If the cardholder name, service code or expiration date is stored in conjunction with the PAN, these data elements must be protected.

<< 3.11 – 3.16 removed for sample purposes >>

### ***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).