

PCI DSS Charter

Reference: PCI POL 0.1

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 29/06/2020

Organisation Issue Date:

1. Preamble

The Board of Directors and management of Organisation Name, located at

Address line 1

Address line 2

City

County

Country

Postcode

which

"operates in sector z, is in the business of y"

are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to comply with the Payment Card Industry Data Security Standard (PCI DSS). Information and information security requirements (specifically those within the PCI DSS) will continue to be aligned with Organisation Name's goals and the [PCI DSS compliance programme](#). This programme is intended to enable continued compliance and for reducing information-related risks to acceptable levels.

Organisation Name's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks, including those related to cardholder data, "through the establishment and maintenance of an ISMS."

The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled.

2. Definitions

Preserving

This means that management, all full time or part time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts and within the [PCI DSS Roles and Responsibilities](#) document) to preserve information security; to protect cardholder data; to report security breaches

"and to act in accordance with the requirements of the ISMS."

All Employees/Staff will receive information security awareness training and more specialised Employees/Staff will receive appropriately specialised information security training that will encompass all duties relating to the protection of cardholder data.

Confidentiality

This involves ensuring that information, including cardholder data is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to Organisation Name's information

"and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and e-commerce systems."

Integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental; partial or complete; destruction or unauthorised modification of either physical assets or electronic data, other than as required in documented procedures for the protection of individual information or cardholder data.

Availability

This means that information and associated assets should be accessible to authorised Users when required and therefore physically secure. The computer network must be resilient and Organisation Name must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten cardholder data or the continued availability of assets, systems and information.

ISMS

This is the information security management system, of which this policy and other supporting and related documentation is a part, and which has been designed in accordance with the requirements of PCI DSS v3.2.1."

3. Stakeholders

Each element of the PCI DSS compliance programme at Organisation Name should make reference to key stakeholders. For a complete list of stakeholders and their level of involvement in any given process, refer to the [PCI Roles and Responsibilities Matrix](#).

4. Scope of PCI DSS compliance

< < Removed for sample purposes > >

5. Objectives of the PCI DSS compliance programme

The key objectives of the PCI DSS compliance programme in Organisation Name are:

- a. To define activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities.
- b. To understand the limits of the scope that the PCI DSS affects.
- c. Completion of annual PCI DSS assessments.
- d. To ensure continuous validation of PCI DSS requirements.
- e. To determine the potential impact of strategic business decisions on PCI DSS compliance.

6. Accountability for PCI DSS compliance

< < Removed for sample purposes > >

7. Business-as-usual activities

Organisation Name has established a PCI DSS compliance programme. As part of this programme, GRCI International Preview performs quarterly reviews to confirm that, at a minimum, the following essential procedures are being performed:

1. Daily log reviews (Requirement 10.6.1)
2. Firewall rule-set reviews (Requirement 1.1.7)
3. Applying configuration standards to new systems (Requirements 2.2, 6.4.6)
4. Responding to security alerts (Requirements 11.1.2, 11.5.1, 12.10.5)
5. Change Management processes (Requirements 1.1.1, 6.4.5)

The

"Enter role"

shall report the results of the quarterly review to the

"Enter role"

along with any other relevant reports or results of the PCI DSS compliance programme and maintain the documentation of these reports and results.

< < Removed for sample purposes > >

8. Communication

< < Removed for sample purposes > >

9. Risk management

"Risks will be managed according to best practice. This will involve the identification of likely risks, planning to avoid them and planning to mitigate any damage should they arise. Unforeseen risks will be responded to in a timely fashion, with all mitigation documented and assessed."

Document Owner and Approval

The Board of Directors 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](#).