DNA PAYMENTS

DNA Payments Limited PCI DSS Charter

Introduction

The Senior Management of DNA Payments Limited, located at 123 Buckingham Palace Road, London, England, SW1W 9SH are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation in order to comply with the PCI DSS. Information and information security requirements (specifically those within the PCI DSS) will continue to be aligned with DNA Payments Limited'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.

DNA Payments Limited'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.

Definitions:

1/ Preserving

This means that management, all full time or part time 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 staff will receive information security awareness training and more specialised staff will receive appropriately specialised information security training.

2/ 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 DNA Payments Limited 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.

3/ 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 DNA Payments Limited information and proprietary knowledge and its systems including its network(s), website(s), and e-commerce systems.

4/ 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.

5/ The 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 current requirements of PCI DSS.

Stakeholders

Each element of the PCI DSS compliance programme at DNA Payments Limited 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.

Scope of PCI DSS Compliance

Compliance with PCI DSS is mandatory for ALL merchants who accept card payments. The Senior Management shall assign responsibility for the protection of cardholder data and a PCI DSS compliance program which shall also determine the scope of compliance within DNA Payments Limited.

Objectives of the PCI DSS Compliance Programme

The key objectives of the PCI DSS Compliance programme in DNA Payments Limited's are:

1/ To define activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities

2/ Completion of annual PCI DSS assessments

3/ To ensure continuous validation of PCI DSS requirements

4/ To determine the potential impact of strategic business decisions on PCI DSS compliance

Accountability for PCI DSS Compliance

Each aspect of the PCI DSS compliance programme, and each implementation objective has accountability assigned.

Communication

Senior Management shall meet at least once a year to discuss the state of PCI DSS compliance within DNA Payments Limited and review the PCI DSS Compliance Programme to ensure its continued effectiveness. Any person with assigned responsibilities within the PCI DSS

Compliance Programme must communicate with Senior Management regarding the status of it at least annually.

Risk Management

Risks will be managed according to best practice[1]. 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 Chief Executive Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed.

A current version of this document is available to all members of staff on the company's internal intranet site. It does not contain confidential information and can be released to relevant external parties.

This charter was approved by the Chief Executive Officer and is issued on a version-controlled basis under his signature.

Signature: Date: 05 November 2019

[1] Best practice risk management frameworks might draw, for instance, on ISO31000, ISO27005 and/or COSO.