# PCIDSS Compliance Guidelines

Version 1.2

17th May 2018

Author: Scott Mackerras

# Table of contents

# PCIDSS Requirements

The following expressions shall have the following meanings:

“Account Data” means “Cardholder Data” and “Sensitive Authentication Data”

“Agreement” means your dealer or distributor agreement with EE/BT.

“Cardholder Data” means the primary account number (‘PAN’) together with any or all of the following items which may be retained with the PAN: “cardholder name”, “service code” and “expiration date” (as those terms are commonly understood in the payment card industry).

“Cardholder Data Environment” means any part of your network or business operations that stores, Processes or transmits the Account Data or can impact the security of that network or business operations.

“Payment Card” means any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.

“Payment Card Industry Approved Scanning Vendor” (PCI ASV) means an organisation which has been approved and added to the Payment Card Industry Security Standards Council list of approved scanning vendors.

“Payment Card Industry Internal Security Assessor” (PCI ISA) means an individual who has successfully been certified by the PCI Security Standards Council as a PCI ISA

“Payment Card Industry Qualified Security Assessor” (PCI QSA) means an individual who has successfully been certified by the PCI Security Standards Council as a PCI QSA and is an employee of a Qualified Security Assessor Company (QSAC).

“PCIDSS” means the Payment Card Industry Data Security Standards issued and amended by the PCI Security Standards Council (‘the Council’) from time to time and set out at https://www.pcisecuritystandards.org.

“PCI SSC” means the Payment Card Industry Security Standards Council

“Processing” means any processing, collection, transmission, managing or storing by any means and in any type of media including paper, or voice recording, or digital images in which Account Data is held, and payment card receipts on which the full PAN is printed. “Processes” shall be construed accordingly.

“Relevant Work” means those elements of the services which include the Processing of EE or BT Customers’ Account Data forming the Data Environment controlled by you.

“Sensitive Authentication Data” means full track data (magnetic-stripe data or equivalent on a chip) and/or “CAV2/CVC2/CV2/CID” and/or “PIN/PIN Block” (as those terms are commonly understood in the payment card industry).

# PCIDSS Compliance:

1. You agree that you comply and shall continuously comply with all requirements of the current version of Payment Card Industry Data Security Standard (PCI DSS) and you will demonstrate your compliance with the PCI DSS by:

   (a) Submitting annually a current and valid Attestation of Compliance (SAQ D as a Service Provider) validated by a certified PCI Qualified Security Assessor (QSA), PCI Internal Security Assessor (ISA) or Senior Company Representative to complaint.review.legal.support@bt.com

   (b) Submitting a passing external network vulnerability scan at the request of BT/EE on a six-monthly basis as performed by a PCI SSC Approved scanning vendor (where applicable) to complaint.review.legal.support@bt.com ; and;

   (c) Submitting annually a current and valid statement about which PCIDSS requirements are managed by them.

2. You must ensure that all PCI DSS assessments are completed accurately and evidences are retained for audit verification and be readily available for review if requested by EE/ BT.

3. Any breach of this policy by you shall be deemed to be a material breach of the Agreement and you shall indemnify EE and BT from and against any costs, losses, damages, proceedings, claims, expenses or demands incurred or suffered by EE and/or BT which arise as a result of such breach.

# Account Data Handling:

1. You shall be responsible for the security of all Account Data in your possession in keeping with the requirements of PCI DSS and for all actions involved in Storing, Processing or Transmitting Account Data.

2. without limitation to the above paragraph:

a) Payment card information MUST not be written down or stored unless otherwise agreed with EE/BT.

b) Unprotected payment card data MUST not be sent via end-user messaging technologies, such as e-mail and instant messaging to EE departments or internally.

c) Storage of sensitive authentication data, such as CV2, PAN, etc. even if encrypted is not permitted beyond the completion of the transaction. Whilst transactions are pending completion, either through automated systems or over the telephone Partners must ensure:

- Strong cryptography to comply with PCIDSS is used to protect data
- If the encrypted cardholder data is being written to disk, that it is being securely deleted once the transaction has completed

d) During distance Sales Calls, if you utilise Credit/Debit card information for identity proof, then call recordings must be paused when card information is disclosed. Where call recordings are not paused and resumed using automated technology to prevent the capturing of PAN and CV2 information (which is supported by quality checks to detect and deal with any accidental capturing of card data), call recordings MUST be encrypted using strong cryptography

(e) Middle eight digits of the card and CV2 MUST be masked when copying Debit/ Credit Cards/ Statement as proof of identification, (see the PCI DSS copy cards 'what to do' document for more information)

3. You shall ensure that the Relevant Work conforms to all requirements of the PCI DSS and such later versions, guidance and/or advice of the PCI DSS which the Council may issue from time to time.

# Sub-Contractors (Including Stockists and Franchisees):

1. You agree that all Relevant Work will be performed by you and any PCI DSS in scope work shall not be subcontracted to any third party without EE/BT's prior written consent.

2. In the event that you use a sub-contractor (including without limitation any Stockist or Franchisee) for any Relevant Work, you agree:

2.1 You shall ensure that each sub-contractor enters into a contract which incorporates all terms which we are imposing on you; and

2.1.1 You shall ensure that each sub-contractor's PCIDSS compliance is demonstrated in accordance with the below:

2.1.2 Stockists or Franchisees are required to complete an SAQ C-VT as a service provider where they have either accepted Credit/ Debit Cards as proof of identification or there is any likelihood of Credit/ Debit Card information being taken for the purposes of proof of identification

2.1.3 All completed assessments must be signed off by the Franchise Owner/ Stockist Principal.

# PCI DSS Incident Reporting:

1. You shall notify EE/BT promptly (but in any event, no later than 12 hours) after becoming aware of any non-compliance with these requirements of PCIDSS or receiving any allegation of non-compliance with PCIDSS and inform EE/BT of the steps you are taking to remedy such non- compliance.

2. In particular, you shall:

2.1.1 Report all PCIDSS security incidents to: The Duty Controller: BT Security Incident Management (24x7) Tel No: 0800 321 999 / +44 1908 641100: Email: security@bt.com ; and

2.1.2 Report all non-compliance to the Head of BT Group PCIDSS Compliance by Email to complaint.review.legal.support@bt.com.

# Right to Audit:

1. The Service Provider shall allow (and ensure that all relevant Service Provider Personnel allow) BT or its authorised representatives such access via supplier personnel to premises, records and provide access to screen image(s) of controls for systems containing any relevant Information as is reasonably necessary to assess the Service Provider's compliance with this clause.

# Secure Data Deletion:

1. Within 30 days of termination, cancellation, expiration, or other conclusion of the Agreement, You shall:

1.1 Return to EE/BT any copies of any and all PCI DSS information relating to the Cardholder Data Environment that is in your possession; or

1.2 if return is not feasible, securely destroy and not retain any such PCI DSS information and provide EE/BT with an appropriate Certificate of Destruction of such PCI DSS information.

# Support and Advice:

1. The EE Indirect Compliance Team are unable to advise as to which sections of the assessments are required to be completed and where required, Partner/ Stockist Management should seek third party support to ensure accurate and relevant completion of assessments

2. More information can be found at: https://www.pcisecuritystandards.org/security_standards/index.php.