BT Supplier PCI DSS Security Policy

(PAYMENT CARD DATA SECURITY STANDARDS)

Owned by BT PCI Governance and Assurance Team
Volume No 5.0

Date 9th November 2021

Information Classification: Public

Contents

1 Scope

This Policy applies to all Suppliers (as defined in this Policy) doing business with BT or acting on our behalf.

Any queries or concerns regarding PCI DSS within BT can be emailed to group.pci.compliance@bt.com .

1.1 Version Control

Version No.	Updated by	Published	Summary of Update
3.0	Ronan Miles	21/04/2020	3rd edition – General revisions in line with PCI DSS
4.0	Ronan Miles	09/10/2020	To reflect changes to VISA Agents program and to support enhancements to BT process.
5.0	David Mayberry	09/11/2021	General revisions to improve language

2 Supplier Requirements

2.1 The Supplier (whether directly involved in Processing Account Data on behalf of a Merchant, or providing services that control or could adversely impact the security of Account Data) represents, warrants, and undertakes that:

2.1.1 it has complied with and will continuously comply with all PCI DSS requirements unless otherwise agreed using the Responsibility Matrix at paragraph 2.1.1.3 below, and it will validate its compliance with PCI DSS:

2.1.1.1 by submitting to group.pci.compliance@bt.com at start of contract and no later than annually thereafter, an Attestation of Compliance (AoC) that is current, adequately describes the service(s) provided to BT and is validated by a certified Payment Card Industry Qualified Security Assessor from an independent Qualified Security Assessor Company or by an Internal Security Assessor (ISA); and

2.1.1.2 upon request submitting a passing external network vulnerability scan (for example, a front sheet or executive summary) of all internet facing IP addresses that relate to the services provided on behalf of BT as performed by a Payment Card Industry Approved Scanning Vendor to group.pci.compliance@bt.com using a pre-agreed secure format, e.g., an agreed password for password protection; and

2.1.1.3 by submitting at the start of the contract and annually thereafter a current Responsibility Matrix agreed between the parties, confirming the apportionment of responsibility for all applicable PCI DSS requirements, and confirming specifically those managed directly by the supplier; and,

2.1.2 the Supplier represents/warrants/undertakes that BT may declare the name of the Supplier as required as part of any compliance programmes mandated by the Payment Card Brands and / or other pertinent organisations.

2.2 The Supplier will permit BT upon reasonable notice to perform additional Security Risk Assessments (SRA), either onsite or remotely – typically via a 3rd-Party entity contracted by BT for that purpose.

2.2.1 In the event of the loss of card data which requires BT to undergo an independent Forensic Investigation, the Supplier will cooperate with BT as is required to support that Forensics Investigation and will do so in a timely manner to enable BT to discharge its obligations to the body requiring the Forensic Investigation.

2.3 The Supplier agrees that all Relevant Work will be performed by the Supplier and any PCI DSS in scope work will not be subcontracted to any third party without BT's prior written consent. Where such work is subcontracted the Supplier will ensure that:

2.3.1 the Subcontractor enters a contract on terms which provide that the Subcontractor has the same obligations as the Supplier as set out in this Policy; and

2.3.2 PCI DSS compliance of the Subcontractor(s) can be demonstrated by inclusion in the Supplier's Attestation of Compliance.

2.3.3 the Supplier will confirm the list of Subcontractors at the same time as submitting the Attestation of Compliance as per 2.1.1.1

2.4 The Supplier is responsible for the security of all Account Data in its possession in keeping with all the requirements of the PCI DSS and, for all actions involved in Processing the Account Data.

2.5 The Supplier will 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 PSI SSC may issue from time to time.

2.6 The Supplier will notify BT without undue delay, (but in any event, no later than 12 hours) after becoming aware of any non-compliance with this Policy or PCI DSS or receiving an allegation of non-compliance with this Policy or PCI DSS and inform BT of the steps it is taking to remedy such noncompliance. In particular, the Supplier will:

2.6.1 Report all PCI DSS security incidents to: BT Security Incident Management Team (24x7) Tel No: 0800 321 999 / +44 1908 641100: Email: security@bt.com ; and

2.5.2. Report all non-compliance to the BT Head of PCI DSS Compliance by email to group.pci.compliance@bt.com

2.7 Any breach of this Policy by the Supplier will be deemed to be a material breach of their contract with BT and the Supplier will indemnify, defend, and hold harmless BT from and against any costs, losses, damages, proceedings, claims, expenses or demands incurred or suffered by BT which arise as a result of such breach.

2.8 The Supplier will allow (and ensure that all relevant Supplier Personnel allow) BT or its authorised representatives such access to premises, systems and records containing any relevant Information as is reasonably necessary to assess the Supplier's compliance with this clause.

2.9 The Supplier will take all reasonable steps to ensure the reliability of any of the Supplier Personnel who are involved in the Relevant Work; that only those Supplier Personnel who need to have access to the Relevant Work are granted access to it; that such access is granted only for the purpose of the proper performance of their contract; and that the Supplier Personnel are informed of the confidential nature of the Relevant Work and comply with the obligations set out in this Policy

2.10 Within 30 days of termination, cancellation, expiration, or another conclusion of their contract with BT, the Supplier will:

2.10.1 return to BT any copies of any and all Account Data relating to the Cardholder Data Environment that is in its possession, and will use reasonable endeavours to procure the return of any such Account Data that is in the Subcontractors' possession; or

2.10.2 if return is not feasible, securely destroy and not retain any such Account Data, use reasonable endeavours to procure the secure destruction and non-retention of any such Account Data that is in the Subcontractors' possession, and provide BT with an appropriate certificate of destruction of such Account Data.

2.10.3 Account Data may be retained where there is a legitimate interest in accordance with the retention policies as agreed with BT. Supplier must provide a list of the Account Data types being retained along with a rationale for agreement with BT within 30 days of termination.

2.11 The terms of this Policy will survive termination or expiry of any contract between the Supplier and BT.

3 Definitions

3.1 The following expressions used in this Policy will have the meanings set out below:

"**Account Data**" means both "Cardholder Data" and "Sensitive Authentication Data".

"**Affiliate**" means any company, partnership, or other entity which from time to time BT:

a) owns (directly or indirectly) at least twenty (20) per cent of the voting stock of another entity

b) has the power (directly or indirectly) to appoint the majority of the board of directors or power (directly or indirectly) to control the general management of another entity; or

c) both BT and the Supplier agree in writing may be considered as under control of that party for the purposes of this Policy.

"**BT**" means British Telecommunications plc and its Affiliates from time to time.

"**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" coupled with any other elements as defined by the PCI SSC from time to time (as those terms are commonly understood in the payment card industry).

"**Cardholder Data Environment**" means any part of the network or business operations of the Supplier that stores, processes, or transmits the Account Data or can impact the security of that network or business operations or any other elements as defined by the PCI SSC from time to time.

"Forensic Investigation" means an organisation qualified by the PCI Security Standards Council's program and must work for a Qualified Security Assessor company that provides a dedicated forensic investigation practice. PCI Forensic Investigators (PFIs) help determine the occurrence of a cardholder data compromise and when and how it may have occurred. They perform investigations within the financial industry using proven investigative methodologies and tools. They also provide relationships with law enforcement to support stakeholders with any resulting criminal investigations.

"Merchant" means any entity that accepts Payment Cards as payment for goods and/or services.

"**Payment Cards**" 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 payment card industry internal security assessor.

"**Payment Card Industry Qualified Security Assessor**" (PCI QSA) means an individual who has successfully been certified by the PCI Security Standards Council as a payment card industry qualified security assessor and is an employee of a Qualified Security Assessor Company (QSAC).

"**PCI DSS**" 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 form of operation performed on Account Data including collection,

transmission, managing or storing by any means via any type of media including and not limited to; paper, voice recording, digital images retained on solid state devices, fixed or removable discs, paper or any other medium, etc. "Processes" will be construed accordingly.

"**Relevant Work**" means those elements of the goods or services which include the formal or

informal Processing of BT customers' Account Data forming the Cardholder Data Environment

controlled by the Supplier.

"**Responsibility Matrix**" means a detailed matrix of PCI DSS requirements, including the description of whether responsibility for each individual control lies with BT, its Supplier or whether responsibility is shared between both parties.

"**Security Risk Assessment**" means a BT defined assessment to review the security practices of the Supplier as pertaining to the current Responsibility Matrix and assess any potential risk to BT.

"**Sensitive Authentication Data**" means full track data (magnetic-stripe data or equivalent on a chip) and/or "CAV2/CVC2/CVV2/CID" and/or "PIN/PIN Block" and/or any other elements as defined by the PCI SSC from time to time (as those terms are commonly understood in the payment card industry).

"**Supplier**" means a business entity directly involved in the processing, storage, or transmission of cardholder data or whose services may impact the security of such whilst acting on behalf of BT. This includes both when BT is the merchant and when the Supplier is the merchant.

"**Supplier Personnel**" means employees and workers engaged by the Supplier in connection with the Relevant Work.

"**Subcontractor**" means a business entity with which the Supplier enters into a contractual

agreement involving the processing, storage, transmission of cardholder data or whose services may affect the security of the cardholder data environment on the Supplier's behalf.