Manx Telecom (MT)

Supplier PCI 12.8 v1.1

High Level Description – Service Provider PCI DSS

CONTROL PAGE

Reference:	**Supplier PCI 12.8 v1.1**
Issued by:	Johnathan Lee
Name:	**Johnathan Lee**
Role:	Group Head of Procurement & Compliance
Approved by:	Liam Bulliment
Name:	As above
Role:	Vendor Manager
Date:	22-08-2022

Document Retention Information	
Review period:	**Six monthly review target – One-year max**
Retention period:	**Current + 1 Year**
Owner while current:	Liam Bulliment
Role:	Vendor Manager
Date when NOT CURRENT	01-08-2023

CHANGE HISTORY

Version	Date	Updated by	Changes
Version Draft	01/08/2022	Johnathan Lee	Draft
Version 1.1a	20/08/2022	Johnathan Lee	Re-approval
Version 1.1b	22/08/2022	Liam Bulliment	1st Draft Approval to Live
Version 1.1c	30/08/2022	Johnathan Lee	Live Final

CONTENTS

1. OVERVIEW

PURPOSE OF THIS DOCUMENT

The purpose of this HLD is to meet the requirements of section 12.8, and the relevant subsections for PCI DSS standards. To achieve this, it will cover in detail the following;

a. 12.8.1: Provide an overall description and list of all service providers and what services they provide to us
   a. PSP – Payment Service Provider
   b. GSP – Gateway Service Provider
   c. CA – Card Acquirer

b. 12.8.2: Provide detailed written agreements on the services provided by 3rd parties and in specific to PCI DSS standards. Whilst also covering off clearly documented information on their commitment to us for the services being provided and adhered to by terms and conditions and any AOC (inbound) to us. Including clear touch points in relation to how they manage card holder information where applicable

c. 12.8.3: a clear process for Vendor Onboarding and due diligence selection

d. 12.8.4: Supplier Performance Reviews. Alongside annual Compliance checks and validation of our AOC status (outbound)

e. 12.8.5: Roles and responsibilities - Workflow

This document:

- provides an analysis and detailed overview at a high level for internal processes relating to PCI DSS standards for Manx Telecom in relation to taking card holder payments via SHOP, ECOM & MOTO

- provides an analysis summary overview at a high level for protocols that external Suppliers/Vendors are required to adhere to whilst providing us services relating to PCI DSS standards and in specific to taking card holder payments via SHOP, ECOM & MOTO

Several supporting guides and or process documents are available on request and or are detailed within.

SCOPE

The scope of this HLD is to list all applicable services and actions in relation to PCI DSS. Including an end to end processes overview PCI DSS standards for 12.8.1, 12.8.2, 12.8.3, 12.8.4 and 12.8.5. For any services relating to taking card payments whether by SHOP, ECOM or MOTO.

HLD MANAGEMENT

This High-Level Description document is to be reviewed on an annual basis - or if there have been significant changes to the PCI DSS standards and in specific to 12.8 that need to be considered and or to be revised.

Suppliers/Vendors are required to attest and confirm to the relevant standards whereby they provide and or support card payment services as enclosed.

These are split into the relevant categories as defined in 12.8.1.

PCI DSS – will be audited and manged via our Compliance Team on a regular basis.

This review will consist of an assessment of the actual measurements currently being undertaken, and the continuing relevance of these measures. Consideration will be given to any current proposals for PCI DSS and or developments which may impact on the document. The document will then be updated accordingly and sent to our Auditors for reference.

The document must be in a form and have content which is acceptable to PCI DSS Auditors prior to the issue of a revised version of the document.

Suppliers & Vendors can also review this document at:

https://www.manxtelecom.com/supplier-terms

Our Supplier Code of Conduct and Supplier GDPR Data Protection Policy is also available at this location.

2. DESCRIPTION OF PCI DSS SERVICES (12.8.1)

SHOP

Manx Telecom offers a range of services, including the ability to pay your bill via the SHOP but in specific for paying for Goods & Services via our retail outlet in Douglas.

Transactions are processed through 3-PED's via:

- PSP – for Inventory Management
- GSP – Gateway service conduit
- Card Acquirer – card transaction settlements

Regular PCI audit tests and checks are performed onsite in-line with Compliance tasks. These are performed monthly

A written process is available for this.

End customers visit the SHOP and a transaction is processed via one of the PED's available in store in a secure manner.

We are implementing (P2PE) via our GSP & Card Acquirer also.

Annual tests of conformity for the services provided to Manx Telecom by the GSP & Card Acquirer via their AOC are required and will be reviewed annually and maybe subject to audit checks as and when required.

ECOM

Manx Telecom offers corporate and business payments to be made via a 3rd party service provider known as a PSP. These link into our GSP and then via our Card Acquirer.

Payments of this nature are typically recurring and are business, corporate in nature and are processed via a secure online ecommerce portal.

Annual tests of conformity for the services provided to Manx Telecom by the PSP, GSP & Card Acquirer via their AOC are required for the GSP and the Card Acquirer and will be reviewed annually and maybe subject to audit checks as and when required. Our PSP will be covered under terms and conditions of a written agreement.

Payments of this nature/type may also be automated for convenience.

Full reconciliation is performed as and when required.

Other transactions maybe processed via the GSP also.

MOTO

Manx Telecom processes payments for MOTO in relation to IVR (Interactive Voice Recognition) platform for end customers. Typically, through our contact centre.

Payments of this nature could be ad-hoc and or recurring in nature.

Payments are processed via a PSP. GSP and a Card Acquirer.

Annual tests of conformity for the services provided to Manx Telecom by the PSP, GSP & Card Acquirer via their AOC are required for the GSP and the Card Acquirer and will be reviewed annually and maybe subject to audit checks as and when required. Our PSP will be covered under terms and conditions of a written agreement.

PSP – PAYMENT SERVICE PROVDIER

Payment Provider

- An intermediary or 3rd party that will assist businesses to accept a wide range of online payments that typically form an interface/conduit at the point of sale process
- This could be via an EPOS (Electronic Point of Sale) and or via web/digital interface enabling part of the initial authorisation process

GSP – GATEWAY SERVICE PROVDIER

Gateway Provider

- An intermediary Service Provider providing gateway services. Typically known as a gateway provider between an PSP and a Card Acquirer to enable support for an E2E (end to end) Service
- A processing gateway is a connection point within the payment journey. A gateway connection your shopping cart, point of sale system or virtual terminate to the next point in the payment authorisation process

CARD ACQURIER

Merchant Provider

- Merchant account services via use of a MID (Merchant Identification Number)
- A settlement provider for a merchant into their receiving bank
- Includes KYC (Know Your Customer)

3. TECHNICAL DELIVERY OF SERVICE

SHOP

For the SHOP based card transactions there is a multi-step process

- Customer visits the SHOP

- PSP performs inventory management control and pricing lookup
- GSP processes transaction technically a PED
- Card Acquirer is utilised to process the transaction via a PED
- Customer leaves the SHOP with their goods and receipt, proof of purchase and terminal receipt
- Finance then reconcile inbound and outbound payments

AOC is available for inbound services to Manx Telecom from the GSP and Card Acquirer. In specific the GSP and the Card Acquirer are the same Service Provider/Supplier

Audit control is available and monitored via Compliance and via a Supplier Management layer.

ECOM

For the ECOM card transactions there is a multi-step process

- Customer utilises a 3rd party secure online interface via a PSP
- Transactions are then processed via a GSP
- Transactions are then processed via a Card Acquirer
- Settlements are then processed and reconciled via Finance
- The Customer will receive a bill clearly showing their charges and what amounts were processed to settle the balance

AOC is available for inbound services to Manx Telecom from the GSP and Card Acquirer. In specific the GSP and the Card Acquirer are the same Service Provider/Supplier

Audit control is available and monitored via Compliance and via a Supplier Management layer.

MOTO

For MOTO card transaction there is a multi-step process for IVR based transactions

- Customers utilises by telephone a 3rd party secure IVR interface via a PSP
- Transactions are then processed via a GSP
- Transactions are then processed via a Card Acquirer
- Settlements are then processed and reconciled via Finance
- The Customer will receive a bill clearly showing their charges and what amounts were processed to settle the balance, or they will have already received a bill via our online portal and or via post

AOC is available for inbound services to Manx Telecom from the GSP and Card Acquirer. In specific the GSP and the Card Acquirer are the same Service Provider/Supplier.

Audit control is available and monitored via Compliance and via a Supplier Management layer.

4. PROCESSES

Written Agreements & Supplier Conformity of Services

Written agreements are in place for each service whether these are via a PSP, GSP and or a Card Acquirer.

Suppliers/Service Providers are required ensure that they adhere and attest to the terms and conditions on an annual basis and they are subject to audit, supplier performance reviews as required and in line with ISO standards

Suppliers my attest and accept our Supplier Code on Conduct which his online at:

https://www.manxtelecom.com/supplier-terms

Supplier Service Provider Engagement & Vendor Onboarding Process

Prior to any applicable Service Providers being onboarded we implement a robust onboarding process:

- Requestee ticket raised in Service Now
- Onboarding forms issued to prospective Supplier for consideration
- Inclusion of key requirements relating to ISO certifications where applicable
- Onboarding process inline with DOA (Delegated Authority Levels)
- Credit Check Performed
- Inclusion of prospective Supplier into our Finance platform
- Banking details validated via headed paper and by checking banking records
- Supplier agrees to Vendor onboarding forms and payments terms (via link)
- Supplier agrees to Supplier Code of Conduct
- Performance reviews are relevant in line with Supplier Tier level and our Supplier Management processes, policies and procedures

In summary the high-level steps are:

- Step 1: Initial Requirement
- Step 2: Procurement Evaluation
- Step 3: Vendor Onboarding Process
- Step 4: Vendor Approved & Vendor Initiation
- Step 5: Supplier Performance Reviews

Supplier Performance Process Overview

Suppliers will be mandated to perform Supplier Performance Reviews inline with our Supplier Code of Conduct and our Supplier Management policies.

These reviews will take base on either a quarterly, half yearly and or annual basis. Depending on Tier Level:

- Tier Red – Critical Supplier or High Risk (up to quarterly reviews)
- Tier Amber – High or Medium Impact Suppliers (up to half yearly reviews)
- Tier Green – Low Impact Suppliers (up to yearly reviews)
- Tier International – Individual assessment within Tier Red, Tier Amber and or Tier Green

Any suppliers that are put at risk and or our Supplier Risk Register, maybe subject to a monthly performance review.

Annual AOC's will be required from a GSP and or a Card Acquirer and the Compliance Team will manage this.

Third Party Management

All 3d party Supplier/Vendor management is controlled via the Procurement team.

You can ask for Procurement help via Service Now (internally) or by e-mailing Procurement at:

- Procurement@manxtelecom.com

Procurement adhere/apply to ISO 9001/14001/45001 & 27001 processes as appropriate.

- https://www.manxtelecom.com/about/certifications/

Key Suppliers relevant to the support for PCI DSS relating card payments services may refer to the following documents:

Can be found at the following Hyperlink:

- PCI DSS:
- https://www.manxtelecom.com/supplier-terms
    - Covering our Code of Conduct

Note: For an up to date list of key suppliers the Procurement Team will be able to identify suppliers against appropriate criteria where relevant to PCI DSS for internal purposes/

Customer Credits, Chargebacks and Refunds

Any requests for queries relating to Customer Credits, Chargebacks and or Refunds will be managed by the Finance department whereby they relate to a 3rd party.

Roles and Responsibilities

Roles and Responsibilities are:

SHOP

- Step 1: MT: Consumer Engagement – Transaction Started via EPOS
- Step 1: PSP (Payment Service Provider) interface utilised
- Step 2: GSP (Gateway Service Provider) interface utilised
- Step 3: MT: Consumer Engagement – Consumer Completes Transaction
- Step 4: CA: Merchant seeks settlement via Card Acquirer to Merchant Bank
- Step 5: MT: Finance reconcile transaction, receipts etc
- Step 6: MT: Overall transaction complete bar any refunds and or chargebacks

ECOM

- Step 1: MT: Consumer Engagement – Transaction Started via Online Portal
- Step 1: PSP (Payment Service Provider) interface utilised
- Step 2: GSP (Gateway Service Provider) interface utilised
- Step 3: MT: Consumer Engagement – Consumer Completes Transaction
- Step 4: CA: Merchant seeks settlement via Card Acquirer to Merchant Bank
- Step 5: MT: Finance reconcile transaction, receipts etc
- Step 6: MT: Overall transaction complete bar any refunds and or chargebacks

MOTO

- Step 1: MT: Consumer Engagement – Transaction Started via IVR interface
- Step 1: PSP (Payment Service Provider) interface utilised
- Step 2: GSP (Gateway Service Provider) interface utilised
- Step 3: MT: Consumer Engagement – Consumer Completes Transaction
- Step 4: CA: Merchant seeks settlement via Card Acquirer to Merchant Bank
- Step 5: MT: Finance reconcile transaction, receipts etc
- Step 6: MT: Overall transaction complete bar any refunds and or chargebacks

5. SUPPLIER PERFORMANCE REVIEWS

Risks related to PCI DSS are collated, monitored and managed through the use of the Revenue Assurance Team.

Supplier performance reviews will be monitored and actioned by the Procurement team inline with the Supplier Performance Process Overview above.

6. PCI DSS STANDARDS

General queries around PCI DSS standards in specific to 12.8 can be located at:

- https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

7. GLOSSARY

PCI DSS	Approvals Body – GRC (Group Risk Committee)
AOC	Attestations of Compliance by a certified (QSA)