Payment Card Industry Data Security Standard (PCI-DSS) Policy

1 Purpose

This policy outlines MTVH's management of payment card security as part of compliance with the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS is a set of standards to help protect people from cardholder data theft or fraud, they represent the minimum standards of security required to safeguard payment card transactions.

All organisations that store, process or transmit cardholder data must comply with the PCI-DSS, failure to do so may result in financial penalties, costly investigations, and damage to MTVH's reputation. This policy must be read in conjunction with the **Payment Card Industry Data Security Standard (PCI-DSS) Procedure**, **Information Security Policy** and **Data Protection Policy**.

2 Scope

This policy applies to all colleagues handling or exposed to cardholder data who have a role in payment processing in any capacity, such as online, over the phone, face to face, via specific devices e.g card machines refer to the **Payment Card Industry Data Security Standard (PCI-DSS) Procedure.**.

For the purposes of this policy, cardholder data includes the following:

- Primary Account Number (PAN)
- Cardholder name
- Expiry date
- Security code (magnetic-stripe data or printed security features),
- Three-digit code (e.g Card Verification Code CVC Code)
- Personal Identification Number (PIN) – secret numeric password known only to the user

3 Responsibilities

Below is a table which sets out the roles and responsibilities of MTVH Colleagues/Teams who are exposed to or handle card data

Role	Responsibilities

Information security	• Oversee PCI-DSS compliance overall
	• Perform quarterly reviews of PCI-DSS scope (identifying all in-scope and out-of-scope networks and system components, and all connected third parties)
	• Perform quarterly scans:
	  ○ Of any cardholder data retention
	  ○ Of any wireless access points.
	  ○ Vulnerability in line with the PCI-DSS
	• Annually review Learning Zone PCI-DSS module compliance
	• Confirm receipt of third-party Attestation of Compliance documentation annually

Role	Responsibilities
Technology	• Install and maintain firewall configuration to protect cardholder data • Regularly test security systems and applications • Encrypt transmission of cardholder data across open, public networks • Develop and maintain secure systems and applications • Monitor and restrict access to cardholder data
Line Managers	• Manage daily cardholder data activities (e.g. tamper checks on devices) • Record and report on training compliance
Colleagues	• Complete the PCI-DSS training course on Learning Zone • Carry out daily cardholder data activities (e.g. tamper checks on devices)

4 Training

Training must be completed by all colleagues handling cardholder data, exposed to the handling of cardholder data, work in an environment where these activities take place, or who have a role in payment processing in any capacity. Training can be accessed on Learning Zone and must be completed as part of induction if appropriate to the role and refreshed annually.

Line managers are responsible for ensuring those who they manage have read and understood the PCI-DSS policy and procedures and have undertaken applicable training. Line managers are responsible for recording and reporting compliance with training.
Unsuccessful or incomplete training must be recorded and the member of staff barred from accessing Card Holder Data (CHD) until it has been successfully completed.

Colleagues who do not comply with the requirements of the training and the MTVH PCI-DSS policy and procedures may be subject to MTVH disciplinary procedures.

5 Our commitment to Equality, Diversity, and Inclusion

In implementing this policy MTVH will not discriminate against any colleague, customer, or stakeholder on the grounds of their sex, sexual orientation, gender reassignment status, ethnic origin, age, religious belief, disability, marital status, and pregnancy/maternity.

An Equality Impact Assessment has been completed for this Policy and is retained by the Policy Team.

6 Key Policy Information

Policy Owner	Information Security
Author	Information Security Manager
Approved by	Chief Information Officer
Effective from	November 2023
Approach to review	This Policy & associated Procedures will be reviewed as required by the owner for changes in legislation, regulation, and operational need. Any amendments will be appropriately consulted on and signed off before being clearly communicated to customers and colleagues. Next expected review is 5 years from the 'Effective date' of this document.
This is a controlled document maintained and accessible via MTVH's intranet, The Hub. When viewed outside of the intranet, this document should be checked against the master copy held by MTVH to verify that it is the current version, or it shall be considered uncontrolled.	