PCI DSS Charter Statement

Policy Owner:	Risk & Compliance	**Policy Number:**	POL - 089

Purpose

This PCI DSS Charter Statement defines the commitment, scope and governance approach for Telehouse International Corporation of Europe's ('the organisation') responsibilities under the Payment Card Industry Data Security Standard (PCI DSS) in respect of its UK and French co-location services.

Organisational Role

The organisation operates data centre facilities in the United Kingdom and France and provides secure colocation services to customers. The organisation acts as a merchant agent and does not store, process or transmit cardholder data or sensitive authentication data on behalf of customers or any other party.

Customers may deploy, operate and manage systems within the organisation's facilities that store, process or transmit cardholder data. The organisation does not have logical, administrative or operational access to customer systems, applications, networks or data repositories where cardholder data may exist.

PCI DSS Scope

The PCI DSS assessment scope for the organisation is limited to the physical security, monitoring and governance controls that the organisation operates for its data centre facilities and associated operational processes. The in-scope PCI DSS requirements are limited to applicable controls within Requirements 9, 10 and 12.

- **Requirement 9:** Restrict physical access to cardholder data by maintaining appropriate facility access controls, visitor management, monitoring, access authorisation, badge management and physical security procedures for areas under the organisation's control.
- **Requirement 10:** Support applicable monitoring and auditability for physical access control systems and security monitoring systems operated by the organisation, including retention and review of relevant access and security event records where applicable.
- **Requirement 12**: Maintain information security policies, roles, responsibilities, risk management practices, incident response arrangements, third-party management processes and security awareness activities relevant to the organisation's limited PCI DSS scope.

All customer-managed systems, customer networks, customer applications, customer media, customer cabinets, payment applications, payment terminals, encryption keys, cardholder data environments and any related processing activities remain outside the organisation's PCI DSS assessment scope unless explicitly agreed in writing.

Last Review Date:	June	**Version:**	2.0
	2026	**Approved by:**	Risk & Compliance

Customer Responsibilities

Each customer is responsible for determining and maintaining the PCI DSS scope of its own environment, including any systems, networks, applications or processes that store, process or transmit cardholder data within the organisation's facilities. Customers remain responsible for implementing and validating all PCI DSS controls applicable to their own cardholder data environments.

The organisation will support customer PCI DSS activities by making available appropriate evidence relating to in-scope physical security controls, subject to contractual terms, confidentiality requirements and applicable legal or regulatory obligations in the United Kingdom and France.

Communication

The organisation is committed to maintaining a secure physical operating environment for its co-location services and to preserving the confidentiality, integrity and availability of facility security controls that may affect customer PCI DSS obligations.

Accountability for this charter rests with senior management, supported by the Risk, Compliance, Security and Operations functions. Applicable policies, procedures and control evidence will be maintained, reviewed and updated to reflect changes in facilities, services, regulatory expectations, customer requirements and PCI DSS guidance.

This charter will be reviewed at least annually and following any material change to the organisation's facilities, services, customer access model, PCI DSS scope or contractual responsibilities.

Last Review Date:	June	**Version:**	2.0
	2026	**Approved by:**	Risk & Compliance