PCI DSS V3.2 Service Provider Responsibilities

Introduction

Through the provision of co-location hosting services Sure (Guernsey) Ltd, Sure (Jersey) Ltd, and Foreshore Ltd provide input into the customer's PCI DSS program, helping the customer to achieve compliance with the PCI DSS V3.2 standard via the controls as detailed in this document. Sure (Guernsey) Ltd, Sure (Jersey) Ltd, and Foreshore Ltd are happy to demonstrate these controls upon request.

Responsibility Matrix

It should be noted that the scope of this assessment is limited to PCI DSS V.3.2 requirements 9 and 12 as consistent with the service provided.

Card Data Environment = CDE

Data Centre/s – DC/s

Reference	Control Objective\Control Question	Responsibility
Requirement 9		
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Sure
9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	Sure
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	Sure
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	Sure
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying new onsite personnel or visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	Sure

PCI DSS V3.2 Service Provider Responsibilities

Reference	Control Objective\Control Question	Responsibility
Requirement 9		
9.3	Control physical access for onsite personnel to sensitive areas as follows: - • Access must be authorised and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	Sure
9.4	Implement procedures to identify and authorise visitors. Procedures should include the following:	Sure
9.4.1	Visitors are authorised before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	Sure
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	Sure
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	Sure
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and datacentres where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorising physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Sure
9.5	Physically secure all media.	Customer
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Customer
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:	Customer
9.6.1	Classify media so the sensitivity of the data can be determined.	Customer
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	Customer
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	Customer

PCI DSS V3.2 Service Provider Responsibilities

Reference	Control Objective\Control Question	Responsibility
Requirement 9		
9.7	Maintain strict control over the storage and accessibility of media.	Customer
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	Customer
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	Customer
9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	Customer
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	Customer
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	Customer
9.9.1	Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	Customer
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	Customer
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behaviour and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Customer
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	Sure - as it relates to security of its DCs Customer - other elements of CDE

PCI DSS V3.2 Service Provider Responsibilities

Reference	Control Objective\Control Question	Responsibility
Requirement 12		
12.1	Establish, publish, maintain, and disseminate a security policy.	Sure
12.1.1	Review the security policy at least annually and update the policy when the environment changes.	Sure
12.2	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal risk assessment	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.1	Explicit approval by authorised parties.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.2	Authentication for use of the technology.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.3	A list of all such devices and personnel with access.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labelling, coding, and/or inventorying of devices).	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.5	Acceptable uses of the technology.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.6	Acceptable network locations for the technologies.	Sure - as it relates to security of its DCs Customer - other elements of CDE

PCI DSS V3.2 Service Provider Responsibilities

Reference	Control Objective\Control Question	Responsibility
Requirement 12		
12.3.7	List of company-approved products.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	Customer
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorised for a defined business need. Where there is an authorised business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	Customer
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.4.1	For service providers. Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance Defining a charter for a PCI DSS compliance program and communication to executive management. *(Best practice until 31 January 2018, after which it becomes a requirement).*	Customer
12.5	Assign to an individual or team the following information security management responsibilities:	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.5.1	Establish, document, and distribute security policies and procedures.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.5.2	Monitor and analyse security alerts and information, and distribute to appropriate personnel.	Sure - as it relates to security of its DCs Customer - other elements of CDE

PCI DSS V3.2 Service Provider Responsibilities

Reference	Control Objective\Control Question	Responsibility
Requirement 12		
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.5.4	Administer user accounts, including additions, deletions, and modifications.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.5.5	Monitor and control all access to data.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	Sure
12.6.1	Educate personnel upon hire and at least annually.	Sure
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Sure
12.7	Screen potential personnel prior to hire to minimise the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	Customer
12.8.1	Maintain a list of service providers.	Customer
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Customer
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Customer
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Customer

PCI DSS V3.2 Service Provider Responsibilities

Reference	Control Objective\Control Question	Responsibility
Requirement 12		
12.9	Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.10	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.10.1	• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.10.2	Test the plan at least annually.	Customer
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	Sure - as it relates to security of its DCs Customer - other elements of CDE
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Sure - as it relates to security of its DCs Customer - other elements of CDE

PCI DSS V3.2 Service Provider Responsibilities

Reference	Control Objective\Control Question	Responsibility
Requirement 12		
12.11	For service providers. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: Daily log reviews Firewall rule-set reviews Applying configuration standards to new systems. Responding to security alerts. Change management processes *(Best practice until 31 January 2018, after which it becomes a requirement)*	Customer
12.11.1	For service providers. Maintain documentation of quarterly review process to include: Documenting results of the reviews Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program. *(Best practice until 31 January 2018, after which it becomes a requirement)*	Customer

sure. International
Batelco Group Member

Guernsey
Centenary House
La Vrangue
St Peter Port
Guernsey
GY1 2EY
01481 757757

Jersey
The PowerHouse
Queens Road
St Helier
Jersey
JE2 3AP
01534 888291

Isle of Man
Atlantic House
4-8 Circular Road
Douglas
Isle of Man
IM1 1AG
01624 692222