American Express Data Security Operating Policy for Service Providers*

These requirements apply to all your equipment, systems, and networks on which American Express Cardmember Information is processed, stored, or transmitted.

Section I – Data Security Standards for Service Providers

Service Providers must, and they must cause their Covered Parties, to:

(i) store Cardmember Information only to facilitate Card transactions in accordance with their agreements; with American Express; and

(ii) comply with the current version of the Payment Card Industry Data Security Standard (PCI Standard, which is available at www.pcisecuritystandards.org) no later than the effective date for implementing that version.

Service Provider's data security procedures for the Card will be no less protective than for Other Payment Products it processes. Service Provider's are liable for Covered Parties' compliance with this subsection.

Covered Parties means any or all of a Service Provider's employees, agents, representatives, subcontractors, Processors, providers of its point of sale equipment or systems or payment processing solutions, and any other party to whom it may provide Cardmember Information access in accordance with its agreement with American Express.

Section 2 – Duty to Notify American Express

Service Providers must notify American Express immediately if they know or suspect that Cardmember Information has been accessed or used without authorisation or used other than in accordance with their agreement with American Express. Service Providers must engage at their sole cost a third party forensic investigator to conduct a thorough audit of such data incident, or they must provide (and obtain any waivers necessary to provide) to American Express and its forensic investigators and auditors, on request and at the merchant's sole cost, full cooperation and access to conduct a thorough audit of such data incident. Service Provider shall promptly provide to American Express, all Card account numbers related to the data incident and audit reports of the data incident. Service Providers must work with American Express to rectify any issues arising from the data incident, including consulting with American Express about their communications to merchants and Cardmembers affected by the data incident and providing (and obtaining any waivers necessary to provide) to American Express all relevant information to verify their ability to prevent future data incidents in a manner consistent with their agreement with American Express. Audits must include forensic reviews and reports on compliance, as well as any and all information related to the data incident, and they must identify the cause of the data incident and confirm whether or not the Service Provider was in compliance with the PCI Standard at the time of the data incident. We may contact a third party security assessor to begin a forensic investigation or site certification.

Contact your Processor Relationship Manager or call the American Express Merchant Help Desk on 01273 67 55 33 if you believe that Cardmember Information has been compromised. Please have several American Express merchant numbers with you when you call, which we can use as a reference.

Section 3 – Indemnity Obligations

Service Provider's indemnity obligations to American Express under their agreement with American Express include, without waiving any of American Express's other rights and remedies, liability for all fraudulent transactions related to such data incidents and all costs, fees, and expenses (including claims from third parties and all costs incurred by American Express related to the notification of Cardmembers, cancellation and reissuance of Cards and fraud monitoring, reasonable legal fees and disbursements, and costs of investigation, litigation, settlement, judgment, interest, and penalties) that American Express incurs as a result of such data incidents unless:

(i) Service Provider notifies American Express pursuant to this section;

* References to "Service Providers" in this policy include Authorised Processors, Processors, Processor's, and any other providers to merchants of point of sale equipment, software, or systems or other payment processing solutions or services.

(ii) the Service Provider is and was in compliance at the time of the data incident with this Data Security Operating Policy; and

(iii) the data incident was not caused by the wrongful conduct of the Service Provider or one of its employees or agents.

Section 4 – IMPORTANT! DEMONSTRATION OF COMPLIANCE WITH DATA SECURITY OPERATING POLICY

Service Providers must take the following steps to demonstrate their compliance with this Data Security Operating Policy.

Step 1 – Validation Requirements

Service Providers must send the following documentation to American Express in order to validate their compliance with this Data Security Operating Policy, annually or quarterly as described below (each such period, a *reporting period*):

(i) Annual Onsite Security Assessment Report; and

(ii) Quarterly Network Scan.

Annual Onsite Security Assessment Validation Documentation

The Annual Onsite Security Assessment is a detailed onsite examination of Service Provider's equipment, systems, and networks (and their components) where Cardmember Information is processed, stored, or transmitted. It must be performed by:

(i) a Qualified Security Assessor (QSA), listed below; or

(ii) the Service Provider and certified by the chief executive officer, chief financial officer, or principal of the Service Provider.

Service Providers must complete and submit the summary of the findings of this assessment (and copies of the full report on compliance, on request) annually to American Express.

For a Service Provider to be deemed compliant with this Data Security Operating Policy, the summary must certify the Service Provider's compliance with all requirements of the PCI Standard. A list of QSAs is available at www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Quarterly Network Scan Validation Documentation

The Quarterly Network Scan is a process that remotely tests a Service Provider's internet-connected computer networks and web servers for potential weaknesses and vulnerabilities. It must be performed by an Approved Scanning Vendor (ASV), listed below. Service Providers must complete and submit the summary of the findings of the scan (and copies of the full scan, on request) quarterly to American Express. For a Service Provider to be deemed compliant with this Data Security Operating Policy, the summary must certify that there are no high risk issues. A list of ASVs is available at www.pcisecuritystandards.org/pdfs/asv_report.html.

Step 2 – Send the Validation Documentation to American Express

Service Providers must submit the validation documentation, in an encrypted format, via compact disc, to American Express at the address below.

American Express Payment Services Limited
GNO Data Security Unit
PO Box 54886
London, SW1W 0YW
United Kingdom

The encryption key required to decrypt the Validation Documentation, as well as the Service Provider name, the Service Provider's data security contact including name, address and phone number must be e-mailed to: AmericanExpressDataSecurityEMEA@aexp.com

Compliance and validation is completed at the Service Provider's expense. By submitting Validation Documentation, Service Providers represent and warrant to American Express that they are authorised to disclose the information contained therein and are providing the Validation Documentation to American Express without violating any other party's rights.

Non-Validation Fees and Termination of Agreement with American Express

Service Providers will be assessed for non-validation fees and their agreement with American Express may also be terminated if they do not fulfil these requirements or fail to provide the validation documentation to American Express by the applicable deadline. American Express will notify Service Providers separately of the applicable deadline for each reporting period.

A non-validation fee will be assessed if the Validation documentation is not received by the first deadline.	£12,500
An additional non-validation fee will be assessed if the Validation Documentation is not received within 30 days of the first deadline.	£18,000
An additional non-validation fee will be assessed if the Validation Documentation is not received within 60 days of the first deadline.	£23,000

If American Express does not receive a Service Provider's validation documentation within 60 days of the first deadline, then American Express may terminate its agreement with the Service Provider in accordance with its terms as well as impose the foregoing non-validation fees on the Service Provider.

Confidentiality Commitment

American Express shall take reasonable measures to keep a Service Provider's report on compliance, including its summary of findings rendered in connection with an Annual Onsite Security Assessment, PCI Annual Self-Assessment Questionnaire and summary of findings rendered in connection with a Quarterly Network Scan (such documents called Validation Documentation) in confidence and not disclose the Validation Documentation to any third party (other than its agents, representatives, service providers and subcontractors) for a period of two years from the date of receipt, except that this confidentiality obligation does not apply to Validation Documentation that:

(i) is already known to American Express prior to disclosure by a Service Provider;

ii) is or becomes available to the public through no breach of this paragraph by American Express;

ii) is rightfully received from a third party by American Express without a duty of confidentiality;

(iv) is independently developed by American Express; or

(v) is required to be disclosed by an order of a court, administrative agency or governmental authority, or by any law, rule or regulation, or by subpoena, discovery request, summons, or other administrative or legal process, or by any formal or informal inquiry or investigation by any government agency or authority (including any regulator, inspector, examiner, or law enforcement agency).

Section 5 — Changes

American Express's Data Security Operating Policy, may be changed upon providing 90 days notice.

Section 6 – Disclaimer

Except as otherwise specified in this policy, a Service Provider's compliance with this Data Security Operating Policy will not in any way relieve its indemnity obligations to American Express under its agreement with American Express, nor relieve or decrease its liability in any way. Service Providers are responsible at their sole expense for providing additional data security measures that they deem necessary to protect their particular data and interests. American Express does not in any way represent or warrant that the measures contained in such agreement or this policy are sufficient or adequate to protect Service Providers' particular data and interests.

American Express hereby disclaims any and all representations, warranties, and liabilities with respect to this Data Security Operating Policy, the PCI Standard, and the designation and performance of QSA or ASV (or both), whether express, implied, statutory, or otherwise, including any warranty of merchantability or fitness for a particular purpose.

Useful Web Sites

American Express Data Security:
www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC for:

- PCI Data Security Standards copy
- Self Assessment Questionnaire copy
- List of Qualified Security Assessors
- List of Approved Scanning Vendors

www.pcisecuritystandards.org