American Express® Data Security Operating Policy for Service Providers*

As a leader in consumer protection, American Express has a long-standing commitment to protect Cardmember Information, ensuring that it is kept secure.

Compromised data negatively impacts consumers, merchants, Service Providers, and card issuers. Even one incident can severely damage a company's reputation and impair its ability to effectively conduct business. Addressing this threat by implementing security operating policies can help improve customer trust, increase profitability and enhance a company's reputation.

In continuously addressing security issues, we have developed this Data Security Operating Policy and are working with Service Providers to help them establish appropriate security programs.

American Express knows that you share our concern and requires, as part of your responsibilities, that you comply with the data security provisions in your agreement with American Express and this policy. 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 then-current Payment Card Industry Data Security Standard ("PCI Standard"). "Covered Parties" means any or all of a Service Provider's employees, agents, representatives, subcontractors, Processors, providers of 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 authorization or used other than in accordance with their agreements with American Express. Service Providers must provide (and obtain any waivers necessary to provide) to American Express and its auditors, on request, full cooperation and access to conduct a thorough audit of such data incident, including providing all Card account numbers related to the incident and audit reports of the incident. Service Providers must work with American Express to rectify any issues arising from the incident, including consulting with American Express about their communications to merchants and Cardmembers (or both) affected by the incident and providing (and obtaining any waivers necessary to provide) American Express all relevant information to verify their ability to prevent future 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 incident, and they must identify the cause of the incident and confirm whether or not the Service Provider was in compliance with the PCI Standard at the time of the data incident.

Service Providers' indemnity obligations to American Express under their agreement with American Express include, without waiving 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 and cancellation and re-issuance of Cards, reasonable legal fees and disbursements, and costs of investigations, litigation, settlement, judgment, interest, and penalties) American Express incurs as a result of such data incidents unless (i) the Service Provider notifies American Express pursuant to this section, (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.

Contact your Third Party Processor Relationship Manager or call 2277 2277 if you believe that Cardmember Information has been compromised.

Section 3 – 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, annually or quarterly as is subsequently described (each such period, a "reporting period").

* References to "Service Providers" in this policy include Authorized Processors, Third Party Processors, Gateway Providers, and any other providers to merchants of point of sale equipment, software, or systems or other payment processing solutions or services.

Step 1 – Compliance Requirements

All Service Providers must send the following documentation to American Express in order to validate their compliance with this policy:

- Annual Onsite Security Audit Report, and
- Quarterly Network Scan

Annual Onsite Security Audit Validation Documentation – The Annual Onsite Security Audit is a detailed onsite examination of a 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 third party security assessor acceptable to American Express or (ii) by 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 executive summary of the results of this audit (and copies of the full audit, 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.

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 a third party security assessor acceptable to American Express. Service Providers must complete and submit the executive summary of the results 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.

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 International Inc.
GNO Data Security Unit 18/F City Plaza 4, 12 Taikoo Wan Road
Taikoo Shing
Hong Kong

The encryption key required to decrypt the documentation, including organization name, should be e-mailed to: AmericanExpressDataSecurityJAPA@aexp.com

Compliance and validation is completed at Service Provider's expense.

Non-Validation Fees and Termination of Agreement with American Express

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

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.

Section 4 – Disclaimer

Except as otherwise specified in this policy, a Service Provider's compliance with this Data Security Operating Policy shall 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 Provider's 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 THIRD PARTY SECURITY ASSESSORS, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY WARRANTY OF MERCHANT-ABILITY OR FITNESS FOR A PARTICULAR PURPOSE.