# American Express® Data Security Operating Policy for Merchants

**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, 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 merchants 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 to accept the American Express Card ("Card Acceptance Agreement"). 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 Merchants

Merchants must, and they must cause their Covered Parties, to: i) store Cardmember Information only to facilitate Card transactions in accordance with their Card Acceptance Agreements and (ii) comply with the then current Payment Card Industry Data Security Standard (PCI Standard). "Covered Parties" means any or all of a merchant's employees, agents, representatives, subcontractors, Processors, Service Providers, 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 Card Acceptance Agreement.

## Section 2 – Duty to Notify American Express

Merchants 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 Card Acceptance Agreement. Merchants 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. Merchants must work with American Express to rectify any issues arising from the data incident, including consulting with American Express about their communications to Cardmembers affected by the incident and providing (and obtaining any waivers necessary to provide) to American Express all relevant information to verify their ability to prevent future incidents in a manner consistent with their Card Acceptance Agreement. Audits must inlcude fornensic reviews and reports on compliance, any and all information related to the incident, and they must identify the cause of the data incident and confirm whether or not the Merchant was in compliance with the PCI Standard at the time of the data incident.

Merchant's indemnity obligations to American Express under their Card Acceptance Agreement 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, reasonable legal fees and disbursements, and costs of investigation, litigation, settlement, judgment, interest, and penalties) American Express incurs as a result of such data incidents *unless*: (i) the merchant notifies American Express pursuant to this section; (ii) the merchant 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 merchant or one of its employees or agents.

Contact your Client 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

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

### *Step 1 – Determine your Merchant Level and Compliance Requirements*

Most Merchant Levels are based on the merchant's volume of American Express Card transactions submitted by its Establishments that roll-up to the highest American Express account level. Merchants fall into one of three levels specified in the table below.

| Level | Definition | Validation Documentation | Requirement |
|---|---|---|---|
| 1 | 2.5 million American Express Card transactions or more per year; or any merchant that has had a data incident; or any merchant that American Express otherwise deems a Level 1 | Annual Onsite Security Audit Report, and Quarterly Network Scan | Mandatory |
| 2 | 50,000 to 2.5 million American Express Card transactions per year | Quarterly Network Scan | Mandatory |
| 3 | Less than 50,000 American Express Card transactions per year | Quarterly Network Scan | Strongly Recommended* |

* Level 3 Merchants need not submit Validation Documentation, but nevertheless must comply with, and are subject to liability under, all other provisions of this Data Security Operating Policy.

Determine your level and the documents that you must send to American Express in order to validate your compliance with this policy.

**Annual Onsite Security Audit Validation Documentation** – The Annual Onsite Security Audit is a detailed onsite examination of merchant 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 merchant and certified by the chief executive officer, chief financial officer, or principal of the merchant. Merchants

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 Merchant to be deemed compliant with this Data Security Operating Policy, the summary must certify the Merchant'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 merchant'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. Merchants 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 Merchant 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.*

Level 1 and Level 2 Merchants must submit the Validation Documentation marked "mandatory" in the table on the first page, 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**

- Level 1 Merchant's validation documentation must include executive summaries of the Annual Onsite Audit Report and Quarterly Network Scan report, as described above.
- Level 2 Merchant's validation documentation must include executive summaries of the Quarterly Network Scan, as described above.
- Level 3 Merchants are not required to submit validation documentation (but must comply with, and are subject to liability under, all other provisions of this policy).

The encryption key required to decrypt the documentation, as well as the Merchant's 10-digit American Express number, must be e-mailed to AmericanExpressDataSecurityJAPA@aexp.com

Compliance and validation is completed at the Merchant's expense.

### Non-Validation Fees and Termination of Card Acceptance Agreement

Merchants will be assessed non-validation fees and their Card Acceptance Agreement may also be terminated if they do not fulfil these requirements or fail to provide the mandatory Validation Documentation to American Express by the applicable deadline. American Express will notify merchants separately of the applicable deadline.

If American Express does not receive a Merchant's mandatory Validation Documentation within 60 days of the first deadline, then American Express may terminate the merchant's Card Acceptance Agreement in accordance with its terms as well as impose the foregoing non-validation fees on the Merchant.

## Section 4 – Disclaimer

Except as otherwise specified in this policy, a Merchant's compliance with this Data Security Operating Policy shall not in any way relieve its indemnity obligations to American Express under its Card Acceptance Agreement, nor relieve or decrease its liability in any way. Merchants 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 the Card Acceptance Agreement or this policy are sufficient or adequate to protect Merchants' 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 EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.