

VISA SUPPLIER SECURITY STANDARDS

Supplier must maintain and enforce policies, standards and processes designed to secure the Visa Data. This document describes the minimum-security measures that must be taken by Supplier. If any other agreement with Supplier requires additional security measures, Supplier will abide by the terms of any such agreement. For the avoidance of doubt, Supplier agrees that it will ensure its Personnel and subcontractors that process or retain Visa Data comply with these Visa Supplier Security Standards as if they were Supplier. The parties agree that reference to Visa under this annex also refer to its affiliates.

Terms not defined herein have the meaning set forth in the Visa Supplier Privacy and Security Terms.

Supplier represents, warrants, and covenants to Visa (including during the term of the Agreement and for any surviving periods thereof) that:

1. **Information Security Policies and Standards.** Supplier shall implement and document appropriate administrative, technical, and physical measures to protect Visa Data against accidental or unlawful destruction, alteration, and unauthorized access, disclosure or use.
 - a) Supplier shall communicate these security requirements to all staff, subcontractors, suppliers, and agents who have access to Visa Data.
 - b) Supplier shall regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures and conducts periodic risk assessments to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Visa Data.
 - c) Supplier must update its information security practices at least annually or whenever there is a material change in Supplier's business practices that may affect the security, confidentiality or integrity of Visa Data, provided that Supplier will not modify its information security practices in a manner that will weaken its controls.
 - d) Upon request, Supplier will provide Visa with information about its security measures.
 - e) Once per year, Supplier will also provide Visa with copies of any applicable Service Organizational Control (SOC) report(s) based on the SSAE 21 model or any successor authoritative guidance for reporting on service organizations ("**SOC 2 Reports**"). Visa understands that the Supplier's security program information and SOC 2 Reports contain confidential information of the Supplier, and Visa will not use or disclose the SOC 2 Reports other than to its auditors, regulators, and advisors in connection with verifying Supplier's compliance with Visa's security and privacy program requirements.
 - f) If Supplier performs any Services that entail access to Visa Systems, include web development or hosting on behalf of Visa, or third parties doing business with Visa, or include development activities in a non-Visa environment Supplier shall, at its sole cost and expense, adhere to and demonstrate adherence to applicable ISO 27002 requirements or other international standards acceptable to Visa.
2. **Security and Risk Assessments.** Without limiting Supplier's obligations in this Exhibit and the **Data Processing Agreement**, Visa, or any designee to whom Supplier is providing a Service, may conduct a detailed security and risk assessment of Supplier ("**Assessment**") to ensure Supplier's ability to comply with this Agreement. Supplier shall reasonably cooperate with Visa during any Assessment. The Assessment may include: (A) Visa or its designated agent performing an onsite or remote assessment of Supplier's security and risk programs during normal business hours; and (B) penetration testing of all software applications, infrastructure, and datacenters that handle or store Visa Data. Visa may re-conduct Assessments annually in its sole discretion. Supplier shall, upon Visa's request and at

Supplier's expense, negotiate in good faith an Order to resolve any issues identified in the Assessment and address Supplier's implementation of any additional security measures that Visa requires. As defined in this Exhibit and the **Data Processing Agreement**, Visa will be entitled to terminate Supplier's Processing of Visa Data or suspend such Processing until all issues identified in the Assessment are resolved or all additional security measures required by Visa are implemented to Visa's satisfaction.

3. **Physical Security.** Supplier shall maintain commercially reasonable security systems at all Supplier sites at which an information system that uses or houses Visa Data is located. Supplier must reasonably restrict access to such Visa Data appropriately and implement controls to prevent unauthorized individuals from gaining access to systems and facilities containing Visa Data.
4. **Organizational Security.**
 - a) Supplier shall maintain records specifying which media are used to store Visa Data.
 - b) When media are disposed of or reused, procedures prevent any subsequent retrieval of any Visa Data stored on them. When media are to leave the premises at which the files are located as a result of maintenance operations, the procedures must prevent undue retrieval of Visa Data stored on them.
 - c) Supplier must implement security policies and procedures to classify data assets based on sensitivity, and to clarify security responsibilities and promote awareness for employees. For purposes of this classification, "Sensitive Information" includes (i) all government-issued identification numbers, (ii) Primary Account Numbers (PANs) or other financial account numbers and all Cardholder Data; or (iii) information on race, religion, ethnicity, sex life or sexual orientation, health information, genetic or biometric information, biometric templates, political, religious or philosophical beliefs or opinions, trade union membership, background check information or judicial data such as criminal records (including alleged commission of an offense).
 - d) Supplier shall manage all security events and incidents in accordance with appropriate incident response procedures.
 - e) Supplier must encrypt, using industry-standard encryption tools, all Sensitive Information that Supplier: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; and (iii) stores on portable devices, in each case, where technically feasible. Supplier will safeguard the security and confidentiality of all encryption keys associated with encrypted Sensitive Information.
 - f) Supplier shall implement controls to ensure that (i) Visa Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage and (ii) the target entities for any transfer of Visa Data by means of data transmission facilities can be established and verified.
 - g) Supplier shall implement controls to ensure that Visa Data collected for different purposes can be processed separately.
5. **Network Security.** Supplier maintains network security using industry-standard equipment and techniques, including firewalls, intrusion detection and prevention systems, access control lists and routing protocols.
6. **Access Control.**
 - a) Supplier shall maintain appropriate access controls, including, but not limited to, restricting access to Visa Data to the minimum number of Supplier Personnel who require such access.
 - b) Only authorized staff can grant, modify or revoke access to an information system that uses or houses Visa Data. Supplier must maintain an audit trail to document whether and by whom Visa

Data have been accessed, entered into, modified, transferred or removed from Processing, which is provided to Visa upon request.

- c) Supplier shall establish and implement User administration procedures that define user roles and their privileges and how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms.
- d) Supplier shall revoke access to terminated employees promptly and without undue delay
- e) All employees and contractors of Supplier must be assigned unique User IDs.
- f) Access rights must adhere to the "least privilege" principle.
- g) Supplier shall implement commercially reasonable physical and electronic security controls to create and protect passwords or other access credentials.
- h) Supplier shall establish controls to prevent Visa Data processing systems from being used accidentally or without authorization, such as through logical access controls.

7. Virus and Malware Controls. Supplier shall implement centrally managed, industry-standard vulnerability management tools and processes, including the latest anti-virus and malware protection software on its systems. Supplier shall implement malware monitoring and system scanning to reduce all Services-related vulnerabilities and to protect Visa Data and the Services from the effects of vulnerabilities or virus infections.

8. Security Events. Supplier will promptly investigate any Security Event, including any alleged or suspected **Data Breach**. Supplier will notify Visa of any event reasonably believed to constitute a Security Event in writing without undue delay, no later than twenty-four (24) hours after discovery of the Security Event. This notification must be made via email to vsirt@visa.com. Supplier will provide Visa with all information about the Security Event reasonably needed by Visa and its Affiliates to assess the potential impact to its information and operations, its incident response obligations, and to comply with applicable law, including (for example) the root cause of the breach, information about the affected individuals or Cardholder Data, and the possible consequences.

- a) Except as required by law, Supplier will not make any notification or announcement about a Security Event without Visa's prior written approval, including (without limitation) any notification to any relevant regulatory body or any announcement to affected individuals or the public. Notwithstanding the preceding sentence, Visa understands that Supplier may notify other companies (such as other clients) that may also be impacted by the incident and may notify law enforcement if appropriate, provided Visa is not identified in such notifications.
- b) If the Security Event results from either (i) the negligence or misconduct of Supplier or its Personnel (including any sub-processor or sub-contractor), or (ii) a failure of Supplier to comply with this Agreement (including this Exhibit), Supplier will bear Visa's costs directly resulting from, or incurred in connection with resolving, the Security Event, including (without limitation), conducting an investigation, engaging appropriate forensic analysis, notifying individuals, regulators and others as required to by law or the Payment Card Industry Data Security Standard, and providing individuals with credit monitoring (or other appropriate remediation service), as well as costs incurred in regulatory proceedings brought or threatened by a third party and all related expenses, including reasonable attorneys' fees, judgments, fines, costs, amounts paid in settlement or any loss or damage related thereto. The Parties agree that the foregoing shall be considered direct damages arising from such Security Event.
- c) For the avoidance of doubt, regardless of the responsibility for the Security Event, Supplier will fully cooperate with Visa and its Affiliates in Visa's investigation of and response to the Security Event and take all reasonable steps required by Visa to assist Visa to appropriately evaluate, contain, notify, and recover following a Security Event.

9. Vulnerability Assessment and Remediation. Supplier will cooperate with Visa to assess and remediate vulnerabilities that could compromise Visa Data, Visa Systems, or critical functioning of the information technology infrastructure of Visa or its clients or customers or that impacts Supplier's external-facing, internal or partner environments or the products or services Supplier provides to Visa. Vulnerabilities shall be classified based on industry recognized scoring methodologies (e.g., CVSS 3.1 or above). Remediation shall be performed at Supplier's expense following notification by Visa of matter requiring remediation based on the following schedule (the "**Visa Remediation Timeline**"):

- Critical severity matter(s) must be remediated within seven (7) calendar days
- High severity matter(s) must be remediated within thirty (30) calendar day
- Medium severity matter(s) must be remedied within sixty (60) calendar days
- Low severity matter(s) must be remediated within ninety (90) calendar days
- Very Low severity matter(s) must be remedied within one hundred eighty (180) calendar days

10. Vulnerability Notification. Supplier will

- a) actively monitor industry resources (e.g., www.cert.org, pertinent software vendor mailing lists and websites and information from subscriptions to automated notification services) for applicable security alerts and promptly notify Visa upon the discovery of a critical or high priority vulnerability in its external-facing, internal, subcontractor or partner environments used by Supplier to perform Services or house Visa Data or in the products or Services Supplier provides to Visa.
- b) Within seventy-two (72) hours of either Supplier's discovery of such a vulnerability, or receipt of a Visa inquiry about a vulnerability, Supplier will provide Visa with a written plan to appropriately remediate the vulnerability.
- c) Supplier will also provide Visa with written confirmation as soon as the vulnerability has been remediated. For the avoidance of doubt, any identified vulnerability must be remediated by Supplier in accordance with the Visa Remediation Timeline at Supplier's expense.

11. PCI DSS Compliance. If Supplier performs Services for Visa that include access, store, transmit, or process Cardholder Data, Supplier must, at its sole cost and expense

- a) conduct or have conducted the audits required for PCI DSS certification,
- b) obtain both PCI DSS Report of Compliance and PCI Attestation of Compliance ("**PCI Reports**") prior to storing, processing, or transmitting Cardholder Data,
- c) maintain PCI DSS compliance for so long as Supplier stores, processes, or transmits Cardholder Data
- d) remain at all times compliant with the Payment Card Industry Data Security Standard ("**PCI DSS**") and be aware of changes to PCI DSS and implement such changes when required,
- e) provide a copy of the PCI Reports upon request by Visa, and
- f) provide a copy of the PCI Responsibility Matrix as it applies to the Service upon request by Visa.

12. Logging Requirements. If Supplier provide applications and/or Services that are Visa branded or branded for a third-party doing business with Visa, process Cardholder Data, or are developed specifically for Visa or a third-party doing business with Visa, Supplier must be enrolled in the Visa Logging Program. Supplier shall make the following events available to Visa:

- a) identification and authentication events (username and timestamps)
- b) source and destination IPs
- c) actions performed (create, read, update, delete, escalation of privilege events, account changes)
- d) logging service status
- e) system level objects

- f) administrator-level activities
- g) access to PANs or Cardholder Data
- h) application specific data for intrusion detection standpoint (i.e. Path, URL, GET, POST etc.).

These events may be provided through either: (i) push-based method pursuant to which Supplier can push the logs to the Visa Logging Solution over HTTPS or Syslog, or (ii) pull-based method pursuant to which there is an API available from the Supplier to integrate with the Visa Logging Solution.

13. Penetration Testing. Each calendar year during the term of the Agreement, Supplier will cooperate with Visa to conduct penetration tests (“**PenTests**”) of applications and infrastructure, or other systems used to process and retain Visa Data. Visa will perform all PenTests for applications owned by or developed exclusively for Visa or any third party with whom Visa does business and on any infrastructure that supports such applications. For all other applications or supporting infrastructure (including software-as-a-service), Supplier may decide to have the PenTest performed by Visa or by an industry-standard PenTest provider mutually-agreed upon by the Parties. Supplier shall comply with the below guidelines (the “**Visa Guidelines for Penetration Testing and Reporting**”):

- a) The scope of the PenTest will be jointly defined by Visa’s Cybersecurity team and Supplier’s subject matter experts.
- b) Application PenTest will be performed in a pre-production environment that mimics production. Infrastructure PenTest will be performed in production environment encompassing the production infrastructure following an industry-standard methodology.
- c) If a PenTest provider conducts the PenTest,
 - 1.1 Supplier shall provide Visa with an unaltered copy of the final report or a formal attestation document (“**Report**”) for Visa’s review within fourteen (14) days of the PenTest’s conclusion.
 - 2.1 The Report will highlight the scope, methodology, results, finding summary, status of the findings and an outline of Supplier’s remediation timeline and policies.
 - 3.1 The PenTest must be performed no more than 12 months ago.
 - 4.1 The scope of the PenTest must include all functionalities offered to Visa and the Report must clearly describe the functionalities tested and systems included in the PenTest (i.e., applications, mobile/Mac apps, URLs, and API endpoints).
 - 5.1 Report published to Visa must include finding details with finding severity. Severity scoring must comply with the latest industry standards such as CVSS 3.1 or above. CVSS vector strings must be provided for each individual finding.
- d) If Visa will perform the PenTest, Supplier hereby authorizes Visa to perform the PenTest on the systems and Services that Supplier owns or manages (collectively the “**Tested Systems**”). Supplier certifies that it owns or has the exclusive right to and use of the Tested Systems and that Supplier has notified appropriate Personnel within its organization and any third parties including without limitation any host master, systems administrator, technical manager, and security manager prior to commencement of the PenTest. Supplier acknowledges that a PenTest, including testing, assessing, scanning, or monitoring the Tested Systems, including implementation and deployment, may disclose or create problems in the operation of such Tested Systems. Supplier acknowledges and accepts the risks involved with the Tested Systems, which may include without limitation, down time, loss of connectivity or data, system crashes or performance degradation (collectively “**Claims**”). Visa shall not be liable for any such Claims. During the duration of the PenTest, Visa will not perform intentional denial of service (DoS) or social engineering testing.
- e) Any findings identified as a part of the PenTest will be remediated at Supplier’s expense. For new applications or infrastructure supporting such applications, critical, high, and medium severity issues must be remediated prior to launch. For applications or their supporting infrastructure that

are currently in production (i.e., already in use with Supplier's general customer base), any identified matter(s) shall be remediated in accordance with the Visa Remediation Timeline.

14. Vendor Application Security Testing ("VAST"). If Supplier provides applications that are Visa-branded or branded for a third-party with whom Visa does business, store/process/transmit Sensitive Information, or has source code developed specifically for Visa or a third-party with whom Visa does business, such applications are subject to a source code review, and Supplier must participate in Visa's Vendor Application Security Testing (VAST) program. Supplier can meet Visa's VAST requirements by complying with one of the following options:

- a) Provide Visa with the source code, and the Visa Secure Systems Development Lifecycle ("**SSDLC**") team will perform source code review,
- b) Use its own internal source code scanning tools to perform static and dynamic code scanning and submit results via an alternate attestation document provided by the Visa VAST program, or
- c) Enrol in the Visa third-party VAST program ("**Visa Secure Code Program**"). As part of the Visa Secure Code Program, Visa utilizes a third-party vendor to conduct the secure coding activities ("**Code Scans**"). Visa will, at its cost, provide Supplier with static code scanning licenses so that Supplier may perform Code Scans during the Development Lifecycle. In addition, Vendor will act as an intermediary between the Supplier and Visa Cyber team to ensure clear communication of Code Scan results to Visa. If Supplier elects to participate in the Visa Secure Code Program, Supplier will be required to provide documentation regarding its development environment and the application, including security configuration information, and to implement an agreed-upon security test plan.

Supplier must remediate any VAST program findings in accordance with the Visa Remediation Timeline.

15. Vulnerability Management. If Supplier provide applications and/or Services that are Internet Facing AND Visa branded or Visa labeled, branded or labeled for a third-party doing business with Visa, or are developed specifically for Visa or are developed specifically for a third-party doing business with Visa such assets will be subject to Visa's Vulnerability Management program, including Web Application Vulnerability Management, Infrastructure Vulnerability Management, and/or Visa's Private Bug Bounty program (as such terms are commonly understood in the Information Security industry).

- a) If Supplier physically hosts, supports or provides any Services for or on behalf of Visa or a third party with whom Visa does business that are partially or wholly maintained at Supplier facilities or other Supplier locations (e.g., its third-party hosting provider(s) facilities) ("**Hosted Services**"), Supplier consents to ongoing Vulnerability Monitoring by Visa (or its authorized agents) of Supplier's assets providing the Hosted Services, including ongoing, continuous vulnerability testing on live assets using Web Application Vulnerability Management, Infrastructure Vulnerability Management, and/or Visa's Private Bug Bounty Program.
- b) Supplier will provide Visa with an accounting or list or ranges of IP addresses and application details (e.g., web application URLs, API, and network entry points).
- c) With respect to automated vulnerability scanning, upon request, Visa will provide Supplier with a list or ranges of IP addresses from which automated vulnerability testing occurs. Supplier will allowlist the IP addresses provided to prevent issues with vulnerability testing and minimize the number of alerts and events triggered by Visa's testing.
- d) With respect to the Bug Bounty program, Visa has engaged a third-party platform that helps Visa invite members of the platform to help Visa identify vulnerabilities based on URLs, Hostnames, and API endpoints provided.

- e) Visa will promptly advise Supplier of any vulnerabilities identified. Supplier acknowledges that Critical and High severity vulnerabilities identified as part of the Bug Bounty program are time-sensitive and will require immediate action. Supplier shall cooperate with Visa, including but not limited to joining conference calls with Visa, to determine mitigation action(s) and remediation timeline(s). Medium, Low, and Very Low severity vulnerabilities must be remediated in accordance with the Visa Remediation Timeline. Supplier acknowledges that vulnerabilities must be remediated at its expense.

16. Mobile App Store. If Supplier develops and/or hosts mobile apps on behalf of Visa or a third-party doing business with Visa Mobile apps developed and/or hosted exclusively for Visa or Third-Party doing business with Visa must be hosted in Visa Approved App Stores ("**Approved App Stores**"). Visa may periodically update the Approved App Stores and shall communicate such changes to Supplier.

17. SBOM. Supplier will establish and maintain a complete and accurate inventory of software components, also known as software bill of materials (SBOM), containing at least the minimum SBOM elements prescribed by the U.S. Department of Commerce, including any open-source library or third-party software included in or embedded in software related to the delivery of the Services. Supplier will provide the SBOM in an industry-standard data format acceptable to Visa upon initiation of the Services and whenever there is a new release version.

18. Business Continuity. Supplier implements appropriate back-up and disaster recovery and business resumption plans to enable it to continue or resume providing Services (including restoring access to the Visa Data) in a timely manner after a disruptive event. These plans will include processes to enable recovery of any Visa Data that were modified or destroyed due to unauthorized access. Supplier will regularly test and monitor the effectiveness of its business continuity and disaster recovered plans. Upon request, Supplier will provide information about its business continuity and disaster recovery plans to Visa.

19. Supplier Security and Compliance Contact Information. Within seventy-two hours (72hrs) of executing this agreement, Supplier shall provide Visa with the following contact information in the format below. The information must be sent to ask3ptm@visa.com. Throughout the life of this agreement and for any surviving periods thereof, Supplier shall notify Visa of any change to the contact information, within seventy-two hours (72hrs) of such change.

Contact Type	Email Address	
Security Contact Information	[Please insert Supplier Security incident notification email address and/or Security contact's name and phone number. This should preferably be an email address that is 24/7 monitored by your Security Operations Center (SOC)].	Visa will use this information to notify Supplier of any suspected/actual security incidents, vulnerabilities, or threat intelligence, if applicable.
Compliance Contact Information	[Please insert Supplier compliance contact information, including Name and email address].	Visa will use this information to request compliance artifacts (e.g., SOC2, PCI Reports, etc.) and other inquires/requests noted in this Exhibit.