Supplier Security Policy

The Supplier Security Policy ("**Security Policy**") is hereby incorporated into the Purchase Order Terms and Conditions available at **https://www.appsflyer.com/gatedpdfs/pdfs/Purchase-Order-Online-Terms-and-Conditions.pdf**, or any other agreement with AppsFlyer which specifically refers to this Security Policy (the "**Terms**"). Unless expressly agreed otherwise in writing by the Parties, the terms of this Security Policy shall apply to the provision of Services by the Supplier to AppsFlyer under the Terms, if and to the extent applicable.

Capitalized terms not otherwise defined hereunder shall have the meaning ascribed to it under the Terms.

1) **General; Definitions**. At a minimum and as specified herein, in addition to the general requirements set forth in the Terms, Supplier shall provide security for all AppsFlyer's Data, networks and systems ("**AppsFlyer Property**") in support of the Terms. "**Confidential Information**" shall have the same meaning as set forth in the Terms and shall include any non-public AppsFlyer information including, but not limited to, technical processes and formulas, source codes, product designs, sales, cost and other unpublished financial information, product and related business plans, methods of operation, projections, marketing data, AppsFlyer's Data, AppsFlyer customer data, personal information, employee and employee candidate information and other non-public information.

2) **Security Measures**. Supplier's security measures shall in no event be less stringent than: (i) those used to safeguard Supplier's own confidential property; (ii), those used by other companies providing services similar to the Services (i.e., industry standard measures); and (iii) those required by applicable laws, rules and regulations (including those relating to personal information). Such security measures shall include, where appropriate, use of updated firewalls, virus screening software, encryption, intrusion detection systems, logging of incidents, periodic reporting, and prompt application of current security patches, virus definitions and other updates. Supplier shall promptly notify AppsFlyer if, during the term, Supplier modifies the Supplier system or its security measures in a manner that causes Supplier not to comply with the terms of tis Security Policy or otherwise provides a diminution in security to AppsFlyer Property. In no event shall Supplier make a change to its security measures regarding the Supplier system that result in such security measures being less stringent than those currently in effect and disclosed to AppsFlyer. Supplier shall document all such security measures and shall keep them current in light of changes in relevant technology. Supplier shall provide AppsFlyer with such information concerning its compliance with the foregoing as AppsFlyer may reasonably request. Without limiting the foregoing, AppsFlyer may terminate the Terms and/or any PO upon its determination, in its sole discretion, that Supplier's security measures fail to conform to the reasonable policies effectuated by AppsFlyer from time to time with respect to the security of AppsFlyer Property.

3) Without limiting the generality of the foregoing, Supplier's security efforts will include, but not be limited to:

   a) **Logical Access Controls:** Supplier agrees to employ effective logical access control measures over all systems used to create, transmit, or process AppsFlyer Confidential Information including but not limited to:

      i) User authentication must use unique identifiers ("**User ID's**") consistent with individual accountability.

      ii) A complex password policy, including the prohibition of clear-text credentials must be enforced. Passwords should only be known to their holders and should be changed every 90 days. There should be a lockout after 5 failed attempts.

      iii) User access rights/privileges to information resources containing AppsFlyer Confidential Information must be granted on a need-to-know basis consistent with role-based authorization.

      iv) User access to AppsFlyer Confidential Information must be removed immediately upon user separation or role transfer eliminating valid business need for continued access.

      v) Default passwords and security parameters must be changed in third-party products/applications used to support AppsFlyer Confidential Information.

      vi) Two-factor authentication such as token devices, smart cards, biometrics, or public keys shall be used to secure all remote access to AppsFlyer Confidential Information.

   b) **Network Security Architecture:** Supplier agrees to employ effective network security control measures over all systems used to create, transmit, store, or process AppsFlyer Confidential Information including but not limited to:

      i) Firewalls shall be operational at all times and shall be installed at the network perimeter between Supplier's internal (private) and public (Internet) networks.

      ii) Properly configured and monitored IDS/IPS (Intrusion Detection/Prevention Systems) must be used on Supplier's network.

iii) Databases must be logically or physically separated from the web server, and the database may not reside on the same host as the web server, where applicable.

iv) The database and other information systems used for the purposes of processing AppsFlyer Confidential Information must have only those services/processes and ports enabled to perform routine business. All other services/processes on the host must be disabled.

v) All network security control measures, databases and systems should generate logs. Those logs should be monitored and reviewed periodically.

vi) All information systems, repositories, etc. used for AppsFlyer by Supplier, or its business partners, must be physically located in a controlled data center environment used for the purpose of protecting information systems.

vii) Secure channels (e.g., SSL, SFTP, SSH, IPSEC, etc.) must be used at all times when transferring Confidential Information.

c) **Physical Access Controls:** Supplier agrees to maintain servers, databases, and other hardware and/or software components that store AppsFlyer Confidential Information, AppsFlyer Property or any other information related to AppsFlyer's business activities in an access controlled and consistently monitored data center secured by appropriate alarm systems, which will not be commingled with another unrelated party's hardware, software or information.

d) **Risk Assessment:** At no additional cost, Supplier agrees to provide true, correct and complete responses to a risk assessment questionnaire (if provided by AppsFlyer), participate in vulnerability scans of their network and/or application (upon notification).

i) Supplier agrees to perform regular security vulnerability assessments and shall provide AppsFlyer with results of a current security assessment by an accredited third-party (e.g., penetration test results of internet-facing devices, SAS 70-Type II reports, ISO 27001 certification, etc.) as well as action plans describing how Supplier will address all identified security vulnerabilities affecting systems used to store, process or otherwise access AppsFlyer Confidential Information.

ii) Supplier will permit AppsFlyer or its designee to conduct audits of Supplier's operations and security procedures as well as of any AppsFlyer data maintained or stored by the Supplier.

e) **Security Policy:** Supplier agrees to maintain and enforce security policies consistent with security best practices, and all applicable regulatory and legal security and privacy requirements. Upon request, Supplier shall provide a copy of its current security policy and standards as well as security architecture. Supplier shall comply with any AppsFlyer Privacy Policies with respect to any AppsFlyer customer personal information it receives.

f) **Vulnerability Management Controls:** Supplier agrees to employ effective vulnerability management control measures over all of its systems used to create, transmit, or process AppsFlyer Confidential Information, including; but, not limited to:

i) Third-party vulnerability scans or audits of any external-facing (public) infrastructure devices.

ii) Deploy and maintain currency of up-to-date commercially available anti-virus, anti-spam, anti-malware software on all information system components including personal computers, laptops, and interconnecting networks, where applicable, used for the purpose of managing AppsFlyer Confidential Information. Additionally, provide for regular scanning for viral infections and update virus signature files frequently.

iii) Maintain a standard patch management process and practice to ensure the protection of any devices used to access, process or store AppsFlyer Confidential Information. Supplier agrees to provide AppsFlyer with their patch management policies and procedures upon request.

iv) Regular auditing and monitoring to ensure the protection of AppsFlyer Confidential Information and AppsFlyer Property.

v) Any security breach that involves AppsFlyer Confidential Information or AppsFlyer Property must be reported to AppsFlyer without unreasonable delay. Supplier shall immediately perform a root cause analysis as well as provide detailed information about measures taken by the Supplier to prevent future breaches. All efforts to rectify or resolve the situation must include subsequent and regular notification for the reported incident.

vi) Within one (1) hour of suspected fraudulent or malicious activity occurring on the Supplier site, Supplier will notify AppsFlyer's security director by phone at +972549249922 to inform the AppsFlyer team about the

activity. Any request by the AppsFlyer team for such information will be provided to AppsFlyer within two (2) hours.

vii) Supplier agrees to provide full cooperation with AppsFlyer and in the event of a data breach involving AppsFlyer Confidential Information or AppsFlyer Property including, but not limited to, server log information showing network and application traffic.

viii) AppsFlyer must be immediately notified of any known attacks occurring against Supplier systems used to store or process AppsFlyer Confidential Information.

ix) Vulnerabilities discovered by the AppsFlyer's or Supplier's Security Scanning tools must be resolved by following the schedule outlined below (the level of vulnerability will be determined by AppsFlyer):

(1) P1 vulnerabilities: A successful exploit of this vulnerability may result in catastrophic and significant physical or property damage or loss, or there may be a catastrophic and significant loss of revenue or productivity (e.g., Denial of Service Attack, exploit 'kits' exist, buffer overflows high jacking, or source code exposure, etc.). Such vulnerability must be resolved before a site launch or within two (2) hours of discovery if the application is currently publicly available.

(2) P2 vulnerabilities: A successful exploit of this vulnerability may result in moderate physical or property damage, or there may be a moderate loss of revenue or productivity to the organization (e.g., Weak encryption, or possible phishing opportunity, etc.). Such vulnerability must be resolved within two (2) days of site launch or within four (4) hours of discovery if the application is currently publicly available.

(3) P3 vulnerabilities: A successful exploit of this vulnerability may result in minor physical or property damage, or there may be a minor loss of revenue or productivity to the organization (e.g., FTP use or missing service pack, etc.). Such vulnerability must be resolved within three (3) days of a site launch or within eight (8) hours of discovery if the application is currently publicly available.

g) **Data Recovery and Availability:** Supplier must provide detailed disaster recovery and business continuity plans that support the pre-defined recovery time objective (RTO) / recovery point objective (RPO) requirements defined by AppsFlyer:

i) Supplier must utilize industry best practices for data, services, and communications recoverability. Data and applications must be replicated across multiple independent sites and alternate communication channels must be available.

ii) Supplier is expected to validate and verify their existing capabilities through realistic scenario testing. Supplier must agree to participate in periodic recovery testing with AppsFlyer. Proof of successful testing of the Supplier plan must be provided to AppsFlyer upon request.

iii) Supplier must provide company name, address, and contact information on all third-party relationships as well as services provided by each wherever those services create, transmit or process AppsFlyer Confidential Information.

iv) Backups shall be performed regularly and shall be saved in a secured and locked location with access only to limited employees of Supplier as required.

h) **Data Destruction:** Supplier shall ensure that residual magnetic, optical, or electrical representation of AppsFlyer Confidential Information that has been deleted may not be retrieved or reconstructed when storage media is transferred, become obsolete or is no longer usable or required by AppsFlyer and shall certify such destruction to AppsFlyer as provided in the Terms.

i) Supplier should be utilizing minimum 256-bit private key encryption or 2048-bit public key encryption that renders data unreadable when storage is recycled, disposed of, or accessed by any means outside of authorized applications. Key knowledge should be limited to authorized personnel and retirement or replacement of encryption keys included in key management procedures when the integrity of the key has been weakened (such as departure of an employee with key knowledge) or keys are suspected of being compromised.

ii) Supplier data retention and destruction must align with AppsFlyer requirements and policies as provided to Supplier (as updated by AppsFlyer from time to time) as well as comply with applicable laws or regulations.

iii) AppsFlyer information stored on Supplier media (e.g., hard drive, optical discs, tapes, paper, etc.) must be rendered unreadable or unattainable using the NIST Guidelines for Media Sanitization (Special Pub 800-88), prior to the media being recycled, disposed of, or moved off-site.

i) **Application Supplier:** Supplier agrees to adhere to the following controls surrounding application development for applications developed and hosted off-site as well as off-site application development for on-site deployment:

   i) Supplier must provide supporting documentation that commonly accepted web application security guidelines and frameworks are used for developing Internet-facing applications (e.g. Open Web Application Security Project [OWASP], SANS).

   ii) Supplier must provide a data flow diagram that includes the entry points (the main pages and the i-framed pages as may be applicable), a description of the data flowing from each node in the system (e.g., username, password, address, captcha, etc.), a listing of all attributes stored, processed, or transmitted, and how the data is securely stored. The diagram must also demonstrate all security controls in place.

   iii) Supplier must demonstrate how Internet-facing applications are tested for security vulnerabilities and remediated prior to the source code being promoted to production.

   iv) If Supplier has performed prior security testing, the results of such testing must be made available to AppsFlyer for evaluation prior to launch. If Supplier has not performed such testing, Supplier shall allow penetration/vulnerability testing and/or application source code review to be performed by AppsFlyer, when requested.

   v) Supplier must provide supporting documentation describing how fraud is detected and prevented when requested by AppsFlyer.

   vi) Supplier agrees to supply, within the requested timeframe, detailed information, and demonstrate full cooperation with AppsFlyer, pertaining to all inquiries deemed necessary by AppsFlyer to determine the risk of any third-party systems and procedures related to and affecting AppsFlyer. This includes, but is not be limited to, inquiries pertaining to servers, server logs showing detailed application traffic, operating systems, applications, databases, network configuration, data encryption algorithms being utilized, fraud detection and prevention controls, physical inspection of facilities, incident response procedures, and disaster recovery measures.

   vii) Supplier agrees to allow all relevant sites to be monitored by AppsFlyer or a third-party for availability and performance.

j) **Personnel Roles and Responsibilities:** Supplier agrees to identify in writing the person who will be responsible for overall security of the Services and/or Deliverables. The person identified shall be a single senior technical security specialist, to be known as the project Security Lead. The Security Lead shall confirm in writing the security of each Deliverable. The Security Lead shall confirm to AppsFlyer in writing that the Services and/or Deliverables meets the security requirements, all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the confirmation status must be fully documented.