Data Protection Policy

The Data Protection Policy (**"DPP"**) governs the ~~treatment (e.g.,~~ receipt, storage, usage, transfer, and ~~disposition)~~disposal of the data vended and retrieved through the ~~Marketplace~~Amazon Selling Partner APIs (including the Marketplace Web Service APIs). This policy is applicable to all systems that store, process, or otherwise handle data vended and retrieved from the Selling Partner APIs. This Policy supplements the Amazon ~~Marketplace~~Selling Partner API Developer Agreement and the Acceptable Use Policy. Failure to comply may result in suspension or termination of ~~Marketplace~~Selling Partner API access.

~~**Definitions**~~

~~**"Application"** means a software application or website that interfaces with the Marketplace APIs.~~

~~**"Amazon Information"** means any information that is exposed by Amazon through the Marketplace APIs, Seller Central, or Amazon's public-facing websites. This data can be public or non-public, including Personally Identifiable Information about Amazon customers.~~

~~**"Customer"** means any person or entity who has purchased items or services from Amazon's public-facing websites.~~

~~**"Developer"** means any person or entity (including you, if applicable) that uses the Marketplace APIs for the purpose of integrating or enhancing a third-party Seller's systems with the features and functionality permitted by Amazon to be accessed through the Marketplace APIs.~~

~~**"Personally Identifiable Information" ("PII")** means information that can be used on its own or with other information to identify, contact, or locate an individual (e.g., Customer or Seller), or to identify an individual in context. This includes, but is not limited to, a Customer or Seller's name, address, e-mail address, phone number, gift message content, survey responses, payment details, purchases, cookies, digital fingerprint (e.g., browser, user device), IP Address, geo-location, or Internet-connected device product identifier.~~

~~**"Security Incident"** means any actual or suspected unauthorized access, collection, acquisition, use, transmission, disclosure, corruption, or loss of Amazon Information, or breach of any environment (i) containing Amazon Information, or (ii) managed by a Developer with controls substantially similar to those protecting Amazon Information.~~

~~**"Seller"** means any person or entity (including you, if applicable) selling on Amazon's public-facing websites.~~

1. General Security Requirements

Consistent with industry-leading security standards ~~and other requirements specified by Amazon based on the classification and sensitivity of Amazon Information~~, Developers will maintain physical, administrative, and technical safeguards, and other security measures (i) to maintain the security and confidentiality of ~~Amazon~~ Information accessed, collected, used, stored, or transmitted by a Developer, and (ii) to protect ~~that information~~this Information from known or reasonably anticipated threats or hazards to its security and integrity, accidental loss, alteration, disclosure, and all other unlawful forms of processing. Without limitation, the Developer will comply with the following requirements:

1.1 ~~1.~~ **Network Protection.** Developers must implement network protection controls ~~(e.g., AWS VPC subnet/Security Groups,~~including network firewalls~~)~~, network access control lists to deny access to unauthorized IP addresses ~~and public access must be restricted~~. Developers must implement anti-virus and anti-malware software on end-user devices. Developers must restrict public access only to approved users.

1.2 ~~2.~~ **Access Management.** Developers must assign a unique ID to each person with computer access to ~~Amazon~~ Information. Developers must not create or use generic, shared, or default login credentials or user accounts. Developers must implement baselining mechanisms to ensure that at all times only the required user accounts access ~~Amazon~~ Information. Developers must review the list of people and services with access to ~~Amazon~~ Information ~~on a regular basis (~~at least ~~quarterly)~~every 90 days, and remove accounts that no longer require access. Developers must restrict ~~developer~~ employees and contractors from storing ~~Amazon data~~Information on personal devices. Developers

will maintain and enforce "account lockout" by detecting anomalous usage patterns and log-in attempts, and disabling accounts with access to ~~Amazon~~ Information as needed.

1.3 **Least Privilege Principle**. Developers must implement fine-grained access control mechanisms to allow granting rights to any party using the Application and the Application's operators following the principle of least privilege. Access to Information must be granted on a "need-to-know" basis.

1.4 **Password Management.** Developers must establish minimum password requirements for personnel and systems with access to Information. Password requirements must be a minimum of 8 characters, contain upper and lower case letters, contain numbers, contain special characters, and rotated at least quarterly.

1.5 ~~**3.**~~ **Encryption in Transit.** Developers must encrypt all ~~Amazon~~ Information in transit ~~(e.g., when the data traverses a network, or is otherwise sent between hosts. This can be accomplished using HTTP over TLS (HTTPS).~~ with secure protocols such as TLS 1.2+, SFTP, and SSH-2. Developers must enforce this security control on all applicable internal and external endpoints ~~used by customers as well as internal communication channels (e.g., data propagation channels among storage layer nodes, connections to external dependencies) and operational tooling. Developers must disable communication channels which do not provide encryption in transit even if unused (e.g., removing the related dead code, configuring dependencies only with encrypted channels, and restricting access credentials to use of encrypted channels)~~. Developers must use data message-level ~~encryption (e.g., using AWS Encryption SDK)~~ where channel encryption (e.g., using TLS) terminates in untrusted multi-tenant hardware (e.g., untrusted proxies).

1.6 ~~**4.**~~ **Incident Response Plan.** Developers must create and maintain a plan and/or runbook to detect and handle Security Incidents. Such plans must identify the incident response roles and responsibilities, define incident types that may impact Amazon, define incident response procedures for defined incident types, and define an escalation path and procedures to escalate Security Incidents to Amazon. Developers must review and verify the plan every six (6) months and after any major infrastructure or system change, including changes to the system, controls, operational environments, risk levels, and supply chain. Developers must notify Amazon (via email to 3p-security@amazon.com) within 24 hours of detecting Security Incident or **suspecting** that a Security Incident has occurred. Developers must investigate each Security Incident, and document the incident description, remediation actions, and associated corrective process/system controls implemented to prevent future recurrence ~~(if applicable)~~. Developers must maintain the chain of custody for all evidences or records collected, and such documentation must be made available to Amazon ~~on~~upon request ~~(if applicable).Developers must inform Amazon (via email to 3p-security@amazon.com) within 24 hours of detecting any Security Incidents.~~ If a Security Incident occurred, Developers cannot ~~notify~~represent or speak on behalf of Amazon to any regulatory authority~~, nor any customer, on behalf of Amazon~~ or customers unless Amazon specifically requests in writing that the Developer do so. ~~Amazon reserves the right to review and approve the form and content of any notification before it is provided to any party, unless such notification is required by law, in which case Amazon reserves the right to review the form and content of any notification before it is provided to any party. Developers must inform Amazon within 24 hours when their data is being sought in response to legal process or by applicable law.~~

1.7 ~~**5.**~~ **Request for Deletion or Return.** Developers must ~~promptly (but within no more than 72 hours after Amazon's request),~~ permanently~~,~~ and securely delete ~~(in accordance with industry-standard sanitization processes, e.g., NIST 800-88)~~ or return ~~Amazon~~ Information upon and in accordance with Amazon's notice requiring deletion ~~and/~~or return~~.~~ within 72 hours of Amazon's requests unless the data is required to comply with law. Secure deletion must occur in accordance with industry-standard sanitization processes such as NIST 800-88. Developers must also permanently and securely delete all live (online or network accessible) instances of ~~Amazon~~ Information ~~within~~ 90 days after Amazon's notice. If requested by Amazon, the Developer will certify in writing that all ~~Amazon~~ Information has been securely destroyed.

2. Additional Security Requirements Specific to Personally Identifiable Information

The following additional Security Requirements must be met for ~~all~~ Personally Identifiable Information (~~"PII") (see PII definition in Section 1~~PII). PII is granted to ~~MWS developers~~Developers for select tax and merchant fulfilled shipping purposes, on a must-have basis. If a ~~Marketplace~~Selling Partner API contains PII, or PII is combined with non-PII, then the entire data store must comply with the following requirements:

2.1 ~~**1.**~~ **Data Retention ~~and Recovery~~.** Developers will retain PII for no longer than 30 days after order delivery and only for the purpose of~~,~~ and as long as is necessary to (i) fulfill orders ~~(no longer than 30 days after order shipment), or to~~, (ii) calculate~~/~~ and remit taxes, and (iii) produce tax invoices. If a Developer is required by law to retain archival copies of PII for tax or similar regulatory purposes, ~~this archived Amazon Information~~PII must be stored as a "cold" or offline encrypted backup (e.g., not available for immediate or interactive use) ~~backup stored in a physically secure facility,~~

and all archived data on backup media must be encrypted. In the event that PII is lost, you must be able to recover all PII lost (i.e., the data is erased or unavailable for processing due to system crash or ransomware).

2.2 2. **Data Governance.** Developers must create, document, and abide by a privacy and data handling policy for their Applications or services which govern the appropriate conduct and technical controls to be applied in managing and protecting information assets. Developers must keep inventory of software and physical assets (e.g. computers, mobile devices) with access to PII, and update regularly. A record of data processing activities such as specific data fields and how they are collected, processed, stored, used, shared, and disposed for all PII Information should be maintained to establish accountability and compliance with regulations. Developers must establish a process to detect and comply with privacy and security laws and regulatory requirements applicable to their business and retain documented evidence of their compliance. Developers must establish and abide by their privacy policy for customer consent and data rights to access, rectify, erase, or stop sharing/processing their information where applicable or required by data privacy regulation.

2.3 **Asset Management.** Developers must keep inventory of software and physical assets (e.g. computers, mobile devices) with access to PII, and update quarterly. Physical assets that store, process, or otherwise handle Amazon PII must abide by all of the requirements set forth in this policy. Developers must not store PII in removable media, personal devices, or unsecured public cloud applications (e.g., public links made available through Google Drive) unless it is encrypted using at least AES-128 or RSA-2048 bit keys or higher. Developers must securely dispose of any printed documents containing PII.

2.4 3. **Encryption and Storageat Rest.** Developers must encrypt all PII at rest (e.g., when the data is persisted) using industry best practice standards (e.g. using either AES-128, AES-256,using at least AES-128 or RSA with 2048-bit key size (or higher). The cryptographic materials (e.g., encryption/decryption keys) and cryptographic capabilities (e.g., daemons implementing virtual Trusted Platform Modules and providing encryption/decryption APIs) used for encryption of PII at rest must be only accessible to the Developer's processes and services. Developers must not store PII in removable media (e.g., USB) or unsecured public cloud applications (e.g., public links made available through Google Drive). Developers must securely dispose of any printed documents containing PII.

2.5 **Secure Coding Practices.** Developers must not hardcode sensitive credentials in their code, including encryption keys, secret access keys, or passwords. Sensitive credentials must not be exposed in public code repositories. Developers must maintain separate test and production environments.

4. **Least Privilege Principle.** Developers must implement fine-grained access control mechanisms to allow granting rights to any party using the Application (e.g., access to a specific set of data at its custody) and the Application's operators (e.g., access to specific configuration and maintenance APIs such as kill switches) following the principle of least privilege. Application sections or features that vend PII must be protected under a unique access role, and access should be granted on a "need-to-know" basis.

2.6 5. **Logging and Monitoring.** Developers must gather logs to detect security-related events (e.g., access and authorization, intrusion attempts, configuration changes) to their Applications and systems, including success or failure of the event, date and time, access attempts, data changes, and system errors Developers must implement this logging mechanism on all channels (e.g., service APIs, storage-layer APIs, administrative dashboards) providing access to Amazon Information. All logs must have access controls to prevent any unauthorized access and tampering throughout their lifecycle. Logs themselves shouldmust not contain PII and must be retained for at least 90 days for reference in the case of a Security Incident. Developers must build mechanisms to monitor the logs and all system activities to trigger investigative alarms on suspicious actions (e.g., multiple unauthorized calls, unexpected request rate and data retrieval volume, and access to canary data records). Developers must implement monitoring alarms to detect if Information is extracted from its protected boundaries. Developers should perform investigation when monitoring alarms are triggered, and this should be documented in the Developer's Incident Response Plan.

2.7 **Vulnerability Management**. Developers must create and maintain a plan and/or runbook to detect and remediate vulnerabilities. Developers must protect physical hardware containing PII from technical vulnerabilities by performing vulnerability scans and remediating appropriately. Developers must conduct vulnerability scanning or penetration tests at least every 180 days and scan code for vulnerabilities prior to each release. Furthermore, Developers must control changes to the storage hardware by testing, verifying changes, approving changes, and restricting access to who may perform those actions.

3. Audit and Assessment

Developers must maintain all appropriate books and records reasonably required to verify compliance with the Acceptable Use Policy, Data Protection Policy, and Amazon Marketplace Developer Agreement during the period of this agreement and for 12 months thereafter. Upon Amazon's written request, Developers must certify in writing to Amazon that they are in compliance with these policies.

Upon request, Amazon may, or may have an independent certified public accounting firm selected by Amazon, audit, assess and inspect the books, records, facilities, operations, and security of all systems that are involved with a Developer's application in the retrieval, storage, or processing of ~~Amazon~~ Information. Developers must cooperate with Amazon or Amazon's auditor in connection with the audit or assessment, which may occur at the Developer's facilities and/or subcontractor facilities. If the audit or assessment reveals deficiencies, breaches, and/or failures to comply with our terms, conditions, or policies, the Developer must, at its sole cost and expense, and take all actions necessary to remediate those deficiencies within an agreed-upon timeframe. Upon request, Developer must provide remediation evidence in the form requested by Amazon (which may include policy, documents, screenshots, or screen sharing of application or infrastructure changes) and obtain written approval on submitted evidence from Amazon before audit closure.

4. Definitions

"Application" means a software application or website that interfaces with the Marketplace APIs.

"Customer" means any person or entity who has purchased items or services from Amazon's public-facing websites.

"Developer" means any person or entity (including you, if applicable) that uses the Marketplace APIs for the purpose of integrating or enhancing a third-party Selling Partner's systems with the features and functionality permitted by Amazon to be accessed through the Marketplace APIs.

"Information" means any information that is exposed through the Selling Partner APIs, Amazon Portals, or Amazon's public-facing websites. This data can be public or non-public, including Personally Identifiable Information about Amazon customers.

"Personally Identifiable Information" ("PII") means information that can be used on its own or with other information to identify, contact, identify in context, or locate an Amazon , Customer or Selling Partner. This includes, but is not limited to, a Customer or Selling Partner's name, address, e-mail address, phone number, gift message content, survey responses, payment details, purchases, cookies, digital fingerprint (e.g., browser, user device), IP Address, geo-location, nine-digit postal code, or Internet-connected device product identifier.

"Security Incident" means any actual or suspected unauthorized access, collection, acquisition, use, transmission, disclosure, corruption, or loss of Information, or breach of any environment (i) containing Information, or (ii) managed by a Developer with controls substantially similar to those protecting Information.

"**Selling Partner**" means any person or entity (including you, if applicable) that is participating in one or more of the Amazon Selling Partner Services.

"Selling Partner APIs" means any application programming interface (API) offered by Amazon for the purpose of helping Amazon sellers to programmatically exchange data including but not limited to, listings, orders, payments, and reports.

"**Selling Partner Services**" means services provided or operated by Amazon that allow, enable, or assist a party to sell goods or services either to Amazon or in Amazon's online or offline stores.