BEST BUY MARKETPLACE
SELLER PRIVACY AND SECURITY REQUIREMENTS

I. Purpose and Overview.

Best Buy and Seller have entered into a Marketplace Seller Agreement. These Requirements establish Seller's obligations with respect to Best Buy Data and Best Buy Systems arising thereunder. These Requirements survive termination of any agreement between Best Buy and Seller to the extent that Seller Processes or has access to Best Buy Data or Best Buy Systems.

II. Defined Terms and Interpretation.

A. Defined Terms.

1. Agreement. The Marketplace Seller Agreement.

2. Best Buy. Best Buy Purchasing LLC and its parent, subsidiaries, and affiliates.

3. Best Buy Data. Data that is uploaded, submitted, posted, transferred, transmitted, collected, or otherwise provided to or received by Seller, including but not limited to Customer Information, Order Information, and employee Personal Information in performance of the Agreement. Derivative works of, based on, derived from or otherwise using any Best Buy Data are themselves also Best Buy Data.

4. Best Buy Systems. Computer systems, applications, or networks which are owned, leased, licensed, or otherwise used by Best Buy.

5. CCPA. The California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 *et seq*., as amended from time to time.

6. Cross-Context Behavioral Advertising means the targeting of advertising to a consumer based on the consumer's Personal Information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts.

7. Data Incident. Each of the following is deemed a Data Incident:

   a) a breach of security of Seller's systems that contain Best Buy Data or interface with Best Buy Systems (including without limitation ransomware incidents); or

   b) an incident involving actual or reasonably suspected unauthorized access to or acquisition, use, disclosure, modification, or destruction of Best Buy Data or Best Buy Systems; or

   c) Seller's violation of any applicable law, rule, regulation, ordinance, or industry standard which impacts the privacy or security of Best Buy Data, Best Buy Systems, or Seller Systems which process Best Buy Data.

   External pings and other broadcast attacks on Seller's firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any similar routine attempts or any combination of the above, will not be a Data Incident so long as the attempt does not impact the privacy or security of Best Buy Data, Best Buy Systems, or Seller Systems.

8. Data Protection Laws means all data protection and privacy laws applicable to the respective party in its role in Processing Personal Information under the Agreement including, but not limited to, the CCPA.

9. Personal Information. Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

10. Process, Processes, Processed or Processing. Accessing, using, collecting, creating, receiving, hosting, maintaining, modifying or altering, storing, transmitting, or destroying Best Buy Data.

11. Sell. Has the meaning given to it in the CCPA or other Data Protection Laws.

12. Share. Sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Information about a consumer by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

13. Third-Party Provider. All Seller's contractors, subcontractors, sub-processors and other third parties that may receive or access Best Buy Data, Best Buy Systems and/or Best Buy assets as a representative of or on behalf of Seller (including without limitation cloud hosting providers and payment processors). For purposes of clarity, Seller is responsible for ensuring its Third-Party Providers have substantially similar security and privacy controls and policies as those set forth herein.

14. Seller. The party other than Best Buy subject to these Requirements and the Agreement.

15. Seller Systems. Computer systems or networks owned, leased, licensed, or otherwise used by Seller or Seller's Third-Party Providers.

B. All capitalized terms used herein and not otherwise defined shall have the meanings assigned to such terms in the Marketplace Seller Agreement.

C. **Order of Precedence.** In the event of any conflict between information privacy, security, insurance standards, or any other obligations in the Marketplace Seller Agreement and herein, the conflict will be interpreted to provide the greatest privacy and security protections to Best Buy Systems and Best Buy Data.

III. Suspension of Access.

Seller's access to any Best Buy Data and/or Best Buy Systems is subject to Seller's continuing compliance with these Requirements. To protect the privacy, confidentiality, integrity, and availability of Best Buy Data and Best Buy Systems, or in the event of Data Incident, Best Buy may immediately, automatically, and unconditionally suspend Seller's access, and all links and interfaces, to Best Buy Data and/or Best Buy Systems (including terminating transmission of Best Buy Data to Seller) without liability. Best Buy acknowledges that the inability of Seller to access Best Buy Data and/or Best Buy Systems may result in Seller's inability to fulfill its obligations set forth in the Agreement, and that inability, alone, based on Best Buy's suspension of access, will not be considered a cause for termination by Best Buy, to the extent based on Best Buy's suspension of the access.

IV. Information Retention, Return, and/or Disposal.

Seller will retain Best Buy Data for no longer than sixty (60) days after fulfilling a customer purchase, only for the purpose of Processing permitted under the Agreement and these Requirements, and as long as necessary to meet Seller obligations under the Agreement. Notwithstanding the foregoing, Seller may retain Best Buy Data (i) for as long as strictly necessary for Seller to meet legal compliance obligations or (ii) in backup media/systems, each subject to a written and implemented records-retention program consistent with industry standards.

Upon request by Best Buy, Seller will certify that Seller has completely and permanently destroyed electronic copies of all Best Buy Data, rendering it no longer usable, readable, decipherable and retrievable or identify the permitted purpose for which data is retained and its intended retention period.

V. Assessment of Security Controls.

A. **Best Buy Assessment.** In addition to assessment rights set forth in the Agreement, Best Buy, either directly or via its representatives, may assess the security and privacy posture of Seller in a manner that reasonably minimizes interference with Seller's business operations. Completion of this evaluation does not constitute a waiver of any of Best Buy's rights or Seller's obligations under the Agreement(s). Best Buy's assessment may include the following:

1. Third-Party Risk Assessment (TPRA). Upon Best Buy's request at any time, Seller will complete and return Best Buy's Third-Party Risk Assessment, in the form of an electronic questionnaire, in a complete, accurate, and timely manner.

2. Audit for Reasonable Cause. If Best Buy in good faith believes Seller is in violation of these Requirements, or a Data Incident occurs, Best Buy reserves the right to require an audit conducted by Best Buy or an independent third party. Seller will provide all reasonable assistance requested by or on behalf of Best Buy in such audit.

B. **Remediation.** To the extent that any deficiencies are identified in any of the foregoing reviews or audits, Seller will remedy critical deficiencies within thirty (30) days and remedy all other deficiencies within a reasonable period based upon the nature of the deficiency and the risks arising therefrom.

VI. Minimum Security Terms.

Seller must, at a minimum, implement and maintain information security controls that meet industry standards (such as NIST Cybersecurity Framework (CSF), NIST SP:800-53, ISO 27001 (including 27002 controls)) and are appropriately scaled and tailored to the size and complexity of Seller's business. These security controls will apply to Seller and Seller's Systems to the extent they Process Best Buy Data and access Best Buy Systems and shall include, but not necessarily be limited to, the following:

A. **Information Security Program.** Seller must have a formal and comprehensive information privacy and security program ("Program"), including policies and governance, which meets or exceeds industry standards and applicable regulations and is designed to protect the privacy, confidentiality, integrity, and availability of Best Buy Data and Best Buy Systems. Seller will do at least the following:

1. Governance. Designate a person responsible for overall Program oversight. Annually review the Program for gaps, continued alignment to industry standards, and to ensure the Program addresses evolving threats.

2. Training. Provide annual training for all Seller employees and contractors performing services and support for Best Buy, as relevant to job responsibilities, on the Program and relevant information security and privacy topics (e.g., phishing, malware, social engineering attacks).

B. **Asset Management.** Seller must manage resources through a secure asset lifecycle to protect the privacy, confidentiality, integrity, and availability of Best Buy Data. Seller will, at a minimum, adhere to the following requirements:

1. Responsibility for Assets. Identify and assign ownership of assets used to Process Best Buy Data. Protect such assets in accordance with then-current industry standards.

2. Asset Handling. When accessing Best Buy Data: limit access to electronic and hard copy assets to personnel with a legitimate business need, securely handle all electronic or hard-copy assets at all times, secure all assets when left unattended, and protect assets from environmental exposure.

3. Asset Disposal. Implement procedures (meeting or exceeding then-current NIST or other appropriate industry standards) for the secure sanitization and disposal of assets. Sanitize all assets containing Best Buy Data prior to disposal. Dispose of assets in a manner that ensures the information or information resources cannot be reconstructed to be usable, readable, decipherable, or retrievable.

C. **Workforce Security.** Seller must implement controls to enable employees and all Third-Party Providers to adhere to policies and standards to reduce the risk of theft, fraud, loss, and misuse of information, systems, and facilities. Seller shall, at a minimum:

1. Roles and Responsibilities. Ensure employees understand their responsibilities and are suitable for the roles for which they are considered (including using appropriate background checks/personnel screening). Equip employees and Third-Party Providers to adequately support the Program and to reduce human error. Track initial and recurring annual training of employees as appropriate to their role and responsibilities.

2. Policy Violations. Implement and maintain procedures to promptly remove access to Best Buy Data and Best Buy Systems for employees and Third-Party Providers who violate policies and standards.

D. **Physical and Environmental Security.** Seller must implement, manage, and review appropriate physical controls to prevent unauthorized physical access, damage, and interference to information, infrastructure, and equipment.

E. **Program Operations.** Seller must securely operate Seller Systems which Process Best Buy Data through the application of key operational management controls. Seller shall, at a minimum:

1. Operating Procedures. Document procedures for operational activities associated with information resources. Restrict access to documented procedures to a need-to-know basis.

2. Harmful Code or Messages. Employ then-current industry standard anti-virus, anti-malware, and anti-phishing software to screen its systems, messages, servers, and environment to prevent receipt and dissemination of viruses, worms, Trojan horses, malware, spyware, ransomware, key loggers, phishing, social engineering, and other harmful, disabling, or malicious computer code, files, links, content, scripts, messages, agents, or programs.

3. Patching. Implement processes and procedures that patch systems according to industry standard patching guidelines. Seller shall implement a patch or fix in a timely manner commensurate with the level of risk.

4. Vulnerability Scanning. Routinely perform vulnerability scanning of Seller's internet-facing applications, sites and services, and Seller's network where Best Buy Data may be located. Document and manage vulnerability scanning findings and remediate issues within a reasonable timeframe.

5. Configuration Management. Establish and follow baseline standards to consistently apply security configurations to secure information resources. Security baselines must disable, restrict, or secure unnecessary functions, services, utilities, and commands.

F. **Communications.** Seller will use secure mechanisms for all communications containing Best Buy Data. Seller will authenticate and log web browsing activities, allowing access to trusted websites and blocking malicious ones.

G. **Security Monitoring.** Seller will maintain a security monitoring program. Seller shall, at a minimum:

1. Logging and Monitoring. Leverage appropriate network and endpoint-based controls to facilitate security logging and monitoring of the use of privileged credentials, user activities, exceptions, faults, firewall activity, systems alerts, events, and internal and external communications. Regularly analyze, review, report, and archive collected logs and associated analysis.

2. Network Monitoring. Deploy, maintain, and monitor industry standard network monitoring capabilities (such as intrusion detection systems, intrusion protection systems, and network behavior monitoring) for detecting potential network intrusions and inappropriate activities.

3. Data Loss Prevention. Monitor for and implement controls to prevent unauthorized data exfiltration.

H. **Data Incident Notification & Response.** Seller shall, at a minimum:

1. Incident Response Plan. Create, document, and routinely test an incident response plan. Seller will follow documented responsibilities and procedures to efficiently respond to information security incidents. Upon Best Buy's request, Seller will allow Best Buy to review its incident response plan.

2. Notify Best Buy. Promptly (but not later than forty-eight (48) hours of becoming aware) notify Best Buy of a Data Incident via email to: OfficeofTheCISO@bestbuy.com

   NOTE: Best Buy retains all right, title, and interest to Best Buy's Information. Except as required by law, or as mutually agreed on by the parties in writing by an authorized representative, Seller will not directly contact or notify Best Buy's customers of any Data Incident without Best Buy's prior written approval.

3. Investigate Incidents. Investigate all incidents and provide Best Buy ongoing written reports detailing the known facts of the Data Incident, continuing to provide such reports until Seller and Best Buy agree the incident should be considered closed; and prevent reoccurrence of the Data Incident.

4. Cooperation. Fully cooperate with any investigations, reviews, audits, or assessments of any Data Incidents requested by Best Buy, financial institutions, law enforcement, and/or credit card brand organizations.
5. In addition to any other remedies afforded Best Buy in equity or at law Seller will reimburse Best Buy for its actual and reasonable expenses and costs in connection with a Data Incident, including without limitation:

    a) investigation costs and expenses (including without limitation third-party forensic costs),
    b) data breach notification costs (including without limitation costs relating to email notifications, letters and postage, data incident website, and call center support services),
    c) costs of obtaining third-party identity theft and credit monitoring services for up to two years from a service provider selected by Best Buy,
    d) any applicable damages, judgments, fines, and/or penalties, and
    e) reasonable attorneys' fees and court costs.

I. **Access Controls.** Seller will regulate access to Best Buy Data and Best Buy Systems through security access controls and robust authorization mechanisms. Seller shall, at a minimum:

1. Policies and Procedures. Document and routinely perform access procedures that control user onboarding and access to Best Buy Data and Best Buy Systems.

2. Minimum Access Necessary. Minimize access to information on a need-to-know basis. Additionally, minimize privileged access to Best Buy Systems and Best Buy Data (examples of privileged access users are data base administrators and system administrators). Privileged access accounts must be managed using a password management tool.

3. Authentication. Maintain and enforce a strong password policy(ies) which addresses password length, complexity, lockout, history, and expiration. Employ two-factor (or better) authentication and device-based authentication for access to Seller Systems (e.g. VPN) accessible from the public internet to ensure each user is properly authenticated.

J. **Managing Access to Best Buy Systems.** Seller will appoint a Seller Security Administrator ("SSA") responsible for managing the access of all Seller users of Best Buy Systems. In the event an SSA leaves, the Seller must appoint a replacement prior to or within one (1) business day of their departure.

1. SSA Responsibilities. Seller must ensure SSA:

    a) reviews user access no less frequently than every ninety (90) days for accuracy,
    b) provisions access based on least privileged access principles,
    c) de-provisions user access within twenty-four (24) hours of user status change (e.g. termination, change in job role) or, if revocation of access is managed by Best Buy, Seller will notify Best Buy within twenty-four (24) hours of termination, and
    d) completes any training(s) provided by Best Buy on SSA responsibilities including, without limitation, trainings posted on Best Buy's Seller Hub.

K. **End User Devices.** Seller will implement security requirements for end-user devices (laptops, mobile devices, etc.). Seller shall, at a minimum:

1. Device Configuration and Implementation. Use mobile device and/or mobile application management solution(s) to protect Best Buy Data and meet industry standards.

2. Device Administration. Document and maintain an inventory of all deployed company-owned devices. Obtain and sanitize devices (including mobile devices, laptops, etc.) containing Best Buy Data within seven (7) days of termination of an employee or contractor, unless otherwise instructed or such action is prohibited by law.

3. Acceptable Use. Maintain policies and procedures describing the appropriate use of information systems being used by end user devices. Review, reaffirm, and communicate all such policies and procedures at least annually.

L. **Network Security.** Seller must leverage network specific information security controls to protect Best Buy Data and assets that traverse the Seller's network. Seller shall, at a minimum implement network segmentation, and intrusion detection and prevention mechanisms. Sellers shall appropriately employ, securely configure, and regularly update and test enterprise-wide firewall infrastructure to restrict access to and from untrusted networks and minimize access to extent needed to perform services.

M. **Third-Party Security.** Seller will manage Third-Party Providers to ensure the privacy, confidentiality, integrity, and availability of Best Buy Data and Systems. Seller will oversee and review these providers for risks and compliance, enter into written agreements to maintain confidentiality and security of Best Buy Data and Systems, document and reasonably ensure remediation of Third-Party issues, and notify Best Buy of any new or replacement providers. Best Buy may object to changes to providers within 30 business days, and unresolved objections may lead to termination of affected services.

N. **Information System Lifecycle Security.** To the extent Seller develops systems that Process Best Buy Data, Seller must infuse prudent information security measures based off industry standards, throughout the entire development process.

VII. Privacy Compliance.

A. **Compliance with Laws.** Seller agrees and warrants that, with regard to Processing Best Buy Data, Seller will comply with all then-current applicable international, federal, national, provincial, state, and local laws, rules, regulations, directives, and ordinances in connection with the performance of services.

1. Seller agrees and warrants that

a) Seller is authorized to Process Best Buy Data (including but not limited to Personal Information, Customer Information, and Order Information) only on behalf of, and in accordance with the instructions of, Best Buy. Best Buy instructs Seller to process Personal Information for the following purposes: (i) processing necessary for the provision of the services and in accordance with the Agreement; (ii) Processing initiated by Best Buy's customers in their use of the Services for customer service purposes consistent with the Agreement; and (iii) processing to comply with the other reasonable written instructions provided by Best Buy to Seller (e.g., via email or via support requests) where such instructions are consistent with the terms of the Agreement.

b) Seller will use Best Buy Data (including Personal Information) only for the purposes for which it was provided and for no other purpose.

c) Seller will not (i) Sell Personal Information, (ii) disclose or Share Personal Information for Cross-Context Behavioral Advertising or (iii) retain, use, or disclose Personal

Information (1) for any purpose other those set forth in Section VIIA.1(a) or (2) outside of the direct business relationship between Best Buy and Seller.

2. Seller certifies that it understands and will comply with the requirements and restrictions set forth in Section VII(A) of these Requirements.

B. **Prohibited Parties.**

Notwithstanding anything that may be to the contrary, Seller will not provide Best Buy Data or access to Best Buy Systems to, or use the services of, individuals or entities that are (1) located in countries subject to sanctions by the Office of Foreign Assets Control (OFAC) of the U.S. Department of Treasury, or (2) subject to sanctions as Specially Designated Nationals (SDNs), or (3) in violation of any export control laws or rules including, but not necessarily limited to, 28 C.F.R. Part 202.