VENDOR PRIVACY AND SECURITY POLICY REQUIREMENTS

I. Purpose and Overview.

These Vendor Privacy and Security Policy Requirements ("Requirements") are part of Best Buy's comprehensive privacy and security program which seeks to reduce or eliminate risk of loss to Best Buy, its employees, and its customers. Vendors must comply with these minimum Requirements as applicable to the services and/or products provided by Vendor to Best Buy.

II. Defined Terms and Interpretation.

A. Defined Terms.

1. Agreement. The written document or verbal agreement that memorializes and governs the relationship between Vendor and Best Buy.

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 Vendor, including but not limited to customer and employee Personal Information. 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. Business. Has the meaning given to it in the CCPA or Data Protection Laws.

6. Business Purpose. Has the meaning given to it in the CCPA or other Data Protection Laws.

7. CCPA. The California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 *et seq*.

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

   a) a breach of security of Vendor'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 suspected unauthorized access to or acquisition, use, disclosure, modification, or destruction of Best Buy Data, Best Buy Systems, or Best Buy assets (including without limitation lost/stolen laptops and compromised passwords); or

   c) Vendor'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 Vendor Systems.

   External pings and other broadcast attacks on Vendor'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 Vendor Systems.

9. "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.

10. Personal Information. Any Best Buy Data, regardless of the media in which it is contained, 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 (including, without limitation, the data elements listed as such in section 1798.140(o)(1)(A)-(K) of the CCPA or other Data Protection Laws), that may be (a) Processed at any time by Vendor in anticipation of, in connection with, or incidental to the performance of the Agreement or (b) derived by Vendor from such information.

11. Process, Processes, Processed or Processing. Accessing, using, collecting, creating, receiving, hosting, maintaining, modifying or altering, storing, transmitting, or destroying Best Buy Data, whether or not by automated means.

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

13. Sensitive Information. Any Best Buy Data which is regulated by any applicable state or federal law, rule or regulation, or industry standard, including but not limited to:

    a) individual financial information, such as bank account numbers and payment card numbers;

    b) Social Security numbers or other government-issued identification numbers;

    c) individual health information;

    d) individual geolocation information;

    e) individual biometric information;

    f) usernames and passwords; or

    g) data collected by telecommunications companies about a consumer's telephone calls, which includes the time, date, duration, and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill ("Customer Proprietary Network Information");

    h) Sensitive technical information (e.g. Encryption keys, passwords, API Keys, system vulnerabilities).

14. Service Provider. Has the meaning given to it in the CCPA or other Data Protection Laws.

15. Third-Party Provider. All vendors, 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 Vendor (including without limitation cloud hosting providers and payment processors). For purposes of clarity, Vendor is responsible for ensuring its Third-Party Providers have substantially similar security and privacy controls and policies as those set forth herein.

16. Vendor. The party subject to these Requirements and the Agreement.

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

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

III. Requirements Statement.

Vendor will implement appropriate administrative, technical, and physical safeguards to ensure the privacy, confidentiality, integrity, and availability of Best Buy Data and Best Buy Systems, if and as applicable.

IV. Suspension of Access.

Vendor's access to any Best Buy Data and/or Best Buy Systems is subject to Vendor'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 Vendor's access, and all links and interfaces, to Best Buy Data and/or Best Buy Systems (including terminating transmission of Best Buy Data to Vendor) without liability. Best Buy acknowledges that the inability of Vendor to access Best Buy Data and/or Best Buy Systems may result in Vendor'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.

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

Vendor will only collect, retain, return, and destroy Best Buy Data if/and as permitted in the Agreement. If the Agreement does not address collection, retention, return, and/or destruction of Best Buy Data, then, at a minimum, Vendor's retention must preserve the integrity of Best Buy Data (including metadata).

In addition, if no retention period is specified in the Agreement, Vendor will retain the Best Buy Data for no more than two (2) years from the termination of the Agreement. Prior to the end of this two-year period, Vendor will return or destroy, at the choice and direction of Best Buy, any Best Buy Data at no cost to Best Buy

Upon destruction of Best Buy Data, Vendor will certify that:

A. Vendor has shredded paper copies containing Best Buy Data; and

B. Vendor has completely and permanently destroyed electronic copies of all Best Buy Data rendering it no longer usable, readable, decipherable and retrievable.

If required by law or if required via a Best Buy legal hold notice, Vendor will continue maintaining Best Buy Data, subject to Vendor's confidentiality and security obligations.

VI. 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 Vendor in a manner that reasonably minimizes interference with Vendor's business operations as follows:

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

2. Onsite Review. On an annual basis, during the term of the Agreement and for as long as Vendor retains Best Buy Data, Vendor will allow Best Buy or its representatives to perform an onsite review of any facilities and locations that Process Best Buy Data. The onsite review may include any of the following:

   a) walk-through/visual inspection of facilities;

   b) interview(s) with personnel onsite and/or via phone; and/or

   c) review of Vendor's policies and procedures, as well as any evidence reasonably necessary to validate Vendor is in compliance with these Requirements and the Agreement.

3. Audit for Reasonable Cause. In addition to the annual onsite review, if Vendor violates 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. Vendor will assist Best Buy in such audit.

B. **Third-Party Audits.** Vendor will, on an annual basis, obtain a formal review of its security controls conducted by an unaffiliated third party, and will thereafter provide Best Buy with the written results of the audit and proof of Vendor's compliance with the audit requirements and/or Vendor's remediation plan. The specific third-party audit type may be set forth in the Agreement. If not specified in the Agreement, Vendor will obtain one of the following audits which will be consistent with the services and/or products provided by the Vendor:

1. ISO 27001 Certification. Vendor will engage an independent third party to conduct an ISO 27001 audit.

2. Personal Information - SOC 2 Report. If Vendor Processes Personal Information, Vendor will complete an AICPA SSAE 18 SOC 2 Type II audit ("SOC 2") of all Vendor Systems and processes that Process Best Buy Data. The SOC 2 will include review of controls for the following "Trust Services Principles": security, confidentiality, privacy, availability, and processing integrity.

3. Other Best Buy-Approved Certification(s). If Vendor engages a reputable third party to conduct an audit utilizing other standards (such as the National Institute of Standards and Technology ("NIST") in combination with International Organization for Standardization ("ISO") elements, or the Health Information Trust Alliance ("HITRUST")), Vendor will disclose such standards to Best Buy for its review and acceptance. If accepted by Best Buy in writing, Vendor represents, warrants, and covenants that it is in compliance with, and certified to, such approved standards.

For Vendors hosting or Processing Best Buy Data:

C. **Vulnerability Scans and Penetration Testing.** Vendor will engage a reputable, independent, nationally-recognized third party to perform annual vulnerability scans and penetration testing of all public-facing applications, sites, services and the internal network where Best Buy Data may be located ("Technical Security Assessment(s)"). Upon request, Vendor will provide Best Buy an executive summary report of the annual Technical Security Assessment(s).

D. **Remediation.** To the extent that any deficiencies are identified in any of the foregoing reviews, tests, or audits, Vendor will remedy critical deficiencies within thirty (30) days and remedy all other material deficiencies within a reasonable period.

VII. Minimum Security Terms.

Vendor must, at a minimum, implement and maintain information security controls set forth in these Requirements. These security controls will apply to Vendor's programs and personnel, to the extent they Process or have access to Best Buy Data, Best Buy Systems, and Vendor Systems Processing Best Buy Data.

A. **Information Security Organization.** Vendor must have a formal and comprehensive information privacy and security program ("Program"), meeting or exceeding industry best practices and applicable regulations and laws, that is designed to protect the privacy, confidentiality, integrity, and availability of Best Buy Data and Best Buy Systems. Vendor will do at least the following:

1. Program Framework. Maintain a comprehensive Program which includes documented policies, governance, and security training for Vendor's employees and Third-Party Providers.

2. Annual Review. Annually review the Program for gaps, continued alignment to industry standards, and to ensure the Program addresses evolving threats.

3. Program Manager. Designate a person responsible for overall Program oversight.

4. Training. Provide annual training on the Program and relevant information security and privacy topics (such as phishing, malware, social engineering attacks, etc.) for all Vendor employees and contractors performing services and support for Best Buy.

5. Communication. Communicate changes to the Program to all affected employees and contractors in a timely fashion.

6. Classification Policy. Document a classification policy that:

   a) classifies the sensitivity of information, and

   b) classifies the systems under its care, custody, possession, and control to ensure proper controls are implemented relative to the sensitivity of information.

7. Notification of Material Changes. Promptly notify Best Buy in writing of any

   a) noncompliance with provisions of these Requirements, and

   b) material change to Vendor's Program.

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

a) limit access to electronic and hard copy assets to personnel with a legitimate business need,

b) securely handle all electronic or hard copy assets at all times,

c) secure all assets when left unattended, and

d) 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.** Vendor must implement controls to enable employees and all Third-Party Providers to adhere to policies and standards according to roles and access and to reduce the risk of theft, fraud, loss, and misuse of information, systems, and facilities. Vendor shall, at a minimum:

1. Workforce Screening. Ensure employees understand their responsibilities and are suitable for the roles for which they are considered (including using appropriate background checks/personnel screening).

2. User Acknowledgment. Track initial and recurring annual training of employees. Training shall include the following topics:

a) information security threat landscape (such as phishing, malware, social engineering attacks);

b) role and responsibilities in supporting the Program and reducing threats; and

c) liabilities and associated enforcement actions for failing to fulfill the duty of care.

3. Resources. Equip employees and Third-Party Providers to adequately support the Program and to reduce human error.

4. 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.** Vendor must implement, manage, and review appropriate physical controls to prevent unauthorized physical access, damage, and interference to information, infrastructure, and equipment. Vendor shall, at a minimum:

1. Implementation of Controls. Implement physical security controls that address purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance. For example, a freely available reference is NIST 800-53 rev. 4 (Information Security and Privacy Controls), Appendix F (Controls Catalog), Family PE (Physical and Environmental Protection).

2. Security of Assets. Ensure assets (such as data centers, point of sale devices, and environmental control equipment) are appropriately secured from unauthorized physical access.

3. Environmental Controls. Implement, review, and test physical protections against external and environmental threats such as natural disasters, attacks, or accidents.

E. **Program Operations.** Vendor must securely operate Vendor Systems which support Best Buy Data and assets through the application of key operational management controls. Vendor 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 ("Harmful Code and Messages"). Employ automated screening of all ingoing and outgoing messages for Harmful Code and Messages.

3. Patching. Implement processes and procedures that patch systems according to industry standard patching guidelines. Vendor shall provide a patch or fix as soon as possible, but in no event later than sixty (60) days from the notification of such vulnerability or risk.

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

5. Risk Reporting. If Best Buy provides notice to Vendor of a vulnerability in Vendor's systems and Vendor does not disclose such vulnerability consistent with industry practices, Vendor shall indemnify, defend and hold Best Buy harmless from and against claims (including reasonable attorneys' fees) arising from Vendor's failure to publicly disclose such vulnerability.

6. Testing. Perform periodic static and dynamic application security assessments.

7. 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. **Cryptographic Controls.** Vendor will implement and review cryptographic controls as follows:

1. Encryption.

a) In Transit. Vendor will encrypt all Best Buy Data in transit across public networks using then-current industry encryption standards but using not less than Transport Layer Security version 1.2. Vendor must also independently encrypt data in transit payloads containing Sensitive Information, even though the network protocol used meets the requirements of VII(F)(1)(a)).

b) At Rest. Vendor will encrypt all Sensitive Information at rest using then-current industry encryption standards (but using not less than AES 256). For purposes of clarification and without limiting the foregoing:

i. For structured data, such encryption will be applied at the application or database tier level, and

ii. for unstructured data, such encryption will be applied at disk level.

2. Key Management. Vendor will protect critical cryptographic secrets against unauthorized access using industry standard key management technologies (such as Hardware Security Modules ("HSM")). Vendor will not hard code critical encryption keys or other secrets into the "system" making them retrievable or discoverable, by an unauthorized party.

G. **Communications.** Vendor will use secure communication mechanisms and procedures when transmitting Best Buy Data. Vendor shall, at a minimum:

1. Secured Communications. Conduct all communications containing Best Buy Data (including instant messaging, email, conference calls, video conferences, Voice Over IP, voicemail, and fax) in a secure manner.

2. Security of Website Browsing. Intercept and authenticate web browsing activities to appropriately log and assess the transaction. Implement controls to allow access to trusted websites and prevent access to known malicious websites. Update lists of trusted and malicious websites on a periodic basis.

H. **Security Monitoring.** Vendor will maintain a security monitoring program. Vendor 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.

2. Reviewing and Archiving Logs. Regularly analyze, review, report, and archive collected logs and associated analysis.

3. Network Monitoring. Deploy, maintain, and monitor then-current 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.

4. Data Loss Prevention. Implement data loss prevention software to detect potential data ex-filtration transmissions and prevent them by monitoring, detecting, and blocking sensitive and personal data while in-use, in-motion, and at-rest.

5. Reporting. Communicate information security events and weaknesses associated with information systems in a manner allowing timely corrective action to be taken to the appropriate personnel.

I. **Data Incident Notification & Response.** Vendor shall, at a minimum:

1. Incident Response Plan. Create, document, maintain, and routinely test an incident response plan. Vendor will follow documented responsibilities and procedures to respond to information security incidents (including Data Incidents) quickly, effectively, and in an orderly way. Upon Best Buy's request, Vendor 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, Vendor 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 a daily written report detailing the known facts of the Data Incident, continuing to provide such report until Vendor 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, and without regard to any limitation of liability or disclaimer of liability, Vendor 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.

J. **Access Controls.** Vendor will regulate access to Best Buy Data and Best Buy Systems through security access controls and robust authorization mechanisms. Vendor 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. Password Policy. Maintain and enforce a strong password policy(ies) which addresses password length, complexity, lockout, history, and expiration. Additionally, disable default, weak, or well-known passwords or other well-known 'secrets'.

4. Password Storage. Store and manage passwords and all other authentication secrets in a secure manner consistent with industry standards.

5. Multi-Factor Authentication. Employ two-factor (or better) authentication and device-based authentication for access to Vendor Systems (e.g. VPN) to ensure each user is properly authenticated.

6. Remote Access Policy. Maintain and enforce a remote access policy which addresses connectivity, software and hardware requirements, encryption, multi-factor authentication, user roles, device management, and remote access controls.

7. Termination of Access. Terminate access as soon as it is no longer needed (such as due to termination or a change in job role).

For Vendors accessing Best Buy Systems:

8. Managing Access to Best Buy Systems. Vendor will appoint a Vendor Security Administrator ("VSA") responsible for managing the access of all Vendor users of Best Buy Systems. Vendor must ensure VSA:

   a) reviews user access every ninety (90) days for accuracy,

   b) provisions and de-provisions user access as needed, and

   c) receives training from Best Buy on VSA responsibilities.

   In the event a VSA leaves, the Vendor must appoint a replacement prior to or within one (1) business day of their departure.

9. Provisioning Access to Best Buy Systems. Vendor will document and send all Vendor user access requests to the VSA. Vendor will provision access based on least privileged access principles and terminate access as soon as it is no longer needed (e.g. termination, change in job role). Terminated users must be removed within twenty-four (24) hours of termination. If revocation of access is managed by Best Buy, Vendor will notify Best Buy within twenty-four (24) hours of termination.

For Vendors managing white labelled applications or providing accounts and passwords to consumers, on behalf of Best Buy or in partnership with Best Buy:

K. **Customer Access Control.** Vendor must implement secure mechanisms and configuration requirements when creating and managing customer accounts. Vendor will do the following:

1. Account Provisioning. Provision only one consumer account per unique email address.

2. Password Requirements. Allow the consumer to select and update their password (that is, passwords must not be exclusively assigned to users or be static in nature). Passwords must meet minimum password requirements listed in the Access Control section J of these Requirements. Vendor will prohibit sharing of passwords.

3. Password Lockout. Lock consumer accounts upon ten (10) consecutive incorrect authentication attempts and send a verification code to the consumer's email address for the consumer to unlock their account.

For Vendors developing or enhancing applications or system services which handle Best Buy Data:

L. **Information System Lifecycle Security.** Vendor must infuse prudent information security measures throughout the entire development process. Vendor will implement and adhere to a formal software development life cycle program that is based on industry standards such as the OWASP Application Security Verification Standard 4.0.3 (or its successors), Level 2.

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

1. Device Configuration and Implementation. Use a mobile device and/or mobile application management solution(s) which protects Best Buy Data and meets then-current 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, contractor, or contingent worker, unless otherwise instructed or such action is prohibited by law (such as due to a legal hold). Additionally, return Best Buy devices to Best Buy within seven (7) days.

3. Acceptable Use. Maintain policies and procedures describing the appropriate use of information systems being used by end user devices (including remote access, email, Internet, removable media, social media and social networking, etc.). Review, reaffirm, and communicate all such policies and procedures at least annually.

N. **Network Security.** Vendor must leverage network specific information security controls to protect Best Buy Data and assets that traverse the Vendor's network. Vendor shall, at a minimum:

1. Firewalls. For vendors transmitting or storing Best Buy Data within private networks, appropriately employ, securely configure, and regularly update and test enterprise-wide firewall infrastructure (that supports stateful inspection) to restrict access to and from untrusted networks and minimize access to extent needed to perform services.

2. Weak Protocols. Protect transmission of Sensitive Information and credentials through the network using secure protocols (examples of unacceptable protocols are FTP, telnet, and early implementations of SSL/TLS).

3. Shared Environments. Disclose storage or Processing of Best Buy Data in multi-tenant or shared environments (that is, multiple customers' information exists in the same system or network tenant). Ensure adequate logical separation between access to and processing of each party's information.

O. **Third-Party Security.** Vendor will manage its Third-Party Providers to ensure the privacy, confidentiality, integrity, and availability of Best Buy Data and Best Buy Systems. Vendor will, at a minimum:

1. Risk Assessments. On an ongoing basis, oversee and review all Third-Party Providers that may receive or access Best Buy Data, Best Buy Systems, and/or Best Buy assets for privacy, confidentiality, and information security risks, controls, and compliance.

2. Written Agreements. Enter into written agreements with Third-Party Providers to keep Best Buy Data confidential and not use Best Buy Data for any purposes other than providing services for the benefit of Best Buy. In addition, enter into written agreements with third parties which

require compliance with then-current industry standard information security controls, not less than the security controls described in these Requirements.

3. Remediation. Document and promptly remediate Third-Party Provider findings, issues, and non-compliance.

4. Third-Party Provider Notice. Vendor will notify Best Buy of the names of any new and replacement Third-Party Providers prior to them beginning sub-processing of Personal Information. Within thirty (30) business days of receiving notice of a Third-Party Provider change, Best Buy may object by providing written notice to Vendor. If Best Buy gives written notice of objection, Vendor and Best Buy will discuss the objection in good faith to seek to resolve it. If no resolution is found within 30 days after initial notice of objection is given, Best Buy may terminate the affected Services on 60 days' written notice.

P. **Risk Management.** Vendor must assess and mitigate risks associated with access and use of Best Buy Systems as well as Processing Best Buy Data. Vendor shall, at a minimum:

1. Testing and Monitoring. Regularly (at least annually) test and monitor the effectiveness of Vendor's controls, systems, and procedures.

2. Risk Mitigation. Implement technical and procedural capabilities to timely identify, manage, and mitigate risks that could impact Best Buy Data, Best Buy Systems, or performance of Vendor's services.

For Vendors receiving, refurbishing, reselling, recycling, or otherwise disposing of any product, storage media, or devices from Best Buy that is/are capable of storing data or information ("Products"):

Q. **Product Sanitization.** Vendor must sanitize the Products, making sure all personal data and information (including without limitation usernames, passwords, network information, messages, files, documents, content, images, music, and videos) therein is completely and permanently unusable, unreadable, indecipherable, and irretrievable.

Such sanitization process will include, without limitation, updating firmware, erasing data, clearing all configurations and error codes, and reinitializing factory setting and, in any event, must meet or exceed the standards, requirements, recommendations, and guidelines (1) outlined in the NIST Special Publication 800-88 rev. 1, Guidelines for Media Sanitization, or any successor version; or (2) otherwise mutually agreed upon in writing by Vendor and Best Buy.

In addition, Vendor will remove all personal physical identifiers (e.g., nameplates, etched names, stickers, etc.) placed by previous user(s) on all Products.

VIII. Privacy Compliance.

A. **Compliance with Laws.** If Vendor Processes Best Buy Data, Vendor agrees and warrants that, with regard to Processing Best Buy Data, Vendor will comply with all then-current international, federal, national, provincial, state, and local laws, rules, regulations, directives, and ordinances in connection with the performance of services The nature and type of Personal Information processed by Vendor may be described in the Agreement.

1. Vendor agrees and warrants that

a) (i) If Personal Information is Processed by Vendor on behalf of Best Buy, Vendor will Process Personal Information according to Best Buy's instructions. Best Buy instructs

Vendor 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 end users in their use of the Services; and (iii) processing to comply with the other reasonable written instructions provided by Best Buy to Vendor (e.g., via email or via support requests) where such instructions are consistent with the terms of the Agreement.

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

c) Vendor will not (i) Sell Personal Information, or (ii) retain, use, or disclose Personal Information (1) for any purpose other those set forth in Section VIIIA , or (2) outside of the direct business relationship between Best Buy and Vendor.

d) Vendor will cooperate with Best Buy if an individual requests (i) access to or correction of his or her Personal Information, (ii) information about the categories of sources from which the Personal Information is collected, or (iii) information about the categories or specific pieces of the individual's Personal Information, including by providing the requested information in a portable and, to the extent technically feasible, readily useable format that allows the individual to transmit the information to another entity without hindrance. Vendor will promptly inform Best Buy in writing of any requests with respect to Personal Information.

e) Upon Best Buy's request, Vendor will promptly delete a particular individual's Personal Information from Vendor's records. In the event Vendor is unable to delete the Personal Information for reasons permitted under the CCPA or other Data Protection Laws, Vendor will (i) promptly inform Best Buy of the reason(s) for its refusal of the deletion request, (ii) ensure the privacy, confidentiality, and security of such Personal Information, and (iii) delete the Personal Information promptly after the reason(s) for Vendor's refusal has expired.

2. Best Buy and Vendor acknowledge and agree as follows:

a) The Personal Information that Best Buy discloses to Vendor is provided to Vendor for a Business Purpose.

b) During the time the Personal Information is disclosed to Vendor, Best Buy has no knowledge or reason to believe that Vendor is unable to comply with the provisions of Section VIII(A) of these Requirements.

3. Vendor certifies that it understands and will comply with the requirements and restrictions set forth in Section VIII(A) of these Requirements.

B. **Location of Best Buy Data.** Unless otherwise agreed to in the Agreement, Vendor must Process Best Buy Data and access Best Buy Systems only in secure data facilities located in the United States and adopt security measures to ensure that no person or entity (including without limitation hosting provider) physically located outside of the United States can Process any Best Buy Data or access Best Buy Systems.

Notwithstanding anything that may be to the contrary, Vendor 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 in violation of any export control laws.

For Vendors engaging in any online behavioral advertising in connection with Vendor's products and services (whether by Vendor, through others, or on behalf of Best Buy):

C. **Online Behavioral Advertising.** Vendor represents and warrants that it will comply with the Digital Advertising Alliance ("DAA") Self-Regulatory Program for Online Behavioral Advertising ("DAA Program"), including but not limited to:

1. providing enhanced notice as required by the DAA Program;

2. providing consumers with the ability to opt out of behaviorally-targeted ads as required by the DAA Program;

3. licensing the self-regulatory AdChoices logo from the DAA; and

4. ensuring that, in providing such products and services, Vendor work only with Third-Party Providers that comply with the DAA Program and these Requirements.

Vendor will not use any "Flash Cookies" or "Locally Stored Objects" in connection with online behavioral advertising services provided for or on behalf of Best Buy, without Best Buy's prior written approval. In no event will Vendor use Flash Cookies or Locally Stored Objects for the purpose of circumventing any privacy or security controls or settings.

For Vendors who have access to, or will collect, store, process, or transmit, cardholder data (e.g. credit, debit, stored value, or prepaid card information) or systems containing cardholder data:

D. **Payment Card Industry Data Security Standards ("PCI-DSS").** If Vendor maintains custody, possession, care, or control of cardholder data and/or access to systems containing cardholder data, Vendor represents and warrants that it will, at its own expense (for as long as Vendor maintains custody, care, or control of cardholder data):

1. remain responsible to secure cardholder data in its care, custody, possession, or control;

2. comply with the applicable then-current PCI-DSS;

3. cooperate with Best Buy to complete its Service Provider Responsibility Matrix, as defined and, in compliance with Payment Card Industry ("PCI") requirements covering the Vendor PCI services being provided to Best Buy;

4. provide to Best Buy, Vendor's annual Attestation of Compliance (AOC) completed by an independent Qualified Security Assessor (QSA); and

5. for purposes of clarification, Vendor will provide Best Buy with annual PCI "Attestations of Compliance" for all its applicable Third-Party Providers (including payment processors) that have access to, or will create, receive, store, process, or transmit, cardholder data or systems containing cardholder data.

E. **Point to Point Encryption ("P2PE") Requirements.** Vendor will have formal agreements in place with all Third-Party Providers that perform P2PE functions on behalf of the solution provider which include the following terms:

1. a description of functions each Third-Party Provider is responsible for,

2. agreement to maintain P2PE controls for which they are responsible,

3. notification and documentation of any changes affecting the Third-Party Provider governed by P2PE requirements,

4. required notification to the Vendor of any security-related incidents,

5. agreed upon appropriate service level agreements (SLAs),

6. agreement to comply with applicable P2PE and/or PCI DSS requirements as needed,

7. agreement to provide proof of compliance with P2PE requirements and/or PCI DSS requirements as needed, and

8. agreement to provide reports to solution provider as required in the "Component providers ONLY: report status to solution providers" section of the applicable P2PE domain.

For Vendors who will Process Health Insurance Portability and Accountability Act ("HIPAA") protected health information:

F. **Health Information.** If Vendor Processes Best Buy Data that includes protected health information (as defined by Health Insurance Portability and Accountability Act or "HIPAA"), Vendor represents and warrants that it will (for as long as Vendor maintains custody, care, or control of protected health information):

1. comply with HIPAA, including all applicable provisions of the Privacy Rule, Security Rule, and Breach Notification Rule; and

2. sign Best Buy's Business Associate Agreement (BAA).