WALMART INFORMATION SECURITY AGREEMENT

This Information Security Agreement (the “Agreement”) between Wal-Mart Stores, Inc. (“Walmart”) and Contractor (each a “Party” and collectively the “Parties”) sets forth the Parties’ mutual understanding relating to the privacy and security of Walmart Information and Walmart systems. Walmart requires execution or incorporation of its Information Security Agreement (ISA) for all contract partners (“Contractors”) receiving Walmart Information or accessing Walmart information systems.

Whereas the Parties agree that Contractor will have access to Walmart Information and/or Walmart systems; and

Whereas both Parties wish to meet their legal obligations with respect to access to and potential use and disclosure of Walmart Information and/or Walmart systems;

Therefore, in consideration of the foregoing, the promises and covenants contained in this Agreement, and for other good and valuable consideration, the receipt and the sufficiency of which is hereby acknowledged, the Parties agree as follows:

A. Definitions. For the purposes of this Agreement, the terms below have the following meanings whenever capitalized:

“Claims” means all claims, requests, accusations, allegations, assertions, complaints, petitions, demands, suits, actions, proceedings, causes of action, and judgments.

“Costs” means expenses of any kind, including attorneys’ fees, litigation costs, investigatory costs, costs of providing notice to any person or organization in the event of a Data Incident, and costs of providing consumer protection services to any person in the event of a Data Incident, including credit monitoring or identity restoration services.

“Data Incident” means any reasonably suspected or actual unauthorized access to or acquisition, disclosure, use, or loss of Walmart Information (including hard copy records) or breach or compromise of Contractor’s Security Program that presents a potential threat to any Walmart Information or Walmart system.

“ISD” means Walmart’s Information Systems Division.

“Privacy and Security Requirements” means all of the following: (i) all legal requirements (federal, state, local, and international laws, rules and regulations, and governmental requirements) currently in effect and as they become effective, relating in any way to the privacy, confidentiality, integrity, availability, or security of Walmart Information; (ii) all industry standards concerning privacy, data protection, confidentiality, integrity, availability, or security of information, including without limitation, the Payment Card Industry Data Security Standard, and any other similar standards; (iii) all policies, statements, or notices that are provided to Contractor in writing; and (iv) all controls required by the ISD Security Review, including secure coding standards.

“Security Program” means a comprehensive written information security program described below in Section C.


“Walmart Information” means the following, regardless of form or the media in which it is maintained, that may be accessed, used, or disclosed to Contractor in connection with or incidental to the performance of services for or on behalf of Walmart or by any other means:
(1) Any information relating to an identified or identifiable individual irrespective of whether such individual is a Walmart customer, employee, or other status (including, but not limited to, name, postal address, email address, telephone number, date of birth, Social Security number, driver's license number, other government-issued identification number, financial account number, credit or debit card number, insurance ID or account number, health or medical information, consumer reports, background checks, biometric data, digital signatures, any code or password that could be used to gain access to financial resources, or any other unique identifier);

(2) Non-public business information; and

(3) Any information marked “Highly Sensitive” or “Sensitive” or defined as “Confidential” by the Agreement, or information that Contractor should reasonably believe to be confidential.

B. Acknowledgement. Contractor acknowledges that it is solely responsible for the confidentiality and security of Walmart Information in its possession, custody, or control, or for which Contractor is otherwise responsible.

C. Security Program. Contractor has implemented and shall maintain a Security Program that complies with Privacy and Security Requirements and incorporates industry best practices. Contractor’s Security Program includes appropriate administrative, technical, and physical safeguards; assures the confidentiality, availability, integrity, and security of Walmart Information and Walmart systems; and includes at least the following safeguards:

(1) Appropriate user authentication controls, including secure methods of assigning, selecting, and storing access credentials, restricting access to active users, and blocking access after a reasonable number of failed authentication attempts.

(2) Secure access controls, including controls that limit access to Walmart Information to individuals that have a demonstrable genuine business need-to-know, supported by appropriate policies, protocols, and controls to facilitate access authorization, establishment, modification, and termination.

(3) Appropriate and timely adjustments to Contractor’s Security Program based on: periodic risk assessments; regular comprehensive evaluations (such as third-party assessments) of Contractor’s Security Program; monitoring and regular testing of the effectiveness of safeguards; and a review of safeguards at least annually or whenever there is a material change in Contractor’s technical environment or business practices that may implicate the confidentiality, availability, integrity, or security of Contractor’s information systems.

(4) Appropriate, ongoing training and awareness programs designed to ensure workforce members and others acting on Contractor’s behalf are aware of and adhere to Security Program policies, procedures, and protocols.

   a. Monitoring of systems designed to ensure data integrity and prevent loss or unauthorized access to, or acquisition, use, or disclosure of, Walmart Information.

   b. Technical security measures, including firewall protection, antivirus protection, security patch management, logging of access to or use or disclosure of Walmart Information, intrusion detection, and encryption of data in transit and at rest.
c. Physical facility security measures, including access controls, designed to restrict access to Walmart Information to individuals described in Section C.2.

d. Logical segmentation of Walmart Information from data of others, but especially any Walmart competitor.

D. **Supervision.** Contractor shall exercise necessary and appropriate supervision over its relevant employees and others acting on its behalf to maintain confidentiality, integrity, availability, and security of Walmart Information.

E. **Mobility and Transfer of Data.**

1. Walmart Information that is classified by Walmart as Highly Sensitive Data or Sensitive Data shall not be stored on or transported via a laptop, any other mobile device, or any removable storage media, including USB, thumb drives, DVDs, or CDs, unless such devices or media are encrypted using an encryption methodology approved in writing by ISD Security.

2. All electronic data transfers of Walmart Information classified by Walmart as Highly Sensitive Data or Sensitive Data must be accomplished via secure FTP or other protocol or encryption methodology approved in writing by ISD Security.

3. Any physical removal or transfer of Walmart Information classified by Walmart as Highly Sensitive Data or Sensitive Data from Walmart’s or Vendor’s facilities shall be conducted only according to controls developed or approved in writing by ISD Security.

4. Walmart Information may not be transferred, stored, or processed outside the country in which Contractor receives it without prior written approval from Walmart, inclusive of transfers to subcontractors or agents, notwithstanding the provisions of Section G.

F. **Data Incidents.**

1. Contractor agrees to immediately notify Walmart’s Emergency Operations Center by phone (479.277.1001) of any Data Incident. While the initial phone notice may be in summary form, a comprehensive written notice should be given within 48 hours to Walmart’s Privacy Office, 702 SW 8th Street, Bentonville, AR and its Chief Information Security Officer, 805 Moberly Lane, Bentonville, AR. The notice shall summarize in reasonable detail the nature and scope of the Data Incident (including a description of all Walmart Information affected) and the corrective action already taken or to be taken by Contractor. The notice shall be timely supplemented to the level of detail reasonably requested by Walmart, inclusive of relevant investigative or forensic reports.

2. Contractor shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with Walmart and its designees in all reasonable efforts to investigate the Data Incident, mitigate adverse effects, and prevent recurrence. Such cooperation shall include responding to Walmart’s inquiries about the Data Incident in a timely fashion.

3. The Parties shall collaborate on whether it is necessary or advisable to provide notice of the Data Incident to any person, governmental entity, the media, or other party. The Parties shall collaborate on the content of the notice. Walmart will make the final determination as to whether notice will be provided and to whom, the content of the notice, and which Party will be the signatory to the notice.
G. **Third Parties.** Contractor may transfer, disclose, or otherwise provide access to Walmart Information (including through use of third party hosting or cloud services) only to the following parties:

1. Any subcontractor or agent that Contractor engaged prior to executing the Agreement if: (i) the subcontractor or agent, including the proposed access to Walmart Information by the subcontractor or agent, was evaluated in a manner substantially similar to a Security Review; (ii) the subcontractor or agent maintains an information security program substantially equivalent to the Security Program required of Contractor by this Addendum; (iii) Contractor has executed an agreement with the subcontractor or agent that is substantially equivalent to this Addendum; and (iv) the subcontractor or agent has a demonstrable genuine business need-to-know for all Walmart Information to which it is provided access.

2. Any subcontractor or agent that Contractor engages following execution of the Agreement if: (i) Walmart is permitted, at its option, to conduct a Security Review to evaluate Contractor’s engagement of the subcontractor or agent and security controls implemented by that subcontractor or agent; (ii) the subcontractor or agent maintains an information security program substantially equivalent to the Security Program required of Contractor by this Addendum; (iii) Contractor has executed an agreement with the subcontractor or agent that is substantially equivalent to this Addendum and preserves for Walmart or Contractor the rights available to Walmart pursuant to Sections F and K of this Addendum; (iv) the subcontractor or agent has a demonstrable genuine business need-to-know for all Walmart Information to which it is provided access; and (v) Walmart provides prior written approval to Contractor authorizing the sharing, transfer, disclosure, or access.

3. Any other party that is not a subcontractor or agent only with prior written notice to and prior written approval of Walmart.

H. **Notice of Process.** In the event Contractor receives a governmental or other regulatory request for, or legal process requesting, any Walmart Information, Contractor shall immediately notify Walmart’s Legal Department in order that Walmart will have the option to defend such action. Contractor shall reasonably cooperate with Walmart in such defense.

I. **Notice of Individual Requests and Complaints.** Contractor shall immediately notify Walmart in the event that Contractor receives: (i) requests from individuals relating to Walmart Information, including requests to access or rectify personal information; or (ii) complaints of any kind from individuals relating to the privacy, confidentiality, or security of Walmart Information. Contractor shall not respond to any such request or complaint without Walmart’s prior written approval.

J. **Use Restrictions.** Unless Walmart provides prior written approval, Contractor shall not use, access, disclose, reconfigure, re-identify, or aggregate Walmart Information, nor permit any of the foregoing, for any purpose other than performing services pursuant to the Agreement, fulfilling the obligations of this Addendum, or as strictly necessary to comply with law.

K. **Security Review and Assessment.**

1. ISD Security may conduct a Security Review when determined reasonably required by Walmart.

2. At Walmart’s request, Contractor shall provide Walmart copies of its data privacy and security policies and procedures that apply to Walmart Information. Contractor also may be asked, upon Walmart’s reasonable request, to submit written responses to questions regarding its privacy and information security practices that apply to Walmart Information.
Contractor shall submit written responses within 10 business days of receipt of Walmart’s request.

(3) Contractor shall provide ISD Security with an opportunity to conduct a privacy and security assessment of Vendor’s Security Program and systems and procedures. Such assessment may be conducted on-site by Walmart personnel or Walmart’s contracted third party assessors or through surveys and interviews, at the option of Walmart. Such assessment may be conducted no more than once per year, or more frequently in the event of any Data Incident. When an on-site assessment will be conducted, Walmart shall provide Vendor with reasonable advance notice of not less than 15 business days, except in the event of a Data Incident or if Walmart has a reasonable basis to believe Vendor may not be in compliance with this Addendum, in which case advance notice shall be not less than 48 hours.

(4) Contractor shall provide Walmart with notice of any findings that are likely to adversely impact Walmart Information or Walmart systems that are identified through any security assessment or review of Contractor’s systems or Security Program performed by Contractor or a third party, including vulnerability and penetration assessments. Notice of these findings may be provided in the form of a written summary. Contractor shall keep Walmart timely informed of its remediation efforts to address these findings.

L. Compliance. Contractor shall comply with all applicable Privacy and Security Requirements.

M. Security Certification. Contractor shall maintain a level of security certification or assessment consistent with best practices and conducted by a qualified third party reasonably acceptable to Walmart. Such certifications shall be provided to Walmart upon reasonable request.

N. Indemnification. Contractor shall indemnify, defend, and hold harmless Walmart for and from any Claims, and reimburse Walmart for or bear any Costs, related to any Data Incident or Vendor’s noncompliance with this Agreement notwithstanding any allegation that Walmart was negligent or otherwise at fault.

O. Termination. Walmart may terminate any contract or engagement between the Parties, including the Agreement, in the event: (i) of a Data Incident that Walmart determines is likely to have a substantial adverse impact on Walmart’s relationship with its customers or associates or may otherwise substantially harm its reputation; (ii) of a material violation of this Agreement by Contractor, including any violation of Section G; (iii) of any material misrepresentation made in connection with any Security Review, assessment, or other process described in Sections G or K; or (iv) that Contractor or a third party reviewed pursuant to Section G fails to timely or effectively remediate material adverse findings from a Security Review, assessment, or other process described in Sections G or K, as applicable. This Section O in no way limits any termination rights provided under the Agreement.

P. Secure Return or Disposition; Termination of Access.

(1) Contractor shall return or dispose of Walmart Information in its possession, custody, or control: (i) if no longer needed for Walmart’s business or legal purposes or upon termination of this Agreement, whichever is longer; or (ii) upon Walmart’s direction which may be given at any time.

(2) Notwithstanding the foregoing, Contractor will be permitted to retain: (i) Walmart Information for a longer period if such retention is strictly necessary to meet Contractor’s legal compliance obligations, is done pursuant to Contractor’s fully implemented and documented records management program, and is limited to the minimum Walmart Information and minimum retention period needed to meet these obligations; and (ii)
backup media containing Walmart Information for so long as is permitted by Contractor’s fully implemented and documented records management program, which retention shall not be indefinite and shall not exceed industry standards.

(3) Any disposal of Walmart Information must ensure that Walmart Information is rendered permanently unreadable and unrecoverable.

(4) To the extent Contractor accesses or has contact with Walmart systems, Contractor must ensure that such access is discontinued upon termination of the Agreement.

(5) Upon reasonable notice and if requested by Walmart, Contractor shall provide Walmart with a certification by an officer attesting to Contractor’s compliance with this Section P.

Q. **Survival.** Section N and Section P.5 will survive termination of this Agreement. The remaining provisions of this Agreement will survive until such time as Contractor has fully complied with the provisions of Section P.

R. **Interpretation.** The terms of this Agreement are to be construed to permit compliance with the Parties’ legal obligations with respect to Walmart Information. This Agreement supersedes any inconsistent provisions contained in prior oral or written agreements between the Parties, that are relevant to the subject matter of this Agreement. Notwithstanding the foregoing, provisions in prior agreements between the Parties that impose additional or more stringent obligations than this Agreement with respect to Walmart Information will remain in force. The underlined headings in this Agreement are for convenience only and will not affect the interpretation of this Agreement.

S. **Modifications; Electronic Signatures.** The terms of this Agreement may only be modified or amended by a written agreement signed by authorized representatives of Walmart and Contractor. The Parties consent to use facsimile, electronic and/or digital signatures to execute this Agreement, and the same are binding upon the Parties as if they were original signatures.