Waste Management – Privacy and Data Protection

During the course of providing products and Services, Supplier may be provided access to or otherwise obtain or handle Waste Management Data (as defined below). Without limiting any of Supplier's obligations with respect to Company's confidential information that are contained elsewhere in the Agreement, Supplier agrees to protect all Waste Management Data as detailed in this Attachment.

1. Definitions and Interpretation. For purposes hereof, the following definitions shall apply:

a. "Cardholder Data" has the then-current meaning given in the PCI-DSS (as defined below).

b. "Data Protection Requirements" means, collectively, all national, state and local laws and regulations relating to Personally Identifiable Information in the jurisdictions in which Waste Management Entities (as defined below) do business and that apply with respect to Supplier's handling of Waste Management Data.

c. "Internal Data" means all information (regardless of form) of any Waste Management Entity (as defined below), whether disclosed to or accessed by Supplier in connection with the Agreement, that is not available to the general public, but which does not qualify as Personally Identifiable Data. For the avoidance of doubt, unless such information otherwise meets the definition of Personally Identifiable Data, Internal Data includes, without limitation, all information the Waste Management Entities may possess that is subject to an obligation to maintain the confidentiality of same.

d. "PCI-DSS" means the then-current Payment Card Industry Data Security Standard for the protection of payment card data with which the payment card companies require merchants or service providers to comply.

e. "Personally Identifiable Data" means all information (regardless of form) of any Waste Management Entity (as defined below) 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. Personally Identifiable Data includes, without limitation, the following: (i) identifiers such as a real name, alias, signature, postal address, telephone number, unique personal identifier, online identifier, Internet Protocol address, email address, account name or other similar identifiers; (ii) Special Personally Identifiable Data (as defined below); (iii) commercial information and customer records, including, without limitation, records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies; (iv) Internet or other electronic network activity information, including, without limitation, browsing history, search history and information regarding an individual's interaction with an Internet Web site, application or advertisement; (v) geolocation data; (vi) audio, electronic, visual, thermal, olfactory or similar information; (vii) professional or employment-related information; (viii) education information; (ix) information about transactions with Waste Management Entities; and (x) inferences drawn from any of the information identified in clauses (i) through (ix) of this definition to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes. However, Personally Identifiable Data does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

f. "Protected Health Information" has the then-current meaning given in the HIPAA Privacy Rule (45 C.F.R. Part 160 and Subparts A and E of Part 164).

g. "Sensitive Authentication Data" has the then-current meaning given in the PCI-DSS (as defined above).

h. "Special Personally Identifiable Data" means the following types of Personally Identifiable Data: (i) social security number, taxpayer identification number, passport number, driver's license number and other government-issued identification numbers; (ii) Cardholder Data, Sensitive Authentication Data, financial account number, debit card number, insurance policy number and credit report information, in each case with or without any code or password that would permit access to the account; and (iii) an individual's Protected Health Information, race, religion, ethnicity, biometric data (e.g., fingerprints, retina scans, etc.), digital signature files (i.e., digital identification keys, not scanned images of an individual's signature on paper), background check information and sexual orientation.

i. "Waste Management Data" means, collectively, Personally Identifiable Data, Special Personally Identifiable Data and Internal Data.

j. "Waste Management Entities" means, collectively, Waste Management, Inc. and all entities controlling, controlled by or under common control with Waste Management, Inc. For purposes of this definition: (i) "entity" means any company, partnership, joint venture or other form of enterprise, domestic or foreign; and (ii) "control" and its derivatives means, with respect to any entity, the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity, whether through the ownership of voting securities (or other ownership interest), by contract or otherwise.

k. "Waste Management Systems" means the equipment, software and networks that are operated by or on behalf of any Waste Management Entity.

All references in this Attachment to Waste Management Data, Personally Identifiable Data, Special Personally Identifiable Data, Cardholder Data, Sensitive Authentication Data and Internal Data are to information (regardless of form) that is provided to, or obtained, used, accessed, maintained, developed, produced, processed, stored, transmitted or otherwise handled by or on behalf of, Supplier in connection with providing products and Services, including, without limitation, any additions, modifications, substitutions, upgrades and enhancements thereto and thereof. To the extent the designation of any data or information as Waste Management Data, Personally Identifiable Data, Special Personally Identifiable Data or Internal Data in this Attachment conflicts with any definition of or provisions regarding confidential, proprietary or similar information within the body of the Agreement or any separate agreement, to the fullest extent possible, such conflict shall be interpreted as this Attachment imposing additional or supplemental responsibilities and obligations in connection with such information and not as creating a conflict therewith; provided, however, that if and to the extent any such conflict cannot be resolved in accordance with this sentence, this Attachment shall take precedence and control over any conflict.

2. General Obligations.

a. Supplier shall at all times comply with and treat Waste Management Data in accordance with the requirements of this Attachment and the Data Protection Requirements. Supplier hereby represents and warrants that it shall inform itself regarding, and comply with, all applicable Data Protection Requirements. Supplier shall notify Company in the event that Supplier believes that Company's instructions concerning Waste Management Data, including, without limitation, the requirements of this Attachment, would cause Supplier to violate any Data Protection Requirement. Supplier represents and warrants that it shall not take any actions that shall compromise Company's ability to comply with any Data Protection Requirement.

b. Supplier shall hold Waste Management Data in strict confidence. Except as may be permitted pursuant to this Section, Supplier shall not disclose Waste Management Data to any third party, firm or enterprise, including, without limitation, Supplier's affiliates. Except as may be permitted pursuant to this Section, Supplier shall not use (directly or indirectly) any Waste Management Data for any purpose other than as required to provide roducts and Services.

c. Before providing Waste Management Data to any third party, including, without limitation, any affiliate or potential subcontractor or service provider, Supplier must obtain written approval for such disclosure from an officer of Company, to be given in Company's sole discretion. If Supplier is permitted to disclose Waste Management Data to such third party, such disclosure must be limited to the minimum amount of Waste Management Data necessary for the third party to fulfill its obligations to Supplier. Supplier agrees that if Company consents to Supplier's disclosure of Waste Management Data to such third party, prior to making such disclosure, Supplier shall enter into a written agreement with the third party that includes obligations that are at least as broad in scope and restrictive as those under this Attachment. Nonetheless, Supplier shall remain at all times accountable and responsible for all acts and omissions by such third parties with respect to the disclosed Waste Management Data as if such third parties were a party to this Agreement, including, without limitation, their compliance with the provisions of this Attachment and their violation of applicable Data Protection Requirements.

d. Supplier shall not be entitled to use Waste Management Data for its own purposes or for the purpose of any third party. Without the prior written approval of an officer of Company, to be given in Company's sole discretion, Waste Management Data shall not, other than as required to provide products and Services, be used, monitored, analyzed, individualized, anonymized, aggregated, sold, rented or otherwise commercially exploited in any form (including, without limitation, any individualized, anonymized or aggregated form).

e. At no time shall Supplier acquire any ownership, license, rights, title or other interest in or to Waste Management Data, all of which shall, as between Company and Supplier, be and remain the proprietary and confidential information of Company. Supplier hereby does, and shall cause its personnel, subcontractors and service providers to, irrevocably, perpetually and unconditionally assign to Company without further consideration all rights, title, and interest each may have in any Waste

Management Data, including any intellectual property and other proprietary rights in, to and under the Waste Management Data. Such rights shall vest in Company upon creation of the relevant Waste Management Data.

f. Without limiting Supplier's obligations under the Agreement, Supplier shall develop, implement, monitor, maintain and comply with written processes and procedures for the back-up, storage and remediation of errors, destruction, loss or alteration of Waste Management Data in Supplier's possession or control. Supplier shall promptly notify Company of any errors in, or destruction, loss, or alteration of, any Waste Management Data of which it is aware, and promptly remediate such errors, destruction, losses or alterations that are caused by Supplier or any of Supplier's personnel, subcontractors or service providers at no cost or expense to Company.

g. Upon notice to Supplier, Supplier shall promptly assist and support Company in the event of an investigation by any governmental authority, if and to the extent that such investigation relates to Waste Management Data handled by Supplier. Such assistance and support shall be at Company's sole expense, except where such investigation was required due to Supplier's acts or omissions, in which case, such assistance and support shall be at Supplier's sole expense.

h. Except to the extent otherwise expressly required by applicable law, Supplier shall notify Company within twenty-four (24) hours of receiving any judicial or administrative order, request or inquiry by a governmental authority or any litigant (whether by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or other similar processes) seeking access to or disclosure of Waste Management Data. Company shall have the right, at its own expense, to defend any associated claim in lieu of and on behalf of Supplier. Supplier shall reasonably cooperate with Company in such defense as required by Company. If and to the extent that Supplier is compelled to disclose any Waste Management Data by any mandatory judicial or administrative order, Supplier shall use commercially reasonable efforts to prevent and limit any such disclosure to only such Waste Management Data as Supplier's legal counsel has determined is required to be produced and to otherwise preserve the confidentiality of Waste Management Data, including, without limitation, by cooperating with Company to obtain an appropriate protective order or other reliable assurance that confidential treatment shall be accorded to Waste Management Data.

3. Specific Obligations. Without limiting Supplier's obligations under Section 2 of this Attachment:

a. Supplier shall develop, implement, monitor, maintain and comply with a comprehensive, written system and information security program (the "Data Safeguards") that includes administrative, electronic and physical protocols and controls to safeguard the security, confidentiality and integrity of, prevent the unauthorized or accidental destruction, damage, loss, alteration and use of, and prevent unauthorized physical and electronic access to or acquisition of, Waste Management Systems and Waste Management Data. The Data Safeguard's shall comply with Company's information security policies, practices and requirements as may be issued to Supplier by Company from time to time (including, without limitation, enhanced security provisions governing the use of Special Personally Identifiable Data in order to comply with applicable laws), and shall be no less rigorous than the most stringent of (i) the data security guidelines and requirements set forth this Attachment, (ii) industry standards adopted or required by Company, including, without limitation, the PCI-DSS (to the extent that any Cardholder Data or Sensitive Authentication Data is accessed, used, processed, stored, transmitted or otherwise handled by or on behalf of Supplier in connection with providing products and Services), ISO 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements), ISO 27002:2013 (Information technology – Security techniques – Code of practice for information security management) and, to the extent any cloud-based technology is used to provide the Services, ISO 27017:2015 (Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services) and ISO 27018:2014 (Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors), (iii) the Data Protection Requirements and (iv) prevailing industry practices. Supplier shall maintain and enforce the Data Safeguards at each location from which Supplier or any of its personnel, subcontractors or service providers provides any products or Services. In addition, Supplier shall ensure that the Data Safeguards cover all networks, systems, servers, computers, notebooks, laptops, portable devices, storage media, and other devices and media that process or handle Waste Management Data, or that provide access to Waste Management Data or Waste Management Systems. Supplier shall provide Company with documentation of the Data Safeguards upon Company's request at any time. Supplier shall not alter or modify the Data Safeguards in such a way that shall weaken or compromise the confidentiality and security of Waste Management Data or Waste Management Systems or render Supplier non-compliant with the requirements of this Attachment.

b. The Data Safeguards shall include, without limitation, the following: (i) appropriate access controls consistent with prevailing industry practices, which as of the inception of the Agreement, includes, without limitation, limiting access to the minimum amount of Waste Management Data by the minimum number of Supplier personnel who require such access in order to provide products and Services; and (ii) proven, up-to-date, industry-standard password protections, firewalls and anti-virus and malware protections to protect Waste Management Data stored on Supplier's computer systems.

c. Supplier shall encrypt, using industry standard encryption tools, all records and files containing Waste Management Data that Supplier: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; (iii) where technically feasible, stores on portable devices; and (iv) stores on any device that is transported outside of the physical or logical controls of Supplier. Supplier shall safeguard the security and confidentiality of all encryption keys associated with encrypted Waste Management Data. Mere password protection does not meet the requirements of this subsection.

d. Supplier shall take reasonable steps to ensure the reliability of any personnel who shall be provided access to, or otherwise come into contact with, Waste Management Data, ensuring in each case that access is strictly limited to those individuals who necessarily need to know the relevant Waste Management Data for providing products and Services, and ensuring that all such individuals are subject to written confidentiality undertakings or professional or statutory obligations of confidentiality. Without limiting the immediately preceding sentence, with respect to Supplier personnel who shall be provided access to, or otherwise come into contact with, Waste Management Data, Supplier shall: (i) require such personnel to protect Waste Management Data in accordance with the requirements of Sections 2(b) and 2(c) of this Attachment during the term of their employment or retention and thereafter; (ii) provide such personnel with appropriate training regarding information security and the protection of personal information, such training to occur at least annually or whenever there is a change in Supplier's computer systems, business practices, or industry standards applicable to the security, confidentiality or integrity of Waste Management Data, or as otherwise requested by Waste Management; and (iii) ensure that such personnel shall have the appropriate qualifications and references to handle and to protect Waste Management Data in accordance with the requirements of this Attachment (which include, without limitation, a requirement that Supplier conduct drug and background checks of such personnel prior to such personnel accessing or otherwise coming into contact with any Waste Management Data in accordance with Supplier's Safety and Health Declaration).

e. If Supplier connects or is provided with access to any Waste Management System, Supplier agrees that: (i) Supplier shall not access, and shall not permit any other entity to access, any Waste Management System without the prior written authorization of an officer of Company, to be given in Company's sole discretion, and any such actual or attempted access shall be consistent with any such authorization; (ii) all Supplier connectivity to the Waste Management System and all attempts at same shall be only through Company's security gateways/firewalls; and (iii) Supplier shall use proven, up-to-date, industry-standard virus and malware detection/scanning programs to detect and prevent malware from transferring from Supplier's computer systems to any Waste Management System. In addition, Supplier shall obtain Company's prior authorization, to be given in Company's sole discretion, for all Supplier personnel who are granted access to any Waste Management System, and any such access shall be consistent with any such authorization.

4. Personally Identifiable Data. Without limiting Supplier's other obligations under this Attachment, the following provisions shall apply to Personally Identifiable Data. If and to the extent that any of the other provisions of this Attachment purporting to apply to Personally Identifiable Data conflict or are inconsistent with the provisions of this Section, the provisions of this Section shall take precedence and control.

a. Except to the extent otherwise expressly approved in writing by an officer of Company (to be given in Company's sole discretion) or, if and to the extent required by Data Protection Requirements, otherwise requested by the individual data subject, Supplier shall only use, access, process, manage, transfer and disclose Personally Identifiable Data as required to provide products and Services and only in the minimum amount and to the minimum number of third parties necessary to provide products and Services. Supplier shall not use, access, process, manage, transfer or disclose Personally Identifiable Data to the extent such use, accessing, processing, managing, transferring or disclosure would violate any Data Protection Requirement if done by Company. To the extent that the provision of products and Services involves or necessitates the processing of Personally Identifiable Data, Supplier shall act only on instructions and directions from Company, including, without limitation, as set forth in the Agreement. Supplier shall promptly comply (which shall in no event be longer than any time frame for compliance required by applicable Data Protection Requirements) with any request from Company to access or amend any Personally Identifiable Data or that is necessary to allow Company to comply with applicable Data Protection Requirements.

b. Supplier shall not physically transfer Personally Identifiable Data to, or allow access to Personally Identifiable Data by, its personnel or any third party (including, without limitation, Supplier's affiliates) in or from any location outside the United States of America, without first receiving the prior written approval of an officer of Company, to be given in Company's sole discretion.

c. Supplier shall notify Company promptly in writing (and in any event within five (5) days of receipt) of any communication received from an individual relating to his or her request to access, modify, correct or otherwise exercise a consumer data right relating to Personally Identifiable Data relating to the individual, or his or her request to provide details regarding the processing of Personally Identifiable Data relating to the individual (including, without limitation, the subject matter, duration, the nature and purpose of processing, the types of their Personally Identifiable Data and the categories of data subjects), and in each case Supplier shall comply with all instructions of Company before responding to such communications.

d. Supplier shall document disclosures to third parties of Personally Identifiable Data and information related to such disclosures as would be required for Company to respond to a request by an individual for an accounting of disclosures of his or her Personally Identifiable Data.

e. Supplier shall not store any Personally Identifiable Data on any laptops, portable storage media or other portable devices, or any device that is transported outside of the physical or logical controls of Supplier, in each case without the prior written approval of an officer of Company, to be given in Company's sole discretion.

f. Supplier shall not transfer Personally Identifiable Data directly from a country within the European Economic Area or Personally Identifiable Data originating from such a country (even if stored outside the European Economic Area) to countries deemed by the European Union not to have adequate level of protection for Personally Identifiable Data (nor shall Supplier access Personally Identifiable Data originating from such countries) without first ensuring that such transfers comply with the requirements of the standard contractual clauses approved by the European Commission in European Commission implementing decisions as the standard contractual clauses for the transfer of personal data to data processors in third countries pursuant to Regulation (EU) 2016/679 are in place between the data exporter (which could be Company or any other Waste Management Entity, as designated by Company) and the data importer, in each case to the extent applicable to the relevant transfer. The Parties agree to comply with the requirements of such standard contractual clauses. In the event of any conflict between the terms of this Attachment on the one hand and such standard contractual clauses on the other hand, terms that are more protective of Personally Identifiable Data shall take precedence and control; in case of doubt which term is more protective, the requirements of the standard contractual clauses shall prevail. If, according to legislation (especially legislation replacing Regulation (EU) 2016/679), a decision by a court, the European Commission, or an official statement of a data protection authority in the European Union, the standard contractual clauses do not provide for adequate protection allowing the lawful transfer of Personally Identifiable Data, the Parties shall agree on a different mechanism (however, excluding an obligation of any Waste Management Entity to obtain consent from individuals) under which Supplier shall be able to receive and access Personally Identifiable Data at no cost or expense to Company.

g. The Parties acknowledge that, for purposes of Regulation (EU) 2016/679 and implementing legislation promulgated by the member states of the European Union, Supplier shall be a "processor" of Personally Identifiable Data in its possession and Company shall be the "controller" of Personally Identifiable Data, as the terms "processor" and "controller" are defined in Regulation (EU) 2016/679. Company shall be solely responsible for determining the purposes for which and the manner in which Personally Identifiable Data is to be processed.

h. If any Protected Health Information is accessed, used, processed, stored, transmitted or otherwise handled by or on behalf of Supplier in connection with providing products and Services, then if requested by Company, Supplier shall execute a Business Associate Agreement containing, at a minimum, any terms required by applicable Data Protection Requirements. The Parties agree to comply with such Business Associate Agreement. In the event of any conflict between the terms of this Attachment and the terms of the Business Associate Agreement, the terms that are more protective of Protected Health Information shall take precedence and control; in case of doubt which term is more protective, the requirements of the Business Associate Agreement shall prevail.

i. If any Cardholder Data or Sensitive Authentication Data is accessed, used, processed, stored, transmitted or otherwise handled by or on behalf of Supplier, or if Supplier could impact the security of any of Company's Cardholder Data or Sensitive Authentication Data environments, in each case in connection with providing products and Services, then Supplier shall comply with the PCI-DSS, ensure that the Data Safeguards address and comply with the requirements of the PCI-DSS, maintain a complete audit trail of all transactions and activities associated with Cardholder Data and Sensitive Authentication Data, and not store any Sensitive Authentication Data on any devices. Supplier represents and warrants that it shall not take any actions that shall compromise Company's ability to comply with the PCI-DSS. Supplier further represents and warrants that it shall maintain current certification of its compliance with the PCI-DSS, certified by an independent third party recognized by the payment card industry for that purpose. Without limiting the foregoing requirements of this subsection:

i. Supplier shall perform all tasks, assessments, reviews, penetration tests, scans and other activities required under the PCI-DSS for Level 1 Merchants or Service Providers, as applicable (including, without limitation, any compliance guidance issued by the PCI Security Standards Council or its subordinate bodies), or otherwise to validate its compliance with the PCI-DSS as they relate to any system elements and portions of Company's Cardholder Data or Sensitive Authentication Data environment for which Supplier is responsible (the "PCI Environment").

ii. Supplier shall deliver to Company copies of all documentation necessary to verify Supplier's compliance with the requirements of clause (i) of this subsection ("Verification Documentation"). If Company determines that additional Verification Documentation is required under the PCI-DSS or is likely to be so

required to verify such compliance, including a "Report on Compliance," and an associated unqualified "Attestation of Compliance," then Supplier shall provide such additional Verification Documentation to Company within six (6) months from the date of Company's request or within the timeframe required for Company to remain compliant, whichever occurs first. At least annually thereafter for so long as such documentation is required under the PCI-DSS, Supplier shall deliver to Company a copy of the Verification Documentation applicable to the PCI Environment.

iii. At least quarterly, Supplier shall deliver to Company evidence of a passing vulnerability scan applicable to the PCI Environment conducted within the preceding three (3) months by an independent third party recognized by the payment card industry for that purpose.

iv. Supplier shall notify Company within twenty-four (24) hours of any exception in a Report on Compliance, Attestation of Compliance or quarterly vulnerability scan, or if it learns that it is no longer compliant with the PCI-DSS or reasonably anticipates that it is or shall be non-compliant and shall identify in such notice the steps being taken to remediate such exception or non-compliance.

5. Data Breach.

a. If Supplier discovers or is notified of any suspected or actual unauthorized access, acquisition, destruction, encryption, modification, disclosure, copying or use of any Waste Management Systems that Supplier may access or Waste Management Data that is in Supplier's possession or control (each, a "Data Breach"), then in each case Supplier shall, at Supplier's sole cost and expense:

i. notify Company at BreachReporting@wm.com immediately (but in any event within twenty-four (24) hours of becoming aware thereof) of the date and circumstances of the Data Breach, the nature and content of the Waste Management Data affected (including, if the event is a Personal Data Breach (defined below), the categories and approximate number of data subjects concerned and the categories and approximate number of records concerned), and a description of the likely consequences of the Data Breach;

ii. investigate and determine the exposures that led to the Data Breach;

iii. take all necessary steps to eliminate or contain the exposures that led to the Data Breach;

iv. conduct a post-incident review of all events and actions taken, if any, with a view to making any needed modifications in Supplier's computer systems or business practices relating to the protection of Waste Management Data;

v. within thirty (30) days from the date of discovery of the Data Breach, provide Company with a detailed report indicating the exposures that led to the Data Breach, and an action plan for Company's approval that addresses and corrects those exposures and includes appropriate preventive measures so that the exposures that led to the Data Breach do not recur;

vi. implement the Company-approved action plan in accordance with its terms;

vii. assemble, document and preserve all information collected as part of its investigation of the Data Breach, and all actions taken in response to the Data Breach, in each case in sufficient detail to meet reasonable expectations of forensic admissibility;

viii. cooperate with any investigation relating to the Data Breach that is carried out at the direction of any governmental authority;

ix. assist and cooperate with Company in connection with Company's and its designees' efforts to investigate, respond to, prevent the recurrence of, mitigate and rectify the Data Breach; and

x. regularly (but in any event as requested by Company) keep Company advised as to the status of the Data Breach and all matters related thereto, including, without limitation, Supplier's efforts pursuant to this subsection.

b. In addition to its obligations under subsection (a) of this Section, if a Data Breach involves any Personally Identifiable Data (a "Personal Data Breach"), then if and to the extent required by Company, Supplier shall at its sole cost and expense:

i. assist and cooperate with Company concerning any notifications and other communications to affected individuals, potentially affected individuals, governmental authorities or similar third parties as Company deems appropriate;

ii. establish and maintain for at least two (2) years from the date of the discovery of the Personal Data Breach an informational website in a form and with content specified by Company prior to its posting, for the purposes of providing information to individuals affected and potentially affected by the Personal Data Breach, including, without limitation, providing all associated equipment, software, Internet connectivity and website security;

iii. establish and maintain a telephone call center that is available twenty-four (24) hours a day, seven (7) days a week, for the purposes of answering questions from individuals affected and potentially affected by the Personal Data Breach for a period of not less than six (6) months after the last notification of the Personal Data Breach is delivered to affected and potentially affected individuals, provided that such call center must use Company-provided scripts; and

iv. for a period of at least two (2) years from the date of the discovery of the Personal Data Breach, provide all individuals affected and potentially affected by the Personal Data Breach with identity theft protection that is equivalent to or better than credit monitoring or a protective service and which includes automatic, daily monitoring of all three credit bureaus, fraud victim assistance, One Million Dollars ($1,000,000.00) in identity theft insurance with no deductible, a help desk that is available twenty-four (24) hours a day, seven (7) days a week, and free credit reports.

c. Supplier shall not disclose the existence of any Data Breach or any related information to any individual or any third party without first consulting with, and obtaining the permission of, Company, except as necessary to notify Company, law enforcement, and Supplier's insurers, legal counsel and public relations firms, or as expressly required by applicable Data Protection Requirements. Company shall have final editorial control over the content of any filings, communications, notices, press releases, reports and other disclosures related to any Data Breach.

d. Supplier shall reimburse Company for all costs and expenses incurred by Company in connection with investigating, responding to, preventing the recurrence of, mitigating and rectifying any Personal Data Breach, including, without limitation: (i) reconstruction, recovery, or restoration of Waste Management Data; (ii) forensic and investigation services to investigate the existence and cause of the event and the extent to which Personally Identifiable Data was involved; (iii) preparation and mailing or other transmission of notifications or other communications to any affected individuals, potentially affected individuals, governmental authorities or similar third parties as Company deems appropriate; (iv) public relations and other similar crisis management services; (v) legal, consulting and accounting expenses associated with Company's investigation of and response to the event; (vi) any governmental fines and penalties; (vii) establishing and maintaining the informational website and telephone call center described in clauses (ii) and (iii) of Section 5(b) of this Attachment; and (viii) providing identity theft protection to affected individuals as described in clause (iv) of Section 5(b) of this Attachment.

e. If a Data Breach occurs, Company shall be entitled (at its option and in its sole discretion) to suspend the transfer of Waste Management Data, require Supplier to cease using relevant Waste Management Data and/or immediately terminate the Agreement, in each case without liability or penalty and without payment of any termination charges. Company's exercise of any of the foregoing rights shall not be considered Company's breach of the Agreement.

6. Destruction and Return of Data.

a. Supplier shall (i) promptly provide to Company, in a structured and industry-standard format and on industry-standard media, all or any part of any Waste Management Data in Supplier's possession or control, without additional charge and regardless of whether a dispute may exist, and (ii) unless otherwise specifically directed by Company, destroy all or any part of any Waste Management Data in Supplier's possession or control in accordance with subsection (b) of this Section, in each case upon the earliest of (A) the date of Company's request with respect to all or the specified portion of Waste Management Data, (B) such date on which any Waste Management Data is no longer necessary for purposes of providing products and Services with respect to such Waste Management Data, and (C) the effective date of the expiration or any termination of the Agreement with respect to all Waste Management Data. Upon Company's request, Supplier shall certify to Company that Supplier has complied with the immediately preceding sentence in a notice signed by an officer of Supplier. Supplier shall not withhold any Waste Management Data as a means of resolving any dispute.

b. If Supplier disposes of any paper, electronic or other record containing Waste Management Data (whether or not such Waste Management Data has been intermingled with Supplier's own information or materials), Supplier shall do so by taking all reasonable steps (based on the sensitivity of the Waste Management Data) to destroy the Waste Management Data by: (i) shredding; (ii) permanently and securely erasing and deleting; (iii) degaussing; or (iv) otherwise modifying Waste Management Data in such records to make it unreadable, unreconstructable and indecipherable. All Special Personally Identifiable Data must be disposed of in a manner described in clauses (i) through (iii) of this subsection immediately following such date that the Special Personally Identifiable Data is no longer required to fulfill its obligations under the Agreement.

c. Company may identify to Supplier any part of any Waste Management Data that is subject to a litigation hold or is otherwise not to be destroyed by Supplier. Supplier shall refrain from destroying such Waste Management Data and shall maintain such Waste Management Data in accordance with Company's instructions.

7. Testing.

a. Supplier shall regularly test (and re-test as necessary) and monitor Supplier security procedures and systems, shall conduct periodic reviews to ensure compliance with the requirements set forth in this Attachment, and implement action plans to remediate identified deficiencies. Supplier shall make the results of such reviews available to Company at Company's request.

b. Without limiting Supplier's obligations under subsection (a) of this Section, Supplier shall:

i. review, test (and re-test as necessary) and, as appropriate, revise the Data Safeguards: (A) at least annually or whenever there is a change in Supplier's computer systems or business practices that may adversely affect the security, confidentiality or integrity of Waste Management Data; and (B) as reasonably requested by Company. If Supplier modifies the Data Safeguards following such a review, Supplier shall promptly notify Company of the modifications and shall provide the modifications to Company in writing upon Company's request.

ii. obtain annually, at no additional cost or expense to Company, Service Organization Controls ("SOC") 1 and SOC 2 Type II auditor's reports from a tier 1 or 2 auditing firm for all accounting or internal control systems and activities related to the provision of products and Services and for each facility from which the products and Services are provided (whether by Supplier or any third party supporting the products and Services). The SOC 1 reports shall be issued under the Statements on Standards for Attestation Engagements ("SSAE") No. 18 attest standard. The SOC 2 reports shall be issued under the AT Section 101 attest standard, and shall cover the Trust Service Principles, and Criteria (which include: security, availability, processing integrity, confidentiality and privacy). Each SOC 1 and SOC 2 report shall be completed for the twelve (12) months immediately preceding September 30 of each year, and each such report shall be provided to Company within fifteen (15) days of Supplier's receipt thereof (but in any event no later than November 15 of each year). Supplier shall provide promptly, but no later than January 15 of each year, a written statement as of January 15 of each year attesting that (A) the controls existing as of the most recent SOC 1 and SOC 2 report remain in effect, and (B) no significant deficiency or material weaknesses (as defined by the Public Company Accounting Oversight Board (PCAOB)) have been identified during the period of time from the most recent SOC 1 and SOC 2 report that could affect such controls.

iii. at Company's request, complete Company's standard information security questionnaire, which shall include responses to any questions regarding Supplier's controls for any part of the products and Services performed by a third party by or on behalf of Supplier.

iv. make available an appropriate senior representative of Supplier's information security team to meet with Company's information security team to discuss any questions or concerns Company may have regarding the Data Safeguards.

8. Records and Assessments.

a. Supplier shall establish and maintain complete and accurate books, notices and accounting and administrative records necessary to document compliance with this Attachment, including, without limitation, accounts of all transactions involving Waste Management Data, and shall retain such records in accordance with Company's then-current record retention policies during the term of the Agreement and for at least seven (7) years thereafter.

b. Upon at least five (5) days' prior notice to Supplier, Supplier shall permit Company, its auditors, designated audit representatives and regulators, including, without limitation, data protection regulators, to audit and inspect, at Company's sole

expense (except as provided herein), and no more often than once per year (unless otherwise required by Company's regulators or applicable law, or unless a prior audit or inspection revealed any deficiency): (i) the facilities of Supplier and any third party subcontractors and service providers of Supplier where Waste Management Data is stored or maintained by or on behalf of Supplier; (ii) any computerized or paper systems used to share, disseminate or otherwise handle Waste Management Data; (iii) Supplier's security practices and procedures, facilities, resources, plans and procedures; and (iv) all books, notices and accounting and administrative records required to be retained by Supplier hereunder. Such audit and inspection rights shall be, at a minimum, for the purpose of verifying Supplier's compliance with this Attachment, all applicable Data Protection Requirements and the PCI-DSS. If any audit or inspection conducted pursuant to this subsection reveals a bona fide technical issue, security problem or other non-compliance with this Attachment, any applicable Data Protection Requirements and/or the PCI-DSS, Supplier shall pay Company's costs for conducting such audit or inspection, and within thirty (30) days after the completion of such audit or inspection shall propose an appropriate written response, including, without limitation, a plan for the remediation of the problem within the timeframe reasonably requested by Company. Upon Company's approval of such plan, Supplier shall implement the Company-approved plan in accordance with its terms. Company shall not be responsible for any additional costs or fees related to such remedy.

c. Company may perform periodic security assessments of the Waste Management Systems, which may include, without limitation, assessment of certain portions of the computing systems and networks of Supplier. Supplier agrees that should any such assessment reveal inadequate security by Supplier, Company, in addition to other remedies it may have, may suspend Supplier's access to Waste Management Systems until such inadequate security has been appropriately addressed. Such suspension shall not be considered Company's breach of the Agreement.

9. INDEMNITIES. SUPPLIER SHALL INDEMNIFY, HOLD HARMLESS, AND (AT COMPANY'S OPTION, IN ITS SOLE DISCRETION) DEFEND COMPANY, WASTE MANAGEMENT ENTITIES, AND ITS AND THEIR OFFICERS, DIRECTORS, SHAREHOLDERS, EMPLOYEES, AGENTS, SUCCESSORS, ASSIGNS, AND SUBCONTRACTORS FROM AND AGAINST ANY AND ALL THREATENED CLAIMS, LOSSES, LIABILITIES, DAMAGES, SETTLEMENTS, EXPENSES AND COSTS ARISING FROM, IN CONNECTION WITH, OR BASED ON ALLEGATIONS OF, IN WHOLE OR IN PART, ANY OF THE FOLLOWING: (A) ANY VIOLATION OF THE REQUIREMENTS OF THIS ATTACHMENT OR THE DATA PROTECTION REQUIREMENTS; (B) ANY DATA BREACH OR PERSONAL DATA BREACH; (C) ANY NEGLIGENCE, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF SUPPLIER, ANY OF SUPPLIER'S PERSONNEL, SUBCONTRACTORS OR SERVICE PROVIDERS, OR ANY THIRD PARTY TO WHOM SUPPLIER PROVIDES ACCESS TO WASTE MANAGEMENT DATA OR WASTE MANAGEMENT SYSTEMS, WITH RESPECT TO THE SECURITY, CONFIDENTIALITY OR INTEGRITY OF WASTE MANAGEMENT DATA AND WASTE MANAGEMENT SYSTEMS; (D) ANY REMEDIAL ACTION TAKEN BY COMPANY IN CONNECTION WITH ANY DATA BREACH; AND (E) ANY OTHER COSTS AND EXPENSES INCURRED BY COMPANY WITH RESPECT TO COMPANY'S EXERCISE OF ITS RIGHTS IN THIS ATTACHMENT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS ATTACHMENT, SUPPLIER SHALL BE FULLY RESPONSIBLE FOR, AND SHALL PAY, ALL COSTS AND EXPENSES INCURRED BY SUPPLIER OR ITS PERSONNEL OR AGENTS WITH RESPECT TO SUPPLIER'S PERFORMANCE OF ITS OBLIGATIONS UNDER THIS ATTACHMENT.

10. General.

a. Supplier shall designate a management level employee as Supplier's primary security manager under the Agreement who shall be available to assist Company twenty-four (24) hours a day, seven (7) days a week. Supplier's primary security manager shall be responsible for managing and coordinating the performance of Supplier's obligations set forth in this Attachment.

b. The Parties agree that, to the extent such entity is not a party to the Agreement, each of the Waste Management Entities are intended third party beneficiaries of the provisions of this Attachment and the privacy and data security provisions of the Agreement and such provisions are intended to inure to the benefit of the Waste Management Entities. Without limiting the immediately preceding sentence, the Waste Management Entities shall be entitled to enforce the provisions of this Attachment and all privacy and data security provisions of the Agreement as if each was a signatory to the Agreement.

c. Supplier agrees that, due to the unique nature of Waste Management Data, the unauthorized disclosure or use of Waste Management Data may cause irreparable harm to Company, the extent of which shall be difficult to ascertain and for which there shall be no adequate remedy at law. Accordingly, Supplier agrees that Company, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief enjoining any breach or threatened breach of the provisions of this Attachment without the necessity of posting any bond or other security.

d. Upon Company's request, Supplier shall certify in writing and, when specified, demonstrate to Company, Supplier's compliance with the provisions of this Attachment.

e. In the event that Supplier fails or is unable to comply with the obligations stated in this Attachment, Supplier shall promptly notify Company, and Company shall then be entitled (at its option and in its sole discretion) to suspend the transfer of Waste Management Data, require Supplier to cease using relevant Waste Management Data and/or immediately terminate the Agreement, in each case without liability or penalty and without payment of any termination charges. Company's exercise of any of the foregoing rights shall not be considered Company's breach of the Agreement.