Waste Management Policy

PRIVACY AND DATA PROTECTION

October 2020

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 the confidential information of Waste Management ("Waste Management" or "Company") 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. "Address Harvesting" means the use of a computer program that is designed or marketed for, or used in generating or searching for, and collecting, electronic addresses; or the use of an individual's electronic address that was collected by the use of such a computer program.

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

c. "Commercial Electronic Message" includes any message that is sent in association with the Services to an electronic mail account, instant messaging or SMS account, telephone account, social media account or any similar account by any means of telecommunication, including a text, sound, voice or image message.

d. "Data Protection Requirements" means, collectively, all national, state, provincial/territorial, and local laws, regulations, rulings, and guidelines 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 (including, without limitation, in the United States of America, the Gramm-Leach-Bliley Act and in Canada, the Personal Information Protection and Electronic Documents Act, and the substantially similar provincial privacy laws, and any successors thereto).

e. "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.

f. "PCI Standards" means the then-current security standards for the protection of payment card data with which the payment card companies require merchants or service providers to comply, including, without limitation, the then-current Payment Card Industry Data Security Standards (PCI DSS).

g. "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 identifying, 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, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99); (ix) information about transactions with Waste Management Entities; (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 or other attributes and (xi) such other information as may be subject to the Data Protection Requirements.

be a "processor" of Personally Identifiable Data in its possession and Waste Management shall be the "controller" of Personally Identifiable Data, as the terms "processor" and "controller" are defined in Regulation (EU) 2016/679. Waste Management 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 Waste Management, 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 Waste Management'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 Standards, ensure that the Data Safeguards address and comply with the requirements of the PCI Standards, 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, including but not limited to laptops, portable storage media or other portable devices, or any device that is transported outside of the physical or logical controls of Supplier. Supplier represents and warrants that it shall not take any actions that shall compromise Waste Management's ability to comply with the PCI Standards. Supplier further represents and warrants that it shall maintain current certification of its compliance with the PCI Standards, 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 Standards 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 Standards as they relate to any system elements and portions of Waste Management's Cardholder Data or Sensitive Authentication Data environment for which Supplier is responsible (the "PCI Environment").

ii. Supplier shall deliver to Waste Management copies of all documentation necessary to verify Supplier's compliance with the requirements of clause (i) of this subsection ("Verification Documentation"). If Waste Management determines that additional Verification Documentation is required under the PCI Standards 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 Waste Management within six (6) months from the date of Waste Management's request or within the timeframe required for Waste Management to remain compliant, whichever occurs first. At least annually thereafter for so long as such documentation is required under the PCI Standards, Supplier shall deliver to Waste Management a copy of the Verification Documentation applicable to the PCI Environment.

iii. At least quarterly, Supplier shall deliver to Waste Management 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 Waste Management 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 Standards 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, modification, disclosure, copying, loss, or use of any 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 Waste Management 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, the jurisdictions of the data subjects concerned, and the categories and approximate number of records concerned), and a description of the likely consequences of the Data Breach, and shall update such information if more information becomes known;

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 and to eliminate, mitigate, or contain any consequences stemming from 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 Waste Management with a detailed report indicating the exposures that led to the Data Breach, and an action plan for Waste Management'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 Waste Management-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 Waste Management in connection with Waste Management'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 Waste Management) keep Waste Management 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 Waste Management, Supplier shall at its sole cost and expense:

i. assist and cooperate with Waste Management concerning any notifications and other communications to affected individuals, potentially affected individuals, governmental authorities or third parties as Waste Management 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 Waste Management 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 Waste Management-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, Waste Management, except as necessary to notify Waste Management, law enforcement, and Supplier's insurers, legal counsel and public relations firms, or as expressly required by applicable Data Protection Requirements. Waste Management 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 Waste Management for all costs and expenses incurred by Waste Management in connection with investigating, responding to, preventing the recurrence of, mitigating and rectifying any Personal Data Breach, including, without limitation: (i) forensic and investigation services to investigate the existence and cause of the event and the extent to which Personally Identifiable Data was involved; (ii) preparation and mailing or other transmission of notifications or other communications to any affected individuals, potentially affected individuals, governmental authorities or third parties as Waste Management deems appropriate; (iii) public relations and other similar crisis management services; (iv) legal, consulting and accounting expenses associated with Waste Management's investigation of and response to the event; (v) any governmental fines and penalties; (vi) establishing and maintaining the informational website and telephone call center described in clauses (ii) and (iii) of Section 5(b) of this Attachment; and (vii) 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, Waste Management 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. Waste Management's exercise of any of the foregoing rights shall not be considered Waste Management's breach of the Agreement.

6. Destruction and Return of Data.

a. Supplier shall (i) promptly provide to Waste Management, 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, and (ii) unless otherwise specifically directed by Waste Management, 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 Waste Management'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 Waste Management's request, Supplier shall certify to Waste Management 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. Waste Management 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 Waste Management'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 Waste Management at Waste Management'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 Waste Management. If Supplier modifies the Data Safeguards following such a review, Supplier shall promptly notify Waste Management of the modifications and shall provide the modifications to Waste Management in writing upon Waste Management's request.

ii. obtain annually, at no additional cost or expense to Waste Management, 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 Waste Management 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 Waste Management's request, complete a Waste Management 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 Waste Management's information security team to discuss any questions or concerns Waste Management 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 Waste Management'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 Waste Management, its auditors, designated audit representatives and regulators, including, without limitation, data protection regulators, to audit and inspect, at Waste Management's sole expense (except as provided herein), and no more often than once per year (unless otherwise required by Waste Management'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 Standards. 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 Standards, Supplier shall pay Waste Management' 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 Waste Management. Upon Waste Management's approval of such plan, Supplier shall implement the Waste Management-approved plan in accordance with its terms. Waste Management shall not be responsible for any additional costs or fees related to such remedy.

c. Waste Management 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, Waste Management, 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 Waste Management's breach of the Agreement.

9. Indemnities. Supplier shall indemnify, hold harmless, and (at Waste Management's option, in its sole discretion) defend Waste Management, 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 Waste Management in connection with any Data Breach; and (e) any other costs and expenses incurred by Waste Management with respect to Waste Management'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. Collection of Personally Identifying Information, Sending of Commercial Electronic Messages.

a. In any case where Supplier collects or processes Personally Identifiable Data on behalf of Waste Management, then Supplier shall, and will procure that its staff and subcontractors shall:

i. collect and process Personally Identifiable Data solely in accordance with Waste Management's instructions from time to time;

ii. identify to affected individuals the purpose(s) for which it collects and uses Personally Identifiable Data in the course of providing the Services or Products, and ensure that identified purpose(s) are reasonable;

iii. collect only Personally Identifiable Data that is necessary to fulfill the Services and Products;

iv. obtain any required consents from the individuals for the identified purpose(s);

v. Use any form of consent provided by Waste Management, and secure consent to the Waste Management privacy policy; and

vi. provide Waste Management with a record of such consents on request.

b. In any case where Supplier sends Commercial Electronic Messages for Waste Management, Supplier shall:

i. Ensure that each consent to send a Commercial Electronic Message to a recipient as part of or in relation to the Services shall:

(a) be obtained through an unchecked "opt-in" consent mechanism;

(b) use the form of consent provided by Waste Management;

(c) advise the consenting party that he or she may unsubscribe from receiving Commercial Electronic Messages at any time; and

(d) contain all contact information required under the applicable laws.

ii. Ensure that each Commercial Electronic Message sent or caused to be sent as part of or in relation to the Services shall:

(a) be sent only when Supplier has established that it has from the recipient the necessary consents under the applicable laws to send such messages or is otherwise entitled to send such messages pursuant to the applicable laws;

(b) contain a functioning unsubscribe mechanism;

(c) not include any false or misleading representation in the sender information, subject matter information, locator, or body of the message;

(d) not be sent to an electronic address obtained through Address Harvesting; and

(e) contain all contact information required under the applicable laws.

iii. Supplier shall immediately give effect to any unsubscribe requests that it receives in relation to the Services, shall retain evidence of the timely fulfilment of each such unsubscribe request, and shall immediately provide such request to Waste Management.

iv. Supplier will be solely responsible for the compliance of any Commercial Electronic Messages it sends or causes to be sent under this Agreement with the applicable laws, including without limitation, the Data Protection Requirements, and *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act,* SC 2010, c 23 ("CASL"). Waste Management shall be named as the sender of such Commercial Electronic Messages. Any Commercial Electronic Message that names or depicts Waste Management or its intellectual property, products, or services, shall indicate that it is sent by Waste Management, provide the mailing address and at least one of a telephone number, email, or web address for Waste Management, with the contact information for Waste Management being as provided by Waste Management, and an unsubscribe mechanism as may be provided by Waste Management, that allows recipients to add their email address to Waste Management's opt-out list. Prior to sending any such Commercial Electronic Message, Supplier will disclose the addresses to which the Commercial Electronic Messages will be sent ("List") to Waste Management's designated email services provider, for the purpose of scrubbing the List against Waste Management's unsubscribe list, and/or will follow such other processes for scrubbing the List against Waste Management's unsubscribe list as may be directed by Waste Management. Service Provider shall not send a Commercial Electronic Message that references Waste Management, its brands, products, or includes Waste Management CASL disclosure to any address on the unsubscribe list of Waste Management.

11. General.

a. Supplier shall designate a management level employee as Supplier's primary security manager under the Agreement who shall be available to assist Waste Management 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 Waste Management, the extent of which shall be difficult to ascertain and for which there shall be no adequate remedy at law. Accordingly, Supplier agrees that Waste Management, in addition to any other available remedies, shall have the right to seek and obtain 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 Waste Management's request, Supplier shall certify in writing and, when specified, demonstrate to Waste Management, 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 Waste Management, and Waste Management 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. Waste Management's exercise of any of the foregoing rights shall not be considered Waste Management's breach of the Agreement.