Sustainability-Related Policies

Environment

ENVIRONMENTAL POLICY

Purpose: To communicate Management objectives for commitment to human health and the environment. All Waste Management owned, operated or controlled operations, share responsibility to further the goals of this policy.

Policy: Waste Management is committed to protecting human health and the environment. This commitment is a keystone of all that we do, reflected in the services we provide to customers, the design and operation of our facilities, the conditions under which employees work, and our interactions with the communities where we live and do business. We will be responsible stewards of the environment and protect the health and well being of our employees and neighbors.

The following principles are applicable to Company operations worldwide:

- Protection: Conduct all operations in a manner that protects the environment and our employees, neighbors and customers. Proactively work to implement procedures and programs to prevent pollution.
- Compliance: Comply with all legal requirements and proactively implement programs and procedures to ensure compliance.
- Conservation: Practice and promote the conservation of nature and the earth's energy resources.
- Communication: All Waste Management employees are responsible for helping the Company identify and remedy possible violations. Suspicion of violations of law or Waste Management's Core Values of Ethical Conduct and Practices shall be communicated in accordance with the Company's Business Ethics and Compliance Policy and Environmental Reporting and Incident Notification Policy.

The Company has developed processes, procedures and tools for use in achieving its high standards for environmental performance and compliance. They collectively form the WM Environmental Management System (EMS). The Company's operations, across all lines of business, are responsible for implementation and adherence to the WM EMS at each operating location. This applies to all business endeavors in which WM has a fifty-percent or more ownership.

Management will regularly monitor operations and make recommendations to the Board of Directors on programs to continuously improve the environmental performance of the Company. Environmental goals and objectives will be established, reviewed and approved during management review. The WM Board of Directors and executive management will regularly monitor the environmental performance to ensure adherence to the principles of this policy across the Company.

Policy Owner/Contact: The policy owner is the Senior Vice President, Field Operations. Questions regarding this policy should be directed to the Policy Owner.

Variance Approvals: Policy variances must be obtained from the Policy Owner. Variances must be requested using the Variance Approval Form.

People

1. HUMAN RIGHTS POLICY

Purpose:

This policy reflects Waste Management's (WM) commitment to protect and advance human dignity and human rights in WM business practices. This policy applies to all personnel employed by or engaged to provide services to WM, including, but not limited to, WM's employees, officers, and contingent workers, as well as WM's contractors and suppliers.

Policy:

WM's relationships with its employees, contractors and suppliers and with the countries and communities in which WM operates are intended to reflect the principles, policies, and codes established and referred to in this policy. WM Code of Conduct is founded on responsible, honest and

ethical behavior, and the character of WM is defined by the personal integrity and honesty of its employees. The WM Code of Conduct is the means to implement its human rights values and commitments.

This policy is guided by the Ten Principles of the United Nations Global Compact as derived from: The Universal Declaration of Human Rights, the International Bill of Human Rights and the International Labor Organization's 1998 Declaration on Fundamental Principles and Rights at Work. WM is committed to compliance with all applicable employment, labor, and human rights laws to ensure fair and ethical business practices are followed. WM's respect of human rights is demonstrated in its employment practices, including non-discrimination, diversity and inclusion, minimum age requirements, freedom of association and respect for collective bargaining and fair compensation policies. WM further demonstrates its dedication to human rights in the commitment to providing healthy, safe, and secure workplaces, and to promoting the health and safety of the communities in which it operates.

We expect our employees, contractors and suppliers to comply with the law in each place we do business and to abide by our Business Ethics and Compliance Policy, Code of Conduct or, as applicable, our Supplier Code of Conduct. Implementation of compliance with the Code of Conduct is overseen by the Chief Compliance Officer. WM Human Rights Policy is consistent with and incorporates the principles set forth in our policies which prohibit discrimination, child labor and human trafficking, modern slavery and forced labor.

Our goal is to conduct business with those who share our commitment to these same principles. WM will continue to require commitment to human rights from its contractors and suppliers. To ensure this commitment is met, WM includes in its supplier and service provider agreements a requirement that its business partners operate under business and ethics standards consistent with WM own standards.

Investigations and Audits

WM reserves the right, where applicable, to conduct investigations and audits to verify that business is being conducted in

compliance with this policy. All WM employees and third parties through whom WM conducts business are required to fully, accurately and promptly cooperate.

Policy Compliance

WM is committed to conducting business with the highest levels of integrity, in full compliance with the spirit and integrity of the laws of each country in which we operate as well as in full compliance with our Code of Conduct. We encourage anyone who believes that this policy has been violated to report their concerns to the Chief Compliance Officer. Reports may also be made through the WM Integrity Helpline at 800-265-9381 or its website (ethics@wm.com), both of which allow anonymous reporting as permitted by applicable law. Employees who fail to report actual or suspected misconduct may be deemed in violation of this policy as permitted by applicable law. WM will not tolerate retaliation against an employee for reporting a concern in good faith or for cooperating with a compliance investigation, even when no evidence is found to substantiate the report.

Any violation of this policy may be grounds for disciplinary action, up to and including termination, subject to applicable law. Violation of applicable laws may also result in criminal prosecution of responsible individuals.

Policy Owner/Contact:

The Policy Owner is the Chief Compliance Officer. Questions regarding this policy should be directed to the Policy Owner.

Variance Approvals:

Policy variances must be obtained from the Policy Owner. Variances must be requested using the Variance Approval Form.

Attachments / Links

- Business Ethics and Compliance Policy [ID: 393]
- Code of Conduct [ID: 677]
- Policy Against Human Trafficking and Modern Slavery [ID: 1245]
- Variance Approval Form [ID: 5]

2. Public Policy Overseas

To ensure compliance with international law, Waste Management has adopted an anti-bribery and corruption policy and established a Foreign Corrupt Practices Act (FCPA) Compliance Committee. All employees involved in foreign business projects must receive FCPA training. In addition, the Waste Management Code of Conduct includes a section on doing business overseas to ensure our compliance with local laws as well as U.S. laws that govern our activities in international markets. Visit https://www.wm.com/about/company-profile/ethics/pdfs/Code_of_Ethical_Conduct.pdf.

3. ANTI-BRIBERY POLICY

Waste Management ("WM" or "Company") must not pay any bribe to any third party (public or private) for any purpose, at any time. Responsibility for maintaining this standard lies with everyone at the Company and compliance with this policy is mandatory. No employee will suffer adverse consequences for refusing to pay or refusing to be involved in any bribe, even if it results in losing business.

A. The Foreign Corrupt Practices Act ("FCPA")

The FCPA is a U.S. criminal statute that prohibits bribery of foreign officials. The law may apply to the conduct of Company anywhere in the world and has significant criminal and monetary penalties for violations, including criminal and monetary penalties for individual employees. It not only applies to WM employees' direct dealings with foreign public or government officials, but can also apply to the activities of third parties through whom anything of value could be passed on for the direct or indirect benefit of WM. Bribery involves authorizing, giving, promising to give, or offering anything of value, directly, or indirectly, with a corrupt intent to influence someone to retain or obtain business or any other improper advantage. It does not matter if a bribe is actually paid. The mere offer to pay a bribe is

illegal. A bribe can be committed directly or indirectly, through a third party, and can be anything of value, including money, gifts, entertainment, and donations or contributions.

Facilitating Payments – Under the FCPA, a facilitating payment is a payment made to a foreign official or agency to facilitate or speed up the performance of an existing duty. Although these payments may be authorized under U.S. law in certain circumstances, they can be considered bribery under other laws such as the UK Bribery Act and may be illegal in other countries. Facilitating payments are prohibited by this Policy. Any request to pay a facilitating payment must be reported to the FCPA Committee.

All Bribes Prohibited – Under the FCPA, bribery of foreign officials is prohibited. However, many laws, including certain domestic laws and laws in other countries prohibit all bribery, whether foreign officials are involved or the conduct is between private parties. In addition to this broader scope, many laws make it illegal to both give and receive a bribe. This Policy prohibits giving or attempting to give a bribe to a foreign official or individual party, as well as the receipt of a bribe.

Books and Records –The books and records of the Company must accurately reflect the transactions of the Company. Failure to record all transactions, or the falsification of records to conceal transactions, constitutes a violation of the FCPA.

B. FCPA Compliance Committee

The Company has established an FCPA Compliance Committee (the "FCPA Committee") led by the Company's Chief Compliance Officer to promulgate procedures and provide oversight and training with respect to this Policy and any diligence, audits and/or investigations related to the Company's anti-bribery compliance.

C. Compliance and Suspected Violations

Any Company employee who violates this Policy is subject to discipline, up to and including termination. Employees are encouraged to seek guidance from and must report any concerns or suspected violations of this Policy to the Policy Owner, the Chief Compliance Officer, or through the use of the Company's Compliance and Ethics Helpline. The Company will not tolerate any form of retaliation or detrimental personnel action against anyone reporting a potential violation in good faith or with reasonable grounds for suspicion or concern.

4. POLICY AGAINST HUMAN TRAFFICKING AND MODERN SLAVERY

Purpose: Waste Management (WM) is committed to a work environment that is free from human trafficking and slavery, including forced labor and unlawful child labor. WM will not tolerate human trafficking or slavery in any part of our organization. This policy reflects WM's Code of Conduct and our core values to protect and advance human dignity and human rights in our business practices. This Policy applies to all personnel employed by or engaged to provide services to WM, including, but not limited to, WM's employees, officers, temporary employees, contingent workers, casual staff, and independent contractors, as well as WM's vendors, suppliers and partners.

Every WM employee is responsible for reading, understanding and complying with this Policy.

WM managers are responsible for ensuring that employees who report to them, directly or indirectly, comply with this Policy and complete any certification or training required of them.

Policy: WM prohibits trafficking in persons and slavery. WM employees and others through whom WM conducts business must not engage in any practice that constitutes trafficking in persons or slavery and must comply by all applicable law and contract. This includes, but is not limited to, the following activities: • Engaging in any form of trafficking in persons; • Procuring commercial sex acts; • Using forced labor in the performance of any work; • Denying access by an individual to the individual's identity or immigration documents, such as passports or drivers' licenses, regardless of issuing authority; • Using misleading or fraudulent practices during the recruitment of candidates or offering of employment/contract positions regarding the key terms and conditions of employment; • Using recruiters that do not comply with local labor laws of the country in which the recruiting takes place; • Charging applicants/candidates recruitment fees.

WM and its employees will cooperate fully with the U.S. Government or other appropriate governmental authorities in audits or investigations relating to such violations.

WM will continue to address risks associated with forced labor and human trafficking in its supply chain, including the following: • Evaluating and addressing supply chain risks in coordination with industry partners to increase awareness of human trafficking and to implement EICC programs. • Implement a supplier certification process requiring suppliers to certify to the best of their knowledge that the materials they incorporate into products were generated in compliance with applicable anti- slavery and human trafficking laws. • Training on human trafficking and slavery issues for employees directly managing the direct hardware supply chain.

Investigations and Audits: WM will perform investigations and audits to verify that business is being conducted in compliance with this Policy. All WM employees and third parties through whom WM conducts business are required to fully, accurately and promptly cooperate.

Policy Compliance: Report any conduct that you believe to be a violation of this Policy, either directly to a member of the Ethics and Compliance team, to the WM Legal Department, to the Chief Compliance and Ethics Officer, or to WM's Executive Vice President, General Counsel and Secretary. Reports may also be made through the WM Integrity Helpline at 800-265-9381 or its website (ethics@wm.com), both of which allow anonymous reporting as permitted by applicable law. Employees who fail to report actual or suspected misconduct may be deemed in violation of this Policy as permitted by applicable law. WM will not tolerate retaliation against an employee for reporting a concern in good faith or for cooperating with a compliance investigation, even when no evidence is found to substantiate the report.

Any violation of this Policy may be grounds for disciplinary action, up to and including termination, subject to applicable law. Violation of applicable laws may also result in criminal prosecution of responsible individuals.

5. Safety Policy

At Waste Management, safety is a core value and a cornerstone of operational excellence. This philosophy is embedded in the way we work, the decisions we make and the actions we take.

With more than 50,000 employees and over 25,000 trucks on the road every day, we fully recognize our responsibility to protect our employees, our communities and our customers. Our goal is to attain world-class safety and, more importantly, to be among the safest companies in our industry. Our plan of

action is called Mission to Zero (M2Z), which means zero tolerance for unsafe actions, unsafe decisions, unsafe conditions, unsafe equipment and unsafe attitudes.

- The cornerstone of M2Z is training, which provides classroom and on-the-job site instruction in safety fundamentals for supervisors, drivers and helpers. Operations Rule Book, Driving Science Series videos and Electronic Observation Behavior Assessments are just a few of the tools available to our frontline managers to help them to develop our employees.
- M2Z seeks to enhance understanding, change behaviors and develop company leaders who can make a difference and train and lead others. M2Z does not seek to find fault or punish people.
- M2Z is about being hard on facts and easy on people.

Waste Management sites continuously monitor and measure safety performance. The resulting measurements reflect the reduced frequency and severity of safety incidents, improved employee and customer satisfaction. Through established safety processes and procedures, our goal of zero accidents and injuries is transformed into measurable results that have a positive impact on thousands of people.

Governance

COMPUTER RESOURCES AND DATA SECURITY POLICY

Purpose:

To communicate Management objectives for the acceptable use of company-provided resources and the use of secured data by all employees and agents ("Users") of Waste Management and its subsidiaries ("WM" or "Company").

This policy applies to all Company owned or leased equipment, data transmission equipment, data storage devices, printers, display devices, and data, and is applicable regardless of where the equipment or data reside. This policy also applies to personal devices when used for Company business. All Company authorized methods of securing computer resources (i.e. computer facility access, security access, Company account information, and passwords) are also included in this policy.

Policy:

The Company provides resources that are critical to business functions throughout WM. The use of these resources is granted to personnel for the express purpose of performing their jobs. Examples of these resources include computers, electronic mail, and Internet/Intranet access.

All employees and agents (“Users”)

- Have a duty and a personal responsibility to protect confidential information as part of their business relationship with WM;
- Must comply with appropriate computer security precautions and virus protection procedures; and
- Must handle information such as passwords, identification codes and other confidential information in a secure manner.

Accordingly, this policy provides guidance in the following areas:

- Usage
- Access to WM Computer Resources
- Company Assets

The Employee Handbook, which can be obtained from a local Human Resources representative, provides additional information regarding the usage and accessing of company assets such as email and the internet. It is updated annually and should any information differ from details herein, the Employee Handbook should be followed.

Usage

WM's voice mail, electronic mail, and computer systems network, including software programs and Internet access ("systems"), are provided for the use of its employees, contractors, vendors, and selected other persons (Authorized Users) for the performance of their WM job duties and related activities.

Access to the Company-provided electronic mail and Internet/Intranet services must be approved. Before access to the Company-provided electronic mail and Internet/Intranet services will be granted, the Authorized User is required to acknowledge receipt and understanding of this policy and sign a statement of acceptance.

Internet

The internet is a useful business tool and Authorized Users are expected to demonstrate good judgment in using this tool appropriately. Use of the Company's computer resources during work time for any purposes other than those specifically authorized is prohibited. "Working time" is the time that an individual is engaged or should be engaged in performing his/her work for the Company. Personal use of Company-provided electronic mail and Internet/Intranet services during non-working time is permitted, provided it does not negatively affect the functioning of those systems or otherwise substantially interfere with productivity.

All information posted on the Internet on behalf of WM must be approved by the appropriate corporate department and be consistent with the Company's policy for communicating information to the public.

The Company reserves the right to grant, restrict, or remove access to web sites at any time. Internet access is monitored, and actual web-site connections are recorded for legitimate management purposes. Any inappropriate use may result in loss of access privileges and/or other action as appropriate.

Social Media

Social media can include, but is not limited to, networking sites, personal Web pages, blogs, videos, podcasts, live chats, Internet discussion forums tweets, text messages and instant messages. As an Authorized User, the use of social media to post information, comment, and exchange ideas relating to WM or its business, includes the obligation to act responsibly.

WM has developed guidelines that individuals should adhere to when using social media (or other similar technology) to post information, comment or exchange ideas related to WM or its business.

- Know and follow WM's policies and rules.
- Do not disclose WM's or a third party's confidential or proprietary information.
- Do not post any information or statements that disparage customers, partners or suppliers.
- Do not speak on behalf of WM.
- Each Authorized User is personally responsible (and liable) for the content of any posts.
- Do not discredit WM's services or products.
- Be respectful to fellow associates, customers, members, suppliers or people who work on behalf of WM.
- Refrain from using social media while on work time or on equipment we provide, unless it is work related as authorized by your manager and consistent with company policies.
- Retaliation against any individual for reporting a possible deviation or cooperating in an investigation is prohibited.

Failure to adhere to these guidelines may result in disciplinary action, including termination.

E-mail

E-mail is considered by the Company to be a non-permanent form of communication and messages should be promptly deleted after use. E-mail messages stored in folders or archived should be maintained only so long as they remain in use and should thereafter be deleted. The exception to this policy is when an Authorized User receives notice from the Legal Department that emails must be preserved. Authorized Users receiving such notice will be given specific instructions regarding preserving emails that they must follow.

Recipients of messages or information inadvertently sent or misaddressed to them should not copy, retain or disclose the contents of such messages. It is the policy of the Company that such messages should be deleted with notification, if possible, to the sender of the misaddressed or misdirected message.

Voicemail, Computer Systems

The systems, the related messages, documents and information received, stored and processed by the system are and remain the property of WM. All systems access codes must be available to WM and individuals may not use access codes that are unknown to WM. Authorized Users are prohibited from the unauthorized use of the access code of other individuals and from unauthorized access or attempted access of prohibited areas of the systems, such as personnel files, accounting information, etc.

Computer software necessary for the performance of each Authorized User's duties at WM is installed on the network and is to be used in strict conformity with applicable licenses. Authorized Users are strictly forbidden from the unauthorized (i) reproduction of software programs for use either at WM or elsewhere, and (ii) the installation or

downloading of software from the Internet onto WM's network or any single CPU at WM or downloading software from the internet without the express authorization of the Director of Information Security.

Notwithstanding the unauthorized access prohibition, WM cannot guarantee that the files, messages, documents, and other information stored, created, retrieved or transmitted by an individual will remain confidential. Further, WM reserves the right to access, review, and use for any purpose any and all messages and/or information on its systems at any time without notification, on a regular or random basis, and without regard to:

- The use of passwords or access codes
- Who composed, placed or received the information, document or message

Access to WM Computer Resources

Only company-approved software may be used when connecting to the Internet through the Company's network. Account IDs and passwords for the services are strictly for the use of the Authorized User and should not be shared or made accessible to others. Under circumstances in which passwords must be provided to others to gain access to the computer, such as system maintenance or repair, a new password should be created and used after the completion of that process.

Access to Corporate computer resources will be recorded (logged). The log records will be retained according to the requirements of the business function being supported, as well as the technical and legal requirements. The Company has the right to use these logs for business and investigative purposes, including identifying individuals that are misusing WM's computer resources.

External Connections

Connections to WM's private network by unauthorized persons is prohibited. It should be recognized that under certain conditions these actions might also be in violation of state and/or federal laws.

Employees, contractors, vendors or others that may have access to the Company's networks should not take any action that would block or restrict the Company's efforts to monitor or manage these resources.

Remote Access

WM provides "remote access" to the Company's private network as a method for employees and other Authorized Users to support certain business functions. It also exposes the Company's network to additional risks of unauthorized intrusion. In remote access connections, the level and type of security applied at the remote location is one of the primary factors in determining whether the Company's information is being sufficiently protected. Remote access connections will be subject to periodic random monitoring for business reasons.

WM requires that individual accountability be maintained at all times. To ensure individual accountability when WM resources are being accessed remotely, the

identification and authentication of the person attempting access will be verified prior to the connection being made.

Appropriate WM management authorization is required to access the Company's computing resources from a remote location. This authorization is in addition to any other access authorizations that may be in existence. Access codes will not be shared. Authorization for remote access is granted specifically to one individual and should not be shared without express permission by WM management.

Wireless Access

Wireless connections to WM networks and resources are for business use by WM employees and persons working with or for WM. IT will manage and control the wireless devices to maintain wireless availability within specified parameters. IT Security will also monitor the WM wireless network to ensure only authorized access, and monitor for intrusion on a constant basis. Unauthorized users will be blocked from service.

Company Assets

Employees and other Authorized Users are responsible for maintaining reasonable control and protection of Company assets that have been issued to them or placed in their care. The use of Company time, equipment, supplies, and facilities for personal use must be reasonable and for a lawful purpose and taking Company-owned equipment off Company premises for personal use is permitted only when approved in advance by the individual's department manager.

Computers capable of live access to the Company-provided electronic mail and Internet/Intranet services should not be left unattended. Company information must be protected while being stored or transmitted over the services.

While it is our policy to respect personal privacy, employees and other Authorized Users must recognize that computers, telephones and work spaces belong to the Company and are provided for business purposes. The Company retains the right to monitor and search all Company property.

Information Technology Assets

All Authorized Users are responsible for ensuring that IT security controls (including system password protection) are followed in a manner that will preserve the security objectives of confidentiality, integrity, and protection of WM's information assets.

Office Equipment Assets

The office telephone, fax machine, credit checking services, copy machine facilities, UPS and other delivery services are for business purposes only. It is recognized that some personal telephone calls or faxes may be necessary but should be kept to a minimum and cannot negatively affect the functioning of those systems or otherwise substantially interfere with productivity. Any reported abuse of telephone use or any of the above-mentioned services may lead to disciplinary action, up to and including termination of employment.

Mobile Phone Assets

Company employees and other Authorized Users are prohibited from using any personal or Company communication device while driving or operating a Company owned/leased vehicle or mobile equipment. All Authorized Users must adhere to any local, state or federal restrictions regarding the use of communication devices while driving when those restrictions are more limiting than this policy.

Please refer to the Mobile Device Policy for additional discussion regarding use of mobile phone assets.

Mobile Computing Devices

Individuals who access or maintain a copy of WM information on mobile devices such as laptop computers, external drives, or personal digital assistants (PDA) are responsible for safeguarding these devices. Individuals must take reasonable measures to protect these devices, and the information on these devices, from loss or theft. Corporate Security must be notified immediately in the event of loss or theft.

Please refer to the Information Classification Policy and Protected Information Protection Policy for additional discussion of confidential information.

Unauthorized disclosure is a violation of Company policy and, in some cases, may also violate the law and could result in fines, penalties, or legal action against WM and/or individuals involved. Additionally, any violation of these policies by an employee of the Company or by any person other than an employee of the Company may result in disciplinary action, up to and including termination of employment or termination of contract or service agreement.

Approval Requirements:

N/A

Policy Owner/Contact:

The policy owner is the Senior Vice President of Corporate Affairs and Chief People Officer. Questions regarding this policy should be directed to the Vice President, Corporate Human Resources & Process Information Management, the Director of Information Security or the Policy Owner.

Variance Approvals:

Policy variances must be obtained from the Policy Owner. Variances must be requested using the Variance Approval Form.