PHYSICAL AND CYBERSECURITY POLICY STATEMENT

Waste Connections, Inc., together with its subsidiaries, operating divisions and affiliates (collectively, the "Company" or "Waste Connections"), maintains a robust internal Physical and Cybersecurity Policy or "PCSP", establishing the overriding principles and policies governing the Company's information systems standards and practices.

These principles and policies, as more comprehensively outlined in the PCSP, define the Company's objectives for managing information systems operations and represent the plans and protocols for achieving and maintaining internal control over those systems, as well as compliance with the requirements imposed on the Company related thereto.

Information security is achieved and maintained through the implementation of a set of controls that involve policies, processes, procedures, organizational structures, and software and hardware functions. These controls must be established, implemented, monitored, reviewed, and improved as necessary to meet the specific security and business objectives of the Company.

Elements of the PCSP include, but are not limited to:

Cybersecurity Governance:

Cybersecurity risk oversight is provided by the Board of Directors. Cybersecurity governance is the responsibility of Waste Connections' executive management team to advance the Company's strategies and objectives. The Information Technology team, including the Chief Information Officer (CIO), manages Waste Connection's Information Technology ("IT") resources.

Enforcement:

All personnel accessing the Company's data or IT resources are required to comply with all applicable federal and state laws, rules and regulations, as well as all Company policies and procedures. Any Company personnel who violate this PCSP will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

Policy Requirements:

Each department will protect the Company's resources by adopting and implementing, at a minimum, the security standards and procedures stated within the PCSP and meeting those minimum standards.

Information Systems Security:

The Company's established, documented, and implemented Information Technology Security Program is designed to improving the effectiveness of IT operations and the ability to satisfy regulatory requirements. This program has been implemented to ensure the confidentiality, availability and integrity of Waste Connections' information while maintaining appropriate levels of accessibility.

Risk Assessment:

Annually, or more frequently as determined by the Company's CIO, the Company conducts a risk assessment to identify and assess risk and to reduce threats of impairment to the confidentiality, integrity, and availability of IT resources.

Controls Mechanisms:

Internal controls are designed to provide a reasonable assurance that goals and objectives for Waste Connections are met. Preventive controls are designed to discourage or pre-empt errors or irregularities from occurring. Detective controls are designed to search for and identify errors after they have occurred. Corrective controls are designed to prevent the recurrence of errors.

Information Classification:

Information classification is required to determine the relative sensitivity and importance of information technology resources, which provide the basis for protection efforts and access control.

Scope:

Waste Connections' PCSP applies to the entire Waste Connections organization, including all personnel, consultants and guests who have access to Waste Connections' IT resources. Every employee shares the responsibility for securing information and resources within their respective departments.