RentReporters/CCG
Data Misuse Policy

This policy outlines the processes and procedures to be followed by all employees and stakeholders of the company to prevent, detect, and address the misuse of data. Data misuse refers to any unauthorized, unethical, or inappropriate access, disclosure, alteration, or use of company data, including sensitive or confidential information. This policy aims to establish clear guidelines and expectations regarding data handling and promote a culture of data ethics, security, and compliance within the organization.

Data Access and Authorization. Access to company data shall be granted only to authorized individuals based on their job responsibilities and the principle of least privilege. Each employee shall be assigned appropriate access rights and credentials to ensure that they can access and use data only as necessary to perform their duties. Regular access reviews and audits will be conducted to ensure that access privileges are up to date and aligned with job requirements.

Data Classification and Handling. All company data shall be classified based on its sensitivity and importance, using a defined data classification framework. Employees must adhere to the data classification guidelines and handle data according to the assigned classification level, ensuring proper protection and security measures are applied. Confidential or sensitive data should be encrypted, anonymized, pseudonymized, or de-identified, as appropriate, to minimize risks in case of unauthorized access.

Data Use and Purpose Limitation. Employees shall only use company data for legitimate business purposes and within the scope of their job responsibilities. Data shall not be used for personal gain, unauthorized research, marketing purposes, or any activities that violate applicable laws, regulations, or contractual agreements. Prior approval must be obtained from relevant stakeholders or data owners for any data usage beyond its intended purpose.

Data Sharing and Disclosure. Employees shall exercise caution when sharing company data with third parties, ensuring that appropriate data sharing agreements or contracts are in place. Data shall not be disclosed to unauthorized individuals, unless required by law or with explicit consent from data subjects. When sharing data, proper anonymization, aggregation, or masking techniques should be employed to protect individual privacy and confidentiality.

Reporting Data Misuse. Any employee who suspects or becomes aware of data misuse must immediately report it to their supervisor, the IT department, or a designated reporting channel. Reports should include detailed information about the incident, individuals involved, nature of the misuse, and any supporting evidence. Whistleblower protections shall be in place to encourage employees to report data misuse without fear of retaliation.

Investigation and Corrective Actions. Upon receiving a report of data misuse, the company will conduct a thorough investigation to determine the validity of the claim and take appropriate action. The investigation may involve IT forensic analysis, interviews, documentation review, or engagement of external experts, as necessary. If data misuse is confirmed, disciplinary actions

will be taken in accordance with company policies and applicable laws, which may include warnings, suspension, termination, legal action, or other remedies.

Policy Violations. Any employee found to violate this policy by misusing company data, breaching data handling procedures, or engaging in unauthorized activities may be subject to disciplinary action, up to and including termination.