CARROLS CORPORATION
Syracuse, New York

PERSONNEL POLICY AND PROCEDURE

Subject: **POLICY GOVERNING COLLECTION, USAGE AND RETENTION OF BIOMETRIC IDENTIFIERS AND/OR INFORMATION**

Instruction No: 111-**IL**

Effective Date: November 11, 2019

Affects: All Employees in IL

Approved By: Jerry DiGenova
Title: Vice President, Human Resources

I. PURPOSE AND SCOPE

When authorized to do so, Carrols Corporation (together with its direct and indirect parents, subsidiaries, and affiliates, the "Company") from time to time, collects, uses and/or stores employee information that may qualify as a biometric identifier or biometric information – namely, information collected from employees' fingerprints or any other biometric identified or biometric information – in connection with the administration of its timekeeping system and the maintenance of time and attendance records associated therewith. Accordingly, the Company has established this Policy outlining the Company's retention schedule and guidelines for destroying such information.

The Company, in its sole discretion, reserves the right to amend this Policy at any time.

Please note that under no circumstances will the Company sell, lease, trade, or otherwise profit from employees' potential biometric identifiers or biometric information. Furthermore, absent each employee's consent or unless required by law (such as federal laws and regulations, a valid warrant or subpoena), the Company will not disclose or disseminate such information to third parties.

This Policy applies to all employees of the Company in the State of Illinois and consenting to the policy is a condition of employment for all employees in Illinois.

II. RETENTION SCHEDULE

The Company (when authorized) retains information collected from employees that may qualify as biometric identifiers or biometric information for the entirety of those employees' employment and until the initial purpose for collecting or obtaining such information has been satisfied or within three (3) years of each employee's separation from employment, whichever occurs first. During that time, the Company exercises reasonable care in protecting such information and does so in a manner that is the same or more protective than the manner in which it protects other confidential and sensitive information.

III. GUIDELINES FOR DESTRUCTION

Unless further retention is required by law (e.g., federal laws and regulations, a valid warrant, subpoena, or litigation hold notice), the Company will permanently delete and/or destroy all potential employee

biometric information or identifiers from all Company systems, files and backups, including, but not limited to, its cloud storage systems, when the initial purpose for collecting or obtaining such information has been satisfied or within three (3) years of each employee's separation from employment, whichever occurs first. In doing so, the Company will continue to take reasonable measures to protect this information (to the same extent it protects other confidential and sensitive information) and ensure it is not inadvertently disclosed or disseminated to third parties.

To the extent any employee has authorized disclosure of possible biometric identifiers or information to any contractor, the Company will instruct that contractor to permanently delete such information from all of its systems, files and/or back-ups when the initial purpose for collecting or obtaining such information has been satisfied or within three (3) years of each employee's separation from employment, whichever occurs first, unless further retention is required by law. The Company shall require all such contractors to which/whom disclosure has been authorized to provide a sworn verification attesting that it has permanently deleted and/or destroyed each such employee's potential biometric identifiers and biometric information in accordance with this policy (except, as set forth above, if such third parties are required to retain such information by law). During that time, such contractors shall exercise reasonable care in protecting such information and do so in manner that is the same or more protective than the manner in which it protects other confidential and sensitive information.