BANKIER BIOMETRIC INFORMATION AND SECURITY POLICY

I. Purpose

This Biometric Information and Security Policy ("Policy") defines the policy and procedures of Bankier Companies, Inc. ("Bankier") for collection, use, safeguarding, storage, retention, and destruction of biometric data collected by Bankier and/or its vendors.

Bankier uses biometric identification systems for employee timekeeping with regard to payroll. Bankier and/or its vendor(s) collects, stores, and uses employee biometric data for the purpose of granting employees access to Bankier's timekeeping systems and to document employees '(i) clock in/out time(s); (ii) clock in/out location(s); and (iii) attempts/failures/errors in biometric data scans.

II. Policy

Bankier's policy is to protect and store biometric data in accordance with applicable standards and laws, including, but not limited to the Illinois Biometric Information Privacy Act. An individual's biometric data will not be collected or otherwise obtained by Bankier without prior written consent of the individual. Bankier will inform the employee of the reason his or her biometric information is being collected and the length of time the data will be stored.

III. Definition

Biometric data means personal information stored by Bankier and/or its vendor(s) about an individual's physical characteristics that can be used to identify that person. Biometric data can include fingerprints, voiceprints, a retina scan, or face geometry, or other data.

IV. Procedure

Bankier and/or its vendor(s) collects, stores, and uses biometric data for the purposes of giving employees access to Bankier's timekeeping systems and for maintaining accurate records of employee time. Prior to collecting biometric data, Bankier will obtain the consent of the employee. A sample consent form is included with this policy statement. Bankier will not sell, lease, trade, or otherwise profit from an individual's biometric data. Bankier will not disclose biometric data unless (a) consent is obtained, (b) disclosure is required by law, or (c) disclosure is required by a subpoena.

Bankier will store, transmit, and protect biometric data, including but not necessarily limited to your fingerprint or other biometric data, using a reasonable standard of care and in a manner that is the same as or exceeds the standards followed in maintaining other confidential and sensitive information. Bankier will retain the employee's biometric data throughout the term of the employee's employment by Bankier, and Bankier will permanently destroy an employee's biometric data from Bankier's systems, or the systems of Bankier's vendor(s), within a reasonable

time following the employee's termination from Bankier. In the event Bankier begins collecting biometric data for any additional purpose, Bankier will update this procedure. A copy of this policy is publicly available at http://www.bankier.com.