BIOMETRIC INFORMATION PRIVACY POLICY

In order to efficiently and securely track employees' time records, Staffing Network/Quality Placement Authority ("the Company") may use a biometric timekeeping system where the use of biometric equipment for recording worked hours is a requirement of employment with the client company. The Company may use third-party timeclock vendors or licensors, including, but not limited to, PeopleNet and Bullhorn, to supply it with biometric timekeeping systems. The Company may also rely on biometric timekeeping systems provided by its clients' timeclock vendors.

In order to comply with various laws concerning biometric data (including the Illinois Biometric Information Privacy Act), the Company has instituted the following biometric information privacy policy for its Illinois employees:

Biometric Data Defined

As used in this policy, biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, *et seq.* "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

Purpose for Collection of Biometric Data

The Company may utilize biometric technology for the purpose of identifying employees and recording time entries using systems provided by its third-party timeclock vendors or licensor of the Company's time and attendance software, including, but not limited to, PeopleNet and Bullhorn, or its clients' timeclock vendors. As part of this system, the Company/Vendor/Licensor collects and/or stores employees' biometric identifiers and/or biometric information.

Disclosure

The Company will not sell, lease, trade, or otherwise profit from an employee's biometric identifier or biometric information. Nor will it authorize its timekeeping vendors, licensors, or clients to engage in any such activity. The Company will not disclose or disseminate any biometric data to anyone other than its vendors, licensors, and client to whom the employee is assigned without/unless:

a. First obtaining written employee consent to such disclosure or dissemination;

b. The disclosed data completes a financial transaction requested or authorized by the employee;

c. Disclosure is required by state or federal law or municipal ordinance; or

d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Storage

Once captured, an employee's Biometric Information is converted into an encrypted data string (i.e., biometric template) and stored securely by the Company's timeclock vendors, licensor of the Company's time and attendance software, or the Company's clients' timeclock vendors on the timeclock vendors' or licensors' electronic servers.

The Company shall require its timeclock vendors, licensors, and the Company's clients to use a reasonable standard of care to store, transmit, and protect from disclosure any biometric data collected.

Retention Schedule

The Company shall retain employee biometric data only until, and shall request that its vendors, clients, and licensors permanently destroy such data when, the **first** of the following occurs:

- The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with the Company, or the employee moves to a role within the Company for which the biometric data is not used; or

- Within 3 years of the employee's last interaction with the Company;

Or upon the receipt of a written request to discontinue the use of such information from the employee.