Finger/Hand Scan and Touch/Facial Recognition Policy and Release

FreshEdge, LLC, and/or its operating companies (collectively, "FreshEdge Companies") may use finger/hand scanning and/or touch/facial recognition technology for identification in their respective timekeeping systems ("System"). The FreshEdge Companies may also issue smartphones and laptop computers that have touch or facial recognition security features.

Consent to Collection – Employees are required to use finger scanners included in our timekeeping systems as a condition of employment and to consent the collection finger scan data by these systems. Use of facial recognition or touch security features on mobile devices and laptops is optional. Employees who elect not to use these features may instead log in using a secure passcode. Employees who activate touch or facial recognition features on company-issued mobile devices or laptops consent to the use of any fingerprint or facial data captured by those devices. Employees also consent as a condition of employment to sharing of finger scans, facial recognition or touch security data with device manufacturers and vendors contracted by the FreshEdge Companies for purposes of deployment, set up, operation, maintenance, and administration of the System, laptops, and mobile devices.

Privacy of Data – The FreshEdge Companies store all data generated by finger scanners or touch or facial recognition features in mobile devices or laptops in accordance with applicable standards and laws. The FreshEdge Companies will not sell, lease, trade, or otherwise profit from any data generated by a finger scanner or touch or facial recognition features of mobile devices or laptops. Except as specified above, such data will not be disclosed, redisclosed or disseminated outside of the FreshEdge Companies unless the employee (or the employee's legally authorized representative) consents, the disclosure or redisclosure is necessary to complete a financial transaction requested or authorized by the employee or their legal representative, the disclosure is required by law, or the disclosure is required by a valid warrant or subpoena. Such data will be stored, transmitted, and protected using a reasonable standard of care applicable to the FreshEdge Companies' industry, in a manner that is the same as or that exceeds the standards of care used to protect other confidential information held by the FreshEdge Companies. This includes, among other things, restricting access to data to authorized employees, vendors, and contractors of the FreshEdge Companies who have a business need to access the information, and using reasonable technological means to prevent unauthorized access to the information.

Destruction of Data – The FreshEdge Companies will permanently delete or destroy any data in its possession generated from finger scanners or touch or facial recognition security features when the initial purpose for obtaining or collecting the data has been fulfilled. Facial recognition or touch security information used to log into the FreshEdge Companies' laptops or mobile devices will be permanently deleted from the device issued to you if the device is returned to the FreshEdge Companies, unless it is expected that the device will be re-issued to you, *e.g.,* after software updates or repair. The FreshEdge Companies may retain data beyond these specified periods if it determines that deletion must be postponed due to legal requirements, including but not limited the obligation to preserve evidence related to actual or anticipated litigation. Finger scan data and information from touch or facial recognition features in mobile devices and laptops will not be retained for more than three years after an employee's last interaction with the FreshEdge Companies, unless otherwise required by law.

Distribution and Updates – A copy of this policy will be made publicly available on websites of FreshEdge Companies. FreshEdge, LLC, reserves the right to amend this policy at any time.

~~~~
~~~~