HARBOR CAPITAL ADVISORS, INC. BIOMETRIC DATA POLICY

Harbor Capital Advisors, Inc. (the "Company") is committed to all employees having a secure and efficient means of accessing Company-owned laptop computers and other electronic devices. To help accomplish this purpose, the Company offers employees the option of using facial scan technology to access Company owned electronic devices, as described in this Biometric Data Policy.

Rather than entering a password or passcode, an employee has the option to "log" into the Company-owned laptop computers and other electronic devices using facial scan technology. This technology does not actually capture, collect or store a facial scan. Instead, the system measures certain biometric aspects of an employee's face. Those facial scan biometric data points are immediately converted through a proprietary software program to a unique mathematical representation of that data, which is encrypted and saved in a template. No optical image of a facial scan is kept. Each time an employee accesses a Company-owned device, a new facial scan will be provided and the template from that scan will be compared with the template assigned to the employee to verify the identity of the employee. The Company does not have access to any of the facial scan data. The facial scan biometric data points, or templates, are referred herein as Biometric Data.

If an employee chooses to utilize facial scan technology, that employee will be required to consent as a condition of employment to the Company's capture, collection and storage of Biometric Data from the facial scan technology for purposes of granting access to Company owned laptops and any other electronic devices for which facial scan technology is utilized. If an employee does not wish to consent or would prefer not to use facial scan technology, the Company provides other means of accessing Company owned laptops and other electronic devices. Prior to giving consent, employees should read this Biometric Data Policy, which will be presented to employees upon employment and/or when they are issued a Company owned electronic device that allows the use of facial scan technology, and which is also available at any time through the Company's SharePoint site and Harbor Capital | Policies & Procedures.

The Company understands that in today's world, people may be concerned about the security of their personal information. With this in mind, the Company will store, transmit, and protect from disclosure, all Biometric Data obtained through the facial scan technology using the reasonable standard of care within the industry and in a manner that is the same or more protective than the manner in which the Company stores, transmits and protects any other confidential information.

During an employee's employment, the Biometric Data from the facial scan is not accessible by any Company representative. Due to the technology used, the Biometric Data, or template, is virtually impossible to restore to an image of the original scan of the face. Furthermore, the Company will not sell, lease, trade, or otherwise profit from an employee's Biometric Data. The Company will not disclose or otherwise disseminate an employee's Biometric Data without an employee's consent unless required by any state or federal law, municipal ordinance, valid warrant, or valid subpoena.

Any employee Biometric Data collected will be retained by the Company for the duration of the time period in which the employee gains access to Company owned electronic devices, but in no

event longer than one year after the employee's last interaction with the system, unless required by law to be maintained for a longer period, provided that the current systems are maintained. The Company will permanently destroy an employee's Biometric Data upon expiration of the aforesaid time period.

This Biometric Data Policy is intended to comply with all federal, state, and local laws, and will be interpreted and applied in order to comply with all applicable laws, including but not limited to the Illinois Biometric Information Privacy Act.

If any provision of this Biometric Data Policy or any part thereof contravenes any law, or if the operation of any provision hereof is determined by law or otherwise to be unenforceable, then such offending provision or part thereof shall be severed and the remaining provisions given full force and effect.

Any dispute, claim, or controversy arising out of or relating to this Biometric Data Policy and/or the Company's handling of Biometric Data (collectively, a claim "Claim") shall be resolved by binding arbitration instead of the courts. By executing the Informed Written Consent that follows (the "Written Consent") the employee agrees to resolve any Claim through binding arbitration, which will be administered by JAMS ADR in accordance with its rules and procedures then in effect. The Company and employee expressly waive any right – with respect to any Claim – to submit, initiate or participate in a representative capacity, or as a plaintiff, claimant or member in a class action, or other representative or joint action. A Claim may only be brought in arbitration solely in the party's individual capacity. Arbitration is the exclusive form for the resolution of any Claim, and both the Company and employees mutually waive their respective right to a trial before a judge or jury in federal or state court.

If you have any questions about this Biometric Data Policy, including how the facial scan technology works, how the facial scan technology is used, or how the facial scan technology interfaces with a Company owned electronic device, please contact the IT Service Desk.