GCM Grosvenor's Biometric Information Security Policy and Consent

I. Purpose

GCM Grosvenor L.P. ("GCM") utilizes Windows Hello for the purpose of providing employees with seamless and secure access to GCM-issued computers. As part of the Windows Hello deployment, all employees are required to set a PIN code for authentication when logging in to their GCM-issued computers, as an alternative to using their full GCM password. Additionally, on a voluntary basis, employees may elect to use biometric information (as defined below) for authentication purposes to further enhance the login experience. GCM has established this Biometric Information Security Policy and Consent ("Policy") to ensure such data is reasonably safeguarded and not retained for longer than is necessary. This Policy is intended to comply with all potentially applicable laws including, but not limited to, the Illinois Biometric Information Privacy Act ("BIPA").

II. Definition of Biometric Data

For purposes of this policy, the following definitions shall apply:

- **"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.

- **"Biometric Data"** refers collectively to all Biometric Identifiers and Biometric Information.

III. Collection of Biometric Data

GCM's Windows Hello authentication process allows employees to use one of two types of biometric identifiers to access GCM secure computer network depending on the model of the device used: (1) facial scan; or (2) fingerprint scan. The facial scan uses a digital image of the employee's face to create a facial signature for GCM employees who elect to use this feature. The facial signature is created by mapping the facial features such as the precise location of an employee's eyes, nose, mouth, or other facial differences. Once the facial signature is created, it is encrypted and securely stored locally on the device, utilizing the device's Trusted Platform Module (TPM) or equivalent secure hardware, and is not transmitted to GCM server databases or any other backup systems. The encrypted facial signature cannot be reverse engineered to produce a picture of the employee.

The fingerprint scan operates by creating a numerical code that is generated from the employee's scan of his or her fingerprint. Once the numerical code is created, it is encrypted and stored locally on the device, utilizing the device's Trusted Platform Module (TPM) or equivalent secure hardware, and is not transmitted to GCM server databases or any other backup systems. The encrypted numerical code cannot be reverse engineered to produce a copy of the employee's fingerprint.

The use of a facial scan or fingerprint scan is voluntary. All employees will also be issued a PIN code to access GCM's computer network. If employees do not opt-in to the use of Biometric Data, they can access GCM's computer network solely using their PIN code. Additionally, should an employee's biometric authentication fail, the employee may access GCM's computer network using the PIN code.

IV. Use of Biometric Data

Biometric Data is stored locally on the user-employee's computer and used only to authenticate the employee to provide access to the employee's GCM-issued computer.

V. Access to Biometric Data

Because the Biometric Data referenced herein is stored locally on employee computers, neither GCM nor its agents are able to access any Biometric Data. To the extent GCM requires access to Biometric Data, it will inform employees of the reason such access required and obtain written consent from employees before accessing Biometric Data.

VI. Disclosure of Biometric Data

GCM will not disclose, redisclose, or otherwise disseminate an employee's Biometric Data unless the employee consents to such disclosure or redisclosure.

VII. Retention and Destruction of Biometric Data

As set forth in Section III, above, Biometric Data is stored locally on the employee's computer and is not transferred to any GCM systems or servers. In general, and except as otherwise required by law, legal process, or relevant GCM policies, GCM will destroy an employee's Biometric Data as soon as practicable following the termination of an employee's employment with GCM. Unless otherwise required by law or applicable legal process, GCM will permanently destroy and delete all Biometric Data from its systems no later than three years after the termination of an employee's employment with GCM.

VIII. Safeguarding of Biometric Data

Consistent with GCM's Information Systems and Security Policy, which is incorporated herein by reference, GCM will store and safeguard Biometric Data using a reasonable standard of care in GCM's industry, and in a manner that is the same as or exceeds the standards used to protect other confidential and sensitive information held by GCM. These safeguards include but are not limited to:

- Limiting access to Biometric Data to the employee to whom the Biometric Data belongs;
- Using only the minimum necessary Biometric Data for a particular permissible purpose;
- Encrypting Biometric Data;
- Storing Biometric Data securely and locally on the employee's computer;
- Using facial signatures that cannot be reverse engineered to produce a picture; and
- Using numerical codes that cannot be reverse engineered to produce a fingerprint.

IX. Amendment, Enforcement and Violations

A copy of this Policy is available by contacting your Human Resources Manager. A copy of this policy is also available to the public at: https://www.gcmgrosvenor.com/

GCM reserves the right to amend this Policy at any time for any reason. Employees who violate this Policy may be subject to discipline up to and including termination of employment.