# BIOMETRIC INFORMATION PRIVACY ACT POLICY

The purpose of this policy is to define the procedures for the collection, use, disclosure, storage, retention, and destruction of biometric information collected by the Jewish United Fund / Jewish Federation / JFMC Facilities Corporation (hereafter referred to as "JUF").

To help ensure the security of its facilities, JUF implemented and maintains a security system that collects biometric information for each of its employees or those of its Affiliated Agencies or any other visitor entered into the security system (e.g., board member, contractor, volunteer). For some individuals, JUF may store biometric information for the purpose of entering time and attendance information into the Human Resources / Payroll system. This information, (which may / may not be used in conjunction with a four-digit PIN number), authorizes and restricts an employee's secure access and entry to the JUF facilities or to securely capture time and attendance information.

Biometric information means personal information about an individual's physical characteristics that may be used to identify that person. Biometric information may be based on biometric identifiers such as retina or iris scan, fingerprints, voiceprints, facial shape, or scan of hand or face geometry.

JUF's policy is to protect biometric information in accordance with applicable standards and law including, but not limited to, The Illinois Biometric Information Privacy Act (740 ILCS 14), which regulates the collection, use, disclosure, storage, retention, and destruction of biometric identifiers and information, as defined by the Act. This Biometric Information Privacy Act Policy has been implemented as required under the Act for entities that may possess biometric identifiers or information.

JUF reserves the right to amend this Biometric Information Privacy Act Policy at any time.

**Sale / Disclosure**

JUF affirms that it will not sell, lease, trade or otherwise profit from any biometric identifier or information in its possession. JUF will not disclose or disseminate any biometric identifier or information, unless: 1) it first contains consent by the subject; 2) the disclosure completes a financial transaction authorized by the subject; 3) the disclosure is required by state or federal law; or 4) the disclosure is required pursuant to a valid warrant or subpoena.

**Storage**

JUF shall store, transmit, and protect from disclosure all biometric identifiers and information in its possession using a reasonable standard of care, and in a manner that is the same as or more protective than that in which it stores, transmits, and protects other confidential and sensitive information.

**Retention / Destruction**

JUF affirms that the biometric identifiers or information obtained will be destroyed when the initial purpose for collecting such identifier or information has been satisfied or no more than three years from the individual's last interaction with JUF, whichever occurs first, in accordance with JUF's Document and Electronic File Retention Policy.

October, 2017