The Municipal Employees' Annuity and Benefit Fund of Chicago

Policy on the Use and Protection of Member Data

The Municipal Employees' Annuity and Benefit Fund of Chicago ("MEABF") developed this Policy on the Use and Protection of Member Data to set forth its obligations with respect to a Member's personal information ("Member Data") created or received by the MEABF. The MEABF is committed to protecting the confidentiality of Member Data, including through compliance with all applicable state and federal laws.

Pursuant to the Retirement Systems Reciprocal Act, 40 ILCS 5/20-101, *et seq*., the MEABF will receive Member Data from other participating systems (collectively referred to as "Systems"). In the event the MEABF becomes aware of or suspects any unauthorized use, cybersecurity breach, or theft (collectively "Breaches") involving Member Data received from the Systems, the MEABF shall notify such other Systems within one (1) business day. For the purposes of this Policy, "Breach" is defined as access of Member Data by an unauthorized entity or individual. Such notice shall include, to the extent possible, a brief description of the Breach, the types of information involved, and the steps the MEABF is taking to investigate the Breach, mitigate the harm, and prevent any further Breach. The MEABF may also take any reasonable actions which the Systems affected may reasonably request in writing.

In the event of a Breach of Member Data, the MEABF will endeavor to notify the Member whose information was affected, unless otherwise requested in writing by an appropriate law enforcement agency. This notice shall include the approximate date the Breach occurred, the nature of the Breach, and what steps the MEABF has taken or plans to take relating to the Breach. The MEABF will also provide the Member with toll-free contact information and relevant websites for consumer reporting agencies and the Federal Trade Commission in order to provide the Member with access to resources for fraud alerts and security freezes.

It shall be MEABF's policy to never publicly display a Member's social security number or include social security numbers on any payment checks or other MEABF materials. Further it shall be MEABF's policy not to include such Member Data on materials sent through the regular mail unless allowed or required by law, pursuant to court orders, or as necessary to administer the MEABF. In no event will the MEABF knowingly include such Member Data in a mailing that is not enclosed in an envelope or allow such Member Data to be visible without opening an envelope.

In the event the MEABF possesses Member Data to that is no longer needed by the MEABF and which need not be retained pursuant to any state or federal laws, the MEABF shall dispose of such Member Data in a manner calculated to ensure the continued security and confidentiality of the Member Data. In the event the MEABF discards, sells, donates or otherwise transfers possession of any computers, computer hard drives, or other electronic storage device, the MEABF shall first ensure that all Member Data is deleted, overwritten, or otherwise removed from the device.

When complying with a request pursuant to the Freedom of Information Act ("FOIA"), it shall be the MEABF's policy to redact any social security numbers, phone numbers, home addresses, and all other "personal information", as that term is defined by FOIA, before allowing public inspection or copying of any records. For the purposes of responding to a FOIA request, the MEABF will not treat Member Data received from another System as a "record" subject to FOIA as such Member Data will be considered a record of the originating System. If it is necessary for the MEABF to disclose Member Data to any vendor or contract, the MEABF will first provide such contractor or vendor with this Policy and shall require the vendor or contract to comply with this Policy and any applicable laws related to the protection of Member Data.