**Policy for Ensuring the Security of Not Public Data**
**Minnesota Campaign Finance and Public Disclosure Board**

## Legal requirement

As an agency whose primary purpose is to disclose the information it collects, the Campaign Finance and Public Disclosure Board has very little not public data. The adoption of this policy by the Board satisfies the requirement in Minnesota Statutes section 13.05, subdivision 5, to establish procedures ensuring appropriate access to that limited amount of not public data. By incorporating employee access to not public data in the Board's data inventory required by Minnesota Statutes section 13.025, subdivision 1; by training employees about the laws governing access to not public data, and by adding employee data access provisions as appropriate to individual employee position descriptions, the Board's policy limits access to not public data to employees whose work assignment reasonably requires access to that data.

Please direct all questions regarding this policy to the Board's data practices compliance official:

Andrew Olson
190 Centennial Office Building
658 Cedar St.
St. Paul, MN 55155
(651) 539-1190
Fax: (651) 539-1196
andrew.d.olson@state.mn.us

## Procedures implementing this policy

### Data inventory

As required by Minnesota Statutes section 13.025, subdivision 1, the Board has prepared a data inventory that identifies and describes all not public data on individuals maintained by the Board.

The data inventory describes the employees who have access to not public data on individuals. In the event of a temporary duty as assigned by a manager or supervisor, an employee may access certain not public data for as long as the work is assigned to the employee. The employees referred to in the data inventory include the members of the Board, the Board's senior management team, the Board's responsible authority, the data practices compliance official, and the Board's legal counsel. Any access to not public data will be strictly limited to the data necessary to complete the work assignment.

### Data access training

All employees receive training regarding the laws applicable to access to not public data. Board members also receive training about data privacy laws applicable to the Board.

### Employee position descriptions

Position descriptions may contain provisions identifying any not public data accessible to the employee when a work assignment reasonably requires access.

## Data sharing with authorized entities or individuals

State or federal law may authorize the sharing of not public data in specific circumstances. For example, Minnesota Statutes section 10A.022, subdivision 5 (a), authorizes Board staff to share confidential information concerning a complaint or an investigation as needed to carry out the investigation or take action in the matter. Not public data may be shared with another entity if a federal or state law allows or mandates it. Individuals will have notice of any sharing in applicable Tennessen warnings or the Board will obtain the individual's informed consent. Any sharing of not public data will be strictly limited to the data necessary or required to comply with the applicable law.

## Ensuring that not public data is not accessed without a work assignment

Due to the small size of the Board's staff, all employees have work assignments that require them to have access to not public data either directly or as a backup for a co-worker. The Board will ensure that not public data is secure from unauthorized access by employees and others by taking the following actions:

- Training employees about the laws governing access to not public data;
- Assigning appropriate security roles, limiting access to appropriate shared network drives, and implementing password protections for not public electronic data;
- Password protecting employee computers and locking computers before leaving workstations;
- Securing not public data within locked work spaces and in locked file cabinets; and
- Shredding not public documents before disposing of them.

## Penalties for unlawfully accessing not public data

Minnesota Statutes section 10A.022, subdivision 5 (a), specifies that a civil penalty may be imposed by the Board on an individual who discloses information related to an investigation in violation of that section. There also are penalties for unlawful access to not public data in Minnesota Statutes section 13.09 that include dismissal and referral to the appropriate prosecutorial authority for possible criminal penalties.