

**POLICY – DATA PRACTICES**

Section/Number: 4-1-1	Total Pages: 2
Dept. Responsible: Office of Regional Administrator	Effective Date: 9/11/98
Special Note: Supersedes all previous policies covering data	Last Revision Date: 5/13/15
	Last Review Date: 5/13/15
	Revision No. 2

**I. Policy**

The Metropolitan Council will collect, create, receive, maintain and disseminate government data in accordance with state law, including the Minnesota Government Data Practices Act, Minnesota Statutes chapter 13, and applicable federal law.

**II. Purpose of policy**

To provide guidance to the Metropolitan Council so that while protection is given to individual privacy, neither necessary openness in government nor the orderly and efficient operation of government is curtailed.

To ensure that the Metropolitan Council responds appropriately and promptly to requests for government data.

To ensure that the Metropolitan Council protects data from unauthorized access and use, and that the Metropolitan Council responds to data breaches in accordance with the Minnesota Government Data Practices Act.

**III. Background and reasons for policy**

**A. Reasons for policy**

The Metropolitan Council would like to facilitate its response to requests for data, to clarify the classifications of data, and to adopt procedures for securing data, responding to data breaches, responding to data requests, and disseminating data that are consistent organization-wide.

**B. Responding to data requests**

Government data are presumed to be public and are accessible by the public for both inspection and copying unless federal law, a state statute, or a temporary classification provides that certain data are not public.

The Metropolitan Council regularly receives requests from the public and from its employees for access to data maintained by the Metropolitan Council.

**C. Sharing data with authorized entities or individuals.**

State or federal law may authorize the sharing of *not public data* as defined by Minnesota Statutes in specific circumstances. *Not public data* may be shared with another entity if a federal or state law allows or requires it. In cases of sharing data, the Metropolitan Council will provide individuals with notice and secure informed consent as required by federal or state laws. The Metropolitan Council will limit any sharing of *not public data* to the data necessary to comply with the law.



**D. Ensuring appropriate access to data and protecting data.**

The Metropolitan Council will limit collection and storage of all data on individuals and the use and dissemination of private and confidential data on individuals to what is necessary for the administration and management of the Metropolitan Council’s programs or programs specifically authorized by the legislature or mandated by the federal government. The Metropolitan Council will ensure that *not public data* are only accessible to staff whose work assignments reasonably require access.

**E. Responding to data breaches.**

The Metropolitan Council will act promptly to address and contain a data breach. This includes providing notification and penalizing employee/s if required by Minnesota Statutes section 13.055.

**IV. Implementation/Accountability**

The Metropolitan Council designates the Regional Administrator as the Responsible Authority. (Metropolitan Council Resolution No. 95-20 (April 13, 1995)).

- A. The Office of Regional Administrator, in consultation from the General Counsel, is responsible for implementing and enforcing the policy.
- B. The Responsible Authority designates those employees within the organization who are responsible for receiving and responding to data requests.
- C. Managers, supervisors, and Human Resources personnel are responsible for familiarizing themselves with the policy and procedures and for referring data requests to either the Responsible Authority or the Responsible Authority’s designee.
- D. Managers and supervisors must ensure that employees under their supervision have access only to *not public data* that they need to perform their work assignments. At least annually, managers and supervisors must provide updated information to the Responsible Authority detailing *not public data* maintained by the unit and which employee positions have access to *not public data*.
- E. All Metropolitan Council employees are responsible for following federal laws, state laws, and Metropolitan Council policy and procedures for securing data, responding to data breaches or other instances of compromised data, responding to data requests, and disseminating data.
- F. Metropolitan Council employees will be subject to penalties for unlawfully accessing *not public data*. In the event of a willful violation of the Minnesota Government Data Practices Act, the employee is guilty of a misdemeanor, as provided for in Minnesota Statutes, section 13.09.

Links:

***Revision/Review Tracking***

Date	Revision No.	Review Only – No changes