Committee Report

Business Item No. 2015-84

Management Committee

For the Metropolitan Council meeting of May 20, 2015

Subject: Approval of changes to the Data Practices Policy 4-1-1

Proposed Action

That the Metropolitan Council approves changes to Metropolitan Council Policy 4-1-1 Data Practices.

Summary of Committee Discussion/Questions

Lesley Kandaras, senior project coordinator in Regional Administration, presented the item. Councilmember Barber asked how data become classified as “not public” under the Minnesota Government Data Practices Act. Kandaras responded that the state legislature makes that determination. Chair Chávez asked if the Office of General Counsel reviewed the proposed policy revisions. Kandaras answered “yes;” the Office of General Counsel reviewed the proposed policy revisions and the Office of General Counsel is represented on the Council’s Data Privacy Initiative team that developed the proposed revisions.

Motion made by Councilmember Rummel, seconded by Councilmember Barber and passed.

METROPOLITAN COUNCIL

Management Committee

Meeting date: April 22, 2015

For the Metropolitan Council meeting of May 20, 2015

Subject: Approval of changes to the Metropolitan Council Policy, 4-1-1 Data Practices

District(s), Member(s): All

Policy/Legal Reference: 4-Employees in the Workplace

Staff Prepared/Presented: Lesley Kandaras, Senior Project Coordinator, Regional Administration, 651-602-1609

Division/Department: Regional Administration/Office of the Regional Administrator

Proposed Action

That the Metropolitan Council approves changes to Metropolitan Council Policy 4-1-1 Data Practices.

Background

Policies and policy changes must be presented to the Council for approval and adoption.

Rationale

Updating Policy to Reflect 2014 Legislation

The Metropolitan Council's current data practices policy must be updated to conform to changes in state law and to fully reflect the Council's responsibilities for protecting data under the Minnesota Government Data Practices Act.

In 2014, the Minnesota Legislature amended the Minnesota Government Data Practices Act (Minnesota Statutes Chapter 13) to require government entities such as the Council to:

- Adopt a policy and procedures for "ensuring that all not public data[1] are only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for purposes described in the procedure." As part of this access policy, government entities may adopt a policy for governing access to the data (Minnesota Statutes 13.05, subdivision 5 (a) (2) and (3));

- Conduct an "annual security assessment" of any personal information maintained by the government entity" (Minnesota Statutes 13.055, subdivision 6); and

- Abide by reporting requirements and employee penalties if data breaches occur. (Minnesota Statutes 13.055)

To conform to this legislation, the existing Metropolitan Council Data Practices Policy (4-1-1) and Procedure (4-1-1a) will be revised. This business item is to revise the policy.

---

[1] Minnesota Statutes 13.02, subdivision 8a defines "not public data" as "any government data classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected non-public."

METROPOLITAN COUNCIL

Overview of Proposed Policy Changes

Section I. Policy

- Clarifies that the Metropolitan Council's Data Practices Policy is governed by state and federal law.

Section II. Purpose of policy

- Expands the purpose to include protecting data from unauthorized access and use and responding data breaches.

Section III. Background and reasons for policy

- A. Adds language to reflect the range of the Metropolitan Council's responsibilities and roles in data practices.
- B. Cleans up language for accuracy, readability
- C. Adds new section on the policy for sharing data with authorized entities and individuals if allowed by law.
- D. Adds new section on ensuring appropriate access to data and protecting data.
- E. Adds new section on responding to data breaches.

Section IV.

- Cites the Metropolitan Council Resolution that designates the Regional Administrator as the Responsible Authority under the Minnesota Government Data Practices Act. (This is not a new designation; adding the citation is the change.)
- A and B tighten current language; no substantive changes.
- C. Adds "supervisors" to the list of personnel responsible for familiarizing themselves with the policies and procedures and for handling data requests. This section is also amended to tighten existing language.
- D. Requires that managers and supervisors are responsible to ensure that employees under their supervision have access only to *not public data* that they need to perform their work assignments. Requires managers and supervisors to provide updated information to the Responsible Authority as part of the annual assessment required by law.
- E. States that all Metropolitan Council employees are responsible for following federal and state laws and Council policy and procedure relating to data protection and data requests.
- F. States that employees will be subject to penalties for unlawfully accessing *not public data*. If the unlawful access is a data breach as defined by state law, then the employee is guilty of a misdemeanor as provided for in Minnesota Statutes, section 13.09.

Funding

Not applicable

Known Support / Opposition

The Policy and Procedure Steering Committee reviewed the proposed policy revision. No steering committee member requested changes.

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.

METROPOLITAN COUNCIL

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