

Management Committee

Meeting date: April 22, 2015

For the Metropolitan Council meeting of May 13, 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 data¹ 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 must 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.”

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 to 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 language ensuring appropriate access to data and protecting data. Tightens existing language.
- E. Adds new section on responding to data breaches.

Section IV. Implementation/Accountability

- 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. Adds new section stating that managers and supervisors are responsible for ensuring 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. Adds new section stating 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. Adds new section stating that employees will be subject to penalties for unlawfully accessing *not public data*. In the unlawful access is a willful violation 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.