Minnesota Board of Water and Soil Resources
Data Practices Policy

Approved: March 26, 2014
Update approved by Executive Team: October 12, 2015

Purpose: The purpose of the Minnesota Board of Water and Soil Resources Data Practices Policy is to comply with the requirements of the Minnesota Government Data Practices Act (MGDPA), Chapter 13 of Minnesota Statutes, and Minnesota Rules, Chapter 1205. The MGDPA charges government entities to inform the public about the kinds of not public data they collect, keep, and create; to make the data they have accessible to those with a right to have it; and to develop data protection procedures to assure that data on individuals are accurate, complete, current, and secure.

Rule reference or statute: MS § 13.025, MS § 13.05, subd. 5

Executive Team approval date: February 5, 2014

Board approval date: March 26, 2014

Staff author: Tim Dykstal

Procedure

BWSR's policy to comply with the Minnesota Government Data Practices Act (MGDPA) is described in general in this document. More specific policies, procedures, and forms for complying with the MGDPA and its accompanying rules, Minnesota Rules Chapter 1205, are contained in a larger document entitled *Minnesota Board of Water and Resources Data Practices Manual (BWSR Data Practices Manual*). The manual describes BWSR's public data access policy, data subjects' rights and access policy, and the responsibilities of BWSR employees to protect not public data. It also includes as an appendix a data inventory that describes the kinds of private or confidential data that BWSR has. The Data Practices Compliance Official (DPCO) is responsible for maintaining, updating, and distributing the manual. The manual is available to the public on the BWSR website (http://www.bwsr.state.mn.us/) and to employees on the BWSR intranet.

Data Inventory

Appendix B of the *BWSR Data Practices Manual* is the agency's data inventory.

Public Data Access Policy

The MGDPA presumes that all government data are public unless a state or federal law says the data are not public. Government data is a term that means all information a government entity has.

The MGDPA also provides that government entities keep all government data in a way that makes it easy for data subjects to access public data. Data subjects have the right to look at (inspect), free of charge, all public data that government entities keep. Data subjects also have the right to get copies of public data. The MGDPA allows government entities to charge for copies. Data subjects have the right to look at data, free of charge, before deciding to request copies.

For more information about how data subjects can make a data request, and how BWSR responds to a data request, see the *BWSR Data Practices Manual*.

Data Subjects' Rights and Access Policy

The MGDPA says that data subjects have certain rights related to a government entity collecting, keeping, and creating government data about them. A data subject is any person who can be identified from the data that a government entity maintains.

Data Classifications

The MGDPA presumes that all government data are public unless a state or federal law says that the data are not public. Not public data is classified by state law as private, confidential, nonpublic, or protected nonpublic. Refer to the *BWSR Data Practices Manual* and MS § 13.02 for definitions of these classifications.

Data Subjects' Rights under the MGDPA

Government entities must maintain all government data in a way that makes it easy for data subjects to access data about themselves. Also, government entities can collect, keep, and create only those data about data subjects that government entities need for administering and managing programs that are permitted by law. Data subjects have the following rights.

- To look at (inspect), free of charge, public and private data that government entities have about them
- To be notified when government entities ask them to provide data about themselves that are not public
- To protect the not public data that government entities collect, keep, and create about them, and to establish appropriate safeguards to ensure their security
- To challenge the accuracy and/or completeness of public and private data about them.

For more information about these rights, and about making and responding to a data request, see the *BWSR Data Practices Manual*.

Policy for Ensuring the Security of Not Public Data

The MGDPA says that government entities must establish procedures to ensure that all data on individuals is accurate, complete, and current for the purposes for which it was collected, and to establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public 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. BWSR's procedures for ensuring the security of not public data include designating job classifications that have regular access to not public data in its data inventory, listing individual employees who have that access in a shared spreadsheet, and conducting an annual survey of the personal information that the agency maintains. For more information on BWSR's procedures to ensure the security of not public data, see the *BWSR Data Practices Manual*.

Responsibilities

Data Practices Compliance Official: Every government entity is required to designate an employee to act as the entity's Data Practices Compliance Official. The Data Practices Compliance Official (DPCO) is the agency employee to

whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices issues. The DPCO will be responsible to resolve agency compliance issues.

Designee: A designee is a person appointed in writing by the responsible authority to be in charge of individual files or systems containing government data and to receive and comply with requests for government data. Within BWSR, each unit and region has an appointed designee. The designee is responsible for protecting the data their unit collects and keeps about data subjects, as well as the data that it creates. Designees are also responsible to know how that data is classified, to assist staff with data requests, and to attend and provide related training. Designees will refer to the DPCO to resolve compliance issues.

Responsible Authority: According to Minnesota Rules, Part 1205.0200 subp.13, the responsible authority for BWSR is the Executive Director. The responsible authority is accountable for BWSR compliance with the requirements of the MGDPA. Most of the responsible authority duties are detailed in MS § 13.05.

Staff: Each employee is responsible to protect all not public data that they have about data subjects. They are also responsible to notify their unit designee and the DPCO that they have received a request, to provide for inspection and copies of public data at the direction of the designee, and to assist the designee to answer any questions or concerns related to a request. Staff is required to have a basic knowledge of the MGDPA and to reference the *BWSR Data Practices Manual*.

Specific Tasks

The Responsible Authority will:

- Ensure BWSR compliance with all requirements of the MGDPA and Minnesota Rules, Chapter 1205
- Ensure BWSR policy is developed and implemented to address data practices responsibilities
- Determine when the Attorney General's Office will assist the DPCO with data practices issues
- Appoint or designate a Data Practices Compliance Official
- Appoint or designate unit data practice designees to assist DPCO and staff.

The Data Practices Compliance Official will:

- Be knowledgeable about the MGDPA, any related statutory requirements, and Minnesota Rules, Chapter 1205
- Be familiar with BWSR data and classifications under the MGDPA
- Act as the point of contact to the public for any data practices related question, request, or issue
- Maintain a log of public data requests
- Provide public notice on BWSR request policies and procedures
- Assist BWSR staff and designees in responding to data requests, classifying not public data, and protecting not public data.
- Resolve agency compliance issues
- Assist in providing data practices training to staff and designees
- Work directly with the communications director on any request from the media or related to the Governor's Office
- Provide data practices updates and communications to the responsible authority as requested
- Develop BWSR policies and procedures and revise annually to comply with statute
- Represent BWSR on state agency and other data practices committees and forums.
- Lead the annual security assessment of the personal information that BWSR maintains.

Data Practices Designees will:

- Be familiar with the MGDPA, any related statutory requirements and Minnesota Rules, Chapter 1205

- Be knowledgeable about the data their unit collects, keeps, and creates and its classification
- Assist BWSR staff and DPCO in responding to data requests, classifying not public data, and protecting not public data.
- Work with and assist the DPCO with any related data practices issues
- Refer to the DPCO to resolve any compliance issues
- Participate in BWSR data practices training and meetings.

BWSR Managers will:

- When giving access to not public data to employees, sign the Employee Data Access Approval Form that acknowledges they have granted access to those data.

BWSR Employees will:

- Protect the not public data that they have about data subjects
- Comply with all statutory requirements and BWSR policy regarding the MGDPA and the security of not public data.
- Inform their unit designee and the DPCO about any data practices request from the public, media, or other government entity
- At the direction of the designee, provide for the inspection and copy of government documents created, maintained, collected, or stored by BWSR
- Work with their unit designee, and the DPCO as needed, to respond to data requests
- Have a basic knowledge of the MGDPA and reference the manual as needed.
- When given access to not public data by their manager, sign an Employee Data Access Approval Form to acknowledge that they understand their responsibility to protect those data.

Approved by: BWSR Board of Directors
Date: March 26, 2014
Update approved by Executive Team: October 12, 2015