Minnesota Board of Water and Soil Resources
Data Practices Manual

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

Purpose: The BWSR Data Practices Policy outlines the agency's responsibilities for complying with the Minnesota Government Data Practices Act (MGDPA), Chapter 13 of Minnesota Statutes, and Minnesota Rules, Chapter 1205. The purpose of this manual is to specify BWSR's policies, procedures, and forms for complying with the MGDPA.

Audience: BWSR staff

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

Intended use: This 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.

Executive Team approval date: February 5, 2014

Board approval date: March 26, 2014

Staff author: Tim Dykstal

Table of Contents

Purpose

The BWSR Data Practices Policy outlines the agency's responsibilities for complying with the Minnesota Government Data Practices Act (MGDPA), Chapter 13 of Minnesota Statutes, and Minnesota Rules, Chapter 1205. The purpose of this manual is to specify BWSR's policies, procedures, and forms for complying with the MGDPA.

Scope

Chapter 13, section 25 describes the obligations of each government entity under the MGDPA. Each entity must have:

- A public document or data inventory that describes every kind of private or confidential data the agency has (subd. 1).
- A policy explaining the rights the public has to get access to public data (subd. 2).
- A policy explaining the rights data subjects have to get access to data about themselves (subd. 3).

This 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. Appendix B of the manual is BWSR's data inventory. Other required documents, step-by-step procedures, and forms are included as additional appendixes.

Responsibilities

For the responsibilities of individual BWSR employees, see the *Data Practices Policy*. As a whole, BWSR employees will:

- Protect the not public data they have about data subjects
- Comply with all statutory requirements and BWSR policy regarding the MGDPA and the security of not public data.
- Provide for the inspection and copy of government documents created, maintained, collected, or stored by BWSR
- Inform their unit designee and the Data Practices Compliance Official (DPCO) about any data practices request from the public, media, or other government entity. (For a listing of BWSR's unit designees, see Appendix A.)
- 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

Legal Authority and Remedies

Exhaustion of Administrative Remedies: These policies will be administered consistently with Minnesota law. In the event that a requester believes that these policies or implementations are contrary to Minnesota law, the requester may register an objection in writing with the BWSR Executive Director who will provide a prompt ruling.

Records Retention Schedule: Government entities are required to retain and destroy official government records according to a record retention schedule. Requests for documents under the MGDPA must be made available according to the BWSR general retention schedule and the unit's retention schedule.

Data Classifications

The MGDPA regulates the handling of all government data that is created, collected, received, maintained, or disseminated by a state agency, political subdivision, or statewide system no matter what form the data is in, or how it is stored, or how it is used.

The MGDPA regulates:

- what data can be collected
- who may see or have copies of data
- specific classifications of data
- the duties of state agency personnel in administering the MGDPA
- procedures for access to data
- procedures for classifying information as not public
- charging of fees for copies of data

The act establishes a presumption that unless otherwise provided by law, all government data are public. The act then specifies (1) by what authority public access can be limited, and (2) possible data classifications other than public. Almost all government data is either data on individuals or data not on individuals. *Data on individuals* is classified as public, private, or confidential. *Data not on individuals* is classified as public, nonpublic, or protected nonpublic.

General Rule

All government data are public (can be inspected and copied by anyone) (MS § 13.03, subd. 1), but access may be limited by:

- federal statute
- state statute
- temporary classification issued by the Commissioner of Administration

Classification Types

Data governed by state law that are classified as something other than public are classified in one of the following ways:

- **private**: data identifying an individual that are only available to the individual or with the individual's consent (MS § 13.02, subd. 12)
- **confidential**: data identifying an individual that are not available to anyone outside the entity holding the data, including the individual (MS § 13.02, subd. 3)
- **nonpublic**: data on a business or other entity that are only available to the subject of the data or with the subject's consent (MS § 13.02, subd. 9)
- **protected nonpublic**: data on a business or other entity that are not available to the subject of the data or anyone else outside the entity holding the data (MS § 13.02, subd. 13).

Classifications of Data Under the Minnesota Government Data Practices Act			
Type of Data	**Subject of Data (individual or entity)**	**Access (to whom data are available now)**	**When Data Become Available to Public**
General Rule	Individual, business, or other entity	Public	Upon creation or receipt of the data
Private	Individual	Individual who is the subject of the data	(1) Immediately with consent of data subject, or (2) The later of 30 years after creation or ten years after death of the subject
Confidential	Individual	Government entity only	The later of 30 years after creation or ten years after death of the subject
Nonpublic	Business or Other Entity	Business or entity that is the subject of the data	(1) Immediately with consent of data subject, or (2) Ten years after creation or receipt (unless agency determines not in public interest)
Protected Nonpublic	Business or Other Entity	Government entity only	Ten years after creation or receipt (unless agency determines not in public interest)

Data Classification Changes

In general, data retain the classification provided in statute even if they are transferred from one entity to another. The act contains provisions on when the original classification of various types of data changes.

Summary Data

Summary data is information derived from private or confidential data on individuals, but the individuals are not identified. In other words, the summary data doesn't contain any information that can identify a specific individual. Summary data is public data unless classified by statute, federal law, or temporary classification as not public and can be requested in writing by anyone who is willing to pay the cost of preparing it (MS § 13.10, subd. 19). Authority to prepare summary data is found in MS § 13.05, subd. 7.

Data Security Responsibilities (MS § 13.05)

Everyone in BWSR has the responsibility to secure the data in their possession. To ensure data security, you should only collect and store data on individuals that you need to do your job. You should also take steps to protect the data that you have.

General Standards for Collection and Storage

Collection and storage of all data on individuals and the use and dissemination of not public data on individuals shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government (MS § 13.05, subd. 3).

Limitations on Collection and Use of Data

Not public data on an individual shall not be collected, stored, used, or disseminated by government entities for any purposes other than those stated to the individual at the time of collection, in accordance with the rights of data subjects described in this manual and in MS 13.04, except as provided in MS § 13.05, subd. 4. Private data can only be accessed by those authorized in the Tennessen Warning provided when the data was collected, or by those with informed consent of the data subject.

Ensuring the Security of Not Public Data

According to MS § 13.05, subd. 5, 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 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.

If you use not public data in your job, you must take the following steps now to ensure the data is secure:

- Secure physical folders containing not public data and checks lying on office desktops when unattended or overnight (e.g., place in a lockable file cabinet and lock it).
- Lock file cabinets containing not public data when unattended or overnight.
- Maintain physical control of documents containing not public data. For example:
  - Working out a plan with others for where you pass-off/share applications or checks, not just leaving them on someone's desk.
  - When you copy, scan, fax--staying with the document, rather than coming back to retrieve it later.
- Store not public data separately from public data if possible. If you store a piece of private information related to a project separately from the project file, place a note in the public file indicating that a related, not public file exists. BWSR cannot charge for the time it takes to separate not public data from public data.

If you need additional equipment to take these steps, see your supervisor.

For documents containing not public data not covered by the above scenarios: use your common sense to secure them.

BWSR has controls to restrict access to not public data to only those employees whose job classification or work assignment requires access to the data, and to deter unauthorized access.

Data Inventory

Appendix B of this manual is BWSR's data inventory. It describes every kind of not public data the agency has. The data fields listed in the inventory are taken from the MGDPA.

A column in the inventory, "Employee Work Access," designates the employees who require regular access to not public data. In the inventory, employee work access is listed by job classification, not individual employee name.

An additional column in the inventory, "MN.IT Data Protection Categorization," designates the category of data protection that BWSR has assigned to these data fields, as required by the MN.IT Services Enterprise Data Protection Categorization Standard. As of January 1, 2017, state agencies must identify, categorize and document the common data elements used within the agency using these categories:

- High: Data that is highly sensitive and/or protected by law or regulation. This includes, but is not limited to, Social Security Numbers and bank account numbers.
- Moderate: Data that does not meet the definition of Low or High. This includes not public names and addresses.
- Low: Data that is defined by Minnesota Statutes Chapter 13 as "public."

Data Access Approval Spreadsheet

BWSR requires individual employees and their managers to document the data fields that they have access to. A spreadsheet, modeled on the data inventory, is maintained on the agency's shared drive. Individual employees are listed in separate columns. Managers check the data fields that they have granted their employees access to.

The form assumes that an employee's access to not public data is regular and indefinite. If a manager grants employee temporary access to not public data, the form can be modified via a comment box to specify the time period of access. It is the manager's responsibility to note when that period has expired, and to remove the employee's access and the note of it when that period has expired. Any access to not public data will be strictly limited to the data and time period necessary to complete a work assignment.

The agency's annual security assessment (see below) requires managers to certify that they have reviewed the data access approval spreadsheet and granted access to the employees named there, and also requires individual employees to certify that they understand their responsibility to protect the not public data to which they have been granted access.

Additional Controls to Protect Not Public Data

BWSR's additional controls to restrict access to not public data to only authorized employees, and to deter unauthorized access, include:

- 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
- Shredding not public documents before disposing of them

Data Sharing with Authorized Entities or Individuals

State or federal law may authorize the sharing of not public data in specific circumstances. Individuals will have notice of any sharing in applicable Tennessen warnings (see Minnesota Statutes, section 13.04) or BWSR 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.

Penalties for Unlawfully Accessing Not Public Data

BWSR will utilize the penalties for unlawful access to not public data as provided for in Minnesota Statutes, section 13.09, if necessary. Penalties include suspension, dismissal, or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

Destruction of Not Public Data (MS § 13.05, subd.5 (b))

Not public data must be disposed of in a way that prevents its contents from being determined or known.

Electronic Transfer of Not Public Data

Email messages containing not public data must be encrypted. The state network is encrypted. But, if you are sending an email that contains not public data outside of the state network, contact your MN/IT representative if you need encryption assistance. If you are unclear about the classification of the data (public or not public) contact your unit designee. Private data should only be released after consulting your designee and the DPCO.

Portable Computing Devices

Only those with authorized business needs should have not public data stored on a portable computing device (laptop, thumb drive, etc.). Any not public data stored on a portable computing device must be secured, encrypted, and protected. Contact your MN/IT representative with questions or for assistance.

BWSR laptops are required to be encrypted.

Breach in Security of Data (MS § 13.055)

A state agency that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach. Individuals whose private or confidential data has been acquired by an unauthorized person must be notified, in writing, that the agency will investigate the breach, prepare a report on it, and make the report accessible to them, either by mail or email. In addition, Minnesota Statutes 2013, section 3.971, subd. 9 requires state officials to notify the Legislative Auditor when not public government data may have been accessed or used unlawfully.

The report must include:

- a description of the type of data that were accessed or acquired;
- the number of individuals whose data was improperly accessed or acquired;
- if there has been a final disposition of disciplinary action, the name of each employee determined to be responsible for the unauthorized access or acquisition,
- the final disposition of any disciplinary action taken against each employee in response.

If you suspect that private or confidential data on individuals has been breached, contact your unit designee and the DPCO immediately. You may also contact the Legislative Auditor directly.

Annual Security Assessment (MS § 13.055, subd. 6; 325E.61, subd. 1)

Annually, BWSR conducts a comprehensive security assessment of any personal information that it maintains. Personal or personally identifiable information (PII) means a person's first name or first initial and last name *in combination with* any one or more of the following data elements:

- Social Security number;
- Driver's license number or Minnesota identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

According to Minnesota Statutes, section 325E.61, subd. 1, data elements that are secured by encryption or another method of technology that makes electronic data unreadable or unusable are not PII, unless the encryption key, password, or other means necessary for reading or using the data was also acquired.

The annual security assessment lists the type of PII that BWSR maintains, the data formats it is maintained in, where it is located or stored, who has access to it, and what controls BWSR maintains over the data.

Rights of Data Subjects (MS § 13.04)

The MGDPA establishes specific rights for individuals who are the subject of government data and establishes controls on how entities collect, maintain, store, use, and release data about individuals.

These rights allow the data subject to: decide whether to provide the data being requested; see what information the entity maintains about that subject; determine whether that information is accurate, complete and current and what impact the data may have on decisions the entity has made; prevent inaccurate and or incomplete data from creating problems for the individual.

Individuals who are the subject of government data have the right to:

- be given a notice (Tennessen Warning)[1] when they are asked to provide private or confidential data about themselves
- know whether a government entity maintains any data about them and how this data is classified
- inspect, at no charge, all public and private data about them
- have the content and meaning of public and private data explained to them
- have copies of public and private data about them at actual and reasonable cost
- have private or confidential data about them collected, stored, used, or disclosed only in ways that are authorized by law and that are stated in the Tennessen Warning notice, or in ways that the subject has consented via an informed consent
- not have private or confidential data about them disclosed to the public, unless authorized by law
- consent to the release of private data to anyone
- be informed of these rights and how to exercise them.

Appendix D describes the rights of individuals as the subject of government data.

Collecting Private or Confidential Data

Individuals have the right to know what information BWSR collects and maintains about them and how it is classified. When individuals are asked to supply private or confidential data, they must be given a Tennessen Warning notice (Minnesota Statutes, section 13.04, subd. 2).

The notice must be given when:	• An individual • Is asked to supply • Private or confidential data

[1] In addition to the Tennessen Warning, the federal Privacy Act of 1974 requires federal, state, and local government entities requesting Social Security numbers to provide individuals with a notice, as follows: "[a]ny Federal, State, or local government agency which requests an individual to disclose his Social Security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." This is called a federal Privacy Act notice.

	• Concerning self All four conditions must be present to trigger the notice requirement.
The notice does *not* need to be given when:	• The data subject is not an individual • The subject offers information that has not been requested by the entity • The information requested from the subject is about someone else • The entity requests or receives information about the subject from someone else • The information requested from the subject is public data about that subject.
Statements must be included that inform the individual:	• Why the data are being collected and how the entity intends to use the data • Whether the individual may refuse, or is legally required, to supply the data • Any consequences of either supplying, or refusing to supply, the data • The identity of those authorized by law to receive the data.

According to MS § 13.04, subd. 2 (d), a law enforcement officer is not required to provide a Tennessen Warning prior to collecting investigative data.

Accessing Private or Confidential Data

Private data is available only to

- the data subject
- agency staff whose work responsibilities reasonably require access
- those authorized by law to gain access to the data
- anyone with the written consent of the data subject.

Confidential data is available only to:

- BWSR personnel whose work assignments reasonably require it
- those authorized by state or federal law.

Note: Even though individuals cannot access confidential data about themselves, they have a right to know whether confidential data is maintained by BWSR.

Data subjects have the right to:

- view, at no cost, all public and private data maintained about them
- have the data explained to them, upon request
- receive a copy of public and private data about them
- challenge the accuracy and completeness of any public or private data about themselves
- authorize other agencies or persons to see or use private data about them.

Identification

When requesting access to private or confidential data, the requestor must provide identification verifying that they are the data subject or a person who by law is entitled to access. Reasonable measures might include a personal appearance, notarized signature, or other accepted form of identification.

Minor Data

Under certain circumstances, data about a minor data subject maybe withheld from a parent or guardian. Upon the receipt of a request, the responsible authority must determine whether honoring the request is in the best interests of the minor. (See MS § 13.02, subd. 8.) If you receive a request from a minor to deny parental access to private data regarding a minor who is the subject of the data, contact the DPCO. When the request is made from a minor, the DPCO should document each decision to withhold or release data.

Providing Access to the Data Subject

Access to public or private data by the data subject must be complied with immediately if possible, or within 10 working days.

Access to private data by the data subject may be limited to once every six months unless additional data has been collected or created or there is a pending challenge to the accuracy or completeness of the data.

When providing copies of public or private data to the data subject, you *cannot* charge for search and retrieval time.

Release of Private Data/Informed Consent

Private data about an individual may be collected, stored, used, and disseminated only for those purposes stated to the data subject at the time the data was collected, except as permitted by law. However, private data on individuals may be used by, and disseminated to, any individual or agency if the subject of the data has given their informed consent.

Informed Consent

Informed consent is written permission necessary for:

- an individual to ask the entity to release the data
- a new release of the data by the entity
- a different use than described in the Tennessen Warning
- a different release than described in the Tennessen Warning.

If an informed consent is needed your unit designee and the DPCO will provide direction and assistance.

BWSR Procedures for Handling Data Requests

Access to Government Data by the Public (MS § 13.03)

The MGDPA gives all members of the public the right to see and have copies of all public data. All the data that the department has is public and can be seen by anyone unless there is a state statute or federal law that classifies the data as not public.

Citizens have the right to know what types of data BWSR keeps, how the data is classified, and what the procedures are for requesting data. Agencies must respond to data requests in a prompt and appropriate manner and within a reasonable period of time.

The following documents are available on the BWSR Web Site. Their public notice is required by statute.

- Rights of the Public to Access Government Data (Appendix C).
- Requesting Government Data About You (Appendix D).

Receiving a Request for Data

Any BWSR employee can receive a request for information from the public. If you receive one, you should work with your unit designee to determine if that request falls under the auspices of the MGDPA as a data practices request. If it is a data practices request, your designee will work with the DPCO to respond to it. This is to coordinate BWSR's response to data requests.

Determining If It Is a Data Practices Request

A data practices request is a request to see or have copies of data or documents. The request will be for something in a tangible format: voicemail, text, email, etc. Look for words like:

- Minnesota Government Data Practices Act
- Freedom of Information Act
- Data Privacy
- Request, inspect, copy, pursuant to….

What is *not* considered a data practices request:

- Responding to or answering a question
- Providing copies of brochures, information material, etc., that were developed for public distribution.
- Routinely distributing data that is considered a part of your business or customer service function.
- Answering questions for the media as a part of a story or interview, unless the media is requesting to inspect or have copies of documents to research or investigate a topic. Contact the DPCO if you are unsure if the media request should be handled as a data practices request.

Logging Data Requests

If you and your unit designee determined that the request is a data practices request, the designee should notify the DPCO to log the request and work with the DPCO to determine how the request will be handled.

Handling Data Requests

This section is intended for designees and the DPCO.

In order to properly respond to requests for data it is important to identify the types of data BWSR maintains and to determine how each type of data is classified.

Determine the following:

What specific data is being requested?

To appropriately respond to a request, first determine what specific data is being requested. Seek further clarification from the requestor if needed in order to fully understand what is being requested. *According to Minnesota statute, you cannot require the requester to provide identification, a reason for the request, or to justify the request; however, a person may be asked to provide certain clarifying information for the sole purpose of facilitating access to data.*

Does the data exist in the format requested?

Data should be provided in the format in which it was created for BWSR purposes. You are not required to reproduce data in a different format or to create documents. If data is requested in electronic format and we have it in electronic format, we must provide it in electronic format.

If BWSR maintains the requested data, how is the data classified?
If the data is public data, it must be made available for inspection and copies as soon as reasonably possible.

If you have questions about whether or not the data can be released, let the requester know that you will determine the classification of the data and get back to them.

If it is determined that the data is not public, inform the requestor that the data cannot be released. This may be done orally at the time of the request or in writing as soon as possible after the request has been made. You must cite the specific section of law that classifies the data as not public.

The classification of the data will determine how to respond to a request.

If the Request is for Public Data
Public data is accessible to anyone for any reason. Accessible means the public has the right to come to a BWSR office at reasonable a time to view the data and to obtain copies at a reasonable fee.

According to statute, you must respond to a data request in an appropriate and prompt manner.[2] *It is important to respond to the requester in writing as soon as possible. Let the requester know you have received the request, how the request will be handled, and the approximate time it will take to gather the information.*

Remember that persons are not required to identify themselves, or state a reason for, or justify a request for public data: however, a person may be asked to provide certain clarifying information for the sole purpose of facilitating access to the data.

Agencies are required to keep data easily accessible for convenient use, but are not required to organize data according to the desires of a particular requester or to create data that does not already exist.

BWSR cannot charge for the time it takes to separate not public data from public data.

The requester has a right to have public data explained in an understandable way, including the meaning of technical terminology, abbreviations, words, or phrases.

Request for Copies of Public Data
Copies should be provided as soon as reasonably possible. See Appendix F for copy costs and procedures. Fees must be paid prior to receiving the documents. Complete and submit the Data Copy Cost Worksheet with the payment to your business manager.

If copies are requested in electronic format, and BWSR maintains the data in electronic format, the data must be provided in that format. Staff time can be charged to transmit electronic data. See Appendix F.

---

[2] What is appropriate and prompt depends on the scope of the request and may vary depending on such factors as the type and quantity of data requested, the clarity of the request, and the number of staff available to respond to the request. If the requester is the subject of the data, you MUST respond within 10 days.

For complicated requests or those of special concern, a set of the copies provided to the requester should be kept for future reference.

Request to Inspect Public Data

If the request is to inspect data, it is important that the documents be reviewed during normal work hours at the BWSR office where the data is kept. Staff should be present to answer questions about the meaning of the data and so that original copies do not leave the office. There is never a charge to inspect data.

If copies of the inspected data are requested, copy fees apply. If you are not able to make copies at the time of inspection due to volume, or staff availability, make them as soon as reasonably possible. Payment is required prior to receiving the copies. See Appendix F.

Requestors may bring in their own scanners or copy machines to make copies.

If the Request is for Private Data by Data Subject

If the requester is the subject of the data, see the "Rights of Data Subjects" on page 7. Requests for private data by the data subject must be responded to within 10 working days. For private data, the data subject will be asked for proof of identification.

If the Request is for Summary Data

According to Minnesota Rules 1205.0700, subp. 4, BWSR must prepare summary data if the request is in writing and if the requestor is willing to pay the cost to prepare the data. Within 10 days of receiving a written request for summary data, the requester should be informed of the estimated costs if any, and either:

- be provided with the summary data requested
- receive a written statement describing a time schedule for preparing the summary data, including reasons for any time delays
- be provided access to the private or confidential data for the purpose of preparing the summary data, with the appropriate nondisclosure agreement, or
- receive a written statement stating reasons why it has been determined that the requester's access would compromise the private or confidential data.

If you receive a request for summary data contact your unit designee or the DPCO.

If the Request is for Not Public Data

If data cannot be released because it is classified as not public data, let the requester know as soon as possible and cite the specific statute that prohibits release. BWSR may not share not public data with another entity, unless required or permitted by state statute or federal law.

Appendix A: Data Practices Responsible Authority and Designees

Responsible Authority - The Executive Director is the responsible authority.
Data Practices Compliance Official- The Compliance Coordinator is the data practices compliance official.

"Designee" means any person designated by a responsible authority to be in charge of individual files or systems containing government data and to receive and comply with requests for government data (MS § 13.03, subd. 6.)

Unit	Designee
Administrative Services	Administrative Director/CFO
Easements / Private Lands Conservation	Section Manager
Human Resources	Human Resources Officer
MN.IT Services	MN.IT Services Manager
Central Region	Section Manager
Local Water Management	Assistant Section Manager
Northern Region	Regional Manager
Organizational Effectiveness	Org Effectiveness Manager
Programs and Policy Development	Assistant Director
Regional Operations	Assistant Director
Southern Region	Regional Manager
Strategy and Operations	Assistant Director
Technical Services	Chief Engineer / Manager
Wetland Banking	Wetland Banking Coordinator
Wetlands	Section Manager
WCA Operations	WCA Coordinator

Appendix B: Not Public Data Maintained by the Agency

Minnesota Statutes, section 13.025, subd. 1 requires government entities to prepare and annually update to maintain its accuracy an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's government entity.

Private and confidential data, according to Minnesota Statutes, section 13.02, are data on individuals. Nonpublic and protected nonpublic data, according to Minnesota Statutes are data not on individuals.

Always refer to Chapter 13 and data coded elsewhere to determine the classification of data. Data can change classification depending on variety of circumstance, processes, criteria, or time lines. Nonpublic and protected nonpublic data become public ten years after creation or collection.

Name of Data File or Record	Description	Classification	Statute	Responsible Designee	Employee Work Access
Electronic Access Data	Data created, collected, or maintained about a person's access to a government entity's computer	Private/ Nonpublic	13.15	Information Technology	MN.IT Services Manager, Administrative Director, Organizational Effectiveness Manager, section managers
Federal Contract Data	To the extent that a federal agency requires it as a condition for contracting, data collected and maintained because the agency contracts with a federal agency	Private/ Nonpublic	13.35	Administrative Director, associated program managers	Designated employees in Administrative Services and Easements Section
Social Security Numbers	The Social Security numbers of individuals, whether provided in whole or in part, collected or maintained by a government entity, except to the extent that access to the Social Security number is specifically authorized by law	Private	13.355	Administrative Director, associated program managers	Designated employees in Administrative Services and Easements Section
Contact and Online Account Information	Data on an individual collected, maintained, or received for notification purposes or as part of a subscription list for an entity's	Private	13.356	Organizational Effectiveness Manager	Communications Director; Designated employees on an

Name of Data File or Record	Description	Classification	Statute	Responsible Designee	Employee Work Access
	electronic periodic publications as requested by the individual: • telephone number • e-mail address • internet user name, password, internet protocol address, and any similar data related to the individual's online account or access procedures				as needed basis as part of specific work assignments
General Nonpublic Data	Government data that would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury. E.g., bank account numbers, credit card numbers.	Private/ Nonpublic	13.37	All section managers	Designated employees on an as needed basis as part of specific work assignments
Parking Space Leasing Data	Data on an applicant for, or lessee of, a parking space: • residence address • home telephone number • beginning and ending work hours • place of employment • work telephone number • location of the parking space	Private	13.37	Administrative Director	Administrative Director
Active Investigative Data	Data collected as part of an active investigation undertaken for a pending civil legal action (does not apply to data regarding timeliness of agency response to data request)	Confidential/ Protected Nonpublic	13.39, subd. 2, 4 (Civil)	Administrative Director, associated program managers	Administrative Director, associated program managers
Internal Auditing Data, before publication, or the ending of active pursuit, of an audit	Data, notes, and preliminary drafts of reports created, collected, and maintained by internal audit, or persons performing audits	Confidential/ Protected Nonpublic	13.392, subd. 1	Compliance Coordinator	Compliance Coordinator
Internal Auditing Data	Data on an individual supplying information for an audit or investigation, if the information supplied would not have been	Private	13.392, subd. 2	Administrative Director, Compliance Coordinator,	Administrative Director, Compliance Coordinator,

Name of Data File or Record	Description	Classification	Statute	Responsible Designee	Employee Work Access
	provided without an assurance that the individual's identity would remain private			section managers	section managers
Personnel Data, Applicants	The following data from job applicants are private: • name, unless applicant is selected to be interviewed • address, unless applicant is selected to be interviewed • phone number, unless applicant is selected to be interviewed • information on dependents • SSN	Private	13.43, subd. 3, 4	Administrative Director/Human Resources Officer	Administrative Director/Human Resources Officer/Office and Administrative Specialist Principal
	The following data from job applicants are public: • veteran status • relevant test scores • rank on eligible list • job history • education and training • work availability	Public	13.43, subd. 3, 4	Administrative Director/Human Resources Officer	Public
Personnel Data on individuals, including employees, volunteers, and independent contractors	The following data from employees are public: • name • employee identification number, which must not be the employee's SSN • actual gross salary • salary range • terms and conditions of employment relationship • contract fees • actual gross pension • the value and nature of employer paid fringe benefits • the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary	Public	13.43, subds. 1 and 2 (a)(1)	Administrative Director Human Resources Officer/various units	Public
	• job title and bargaining unit • job description • education and training background	Public	13.43, subd. 2 (a)(2)		Public

Name of Data File or Record	Description	Classification	Statute	Responsible Designee	Employee Work Access
	• previous work experience				
	• date of first and last employment	Public	13.43, subd. 2 (a)(3)		Public
	• work location • work telephone number • badge number • work-related continuing education • honors and awards received	Public	13.43, subd. 2 (a)(7)		Public
	• payroll time sheets or similar data showing employee's work time, (excluding data that would reveal reasons for the use of sick or other medical leave or other not public data.)	Public	13.43, subd. 2 (a)(8)		Public
Individuals who are independent contractors (or are a subcontractor or employee)	• personal phone number • home address • e-mail address • SSN	Private	13.43, subd. 19; 13.43, subd. 17; 13.355	Administrative Director, associated program managers	Administrative Director, associated program managers
Personnel Data on current and former employees, applicants, volunteers, and independent contractors	Other personnel data, including data pertaining to an employee's dependents, not listed in 13.43, including: • address • phone number • information on dependents • use of benefits • SSN	Private	13.43, subd. 1, 4; 13.43, subd. 17	Administrative Director/Human Resources Officer	Administrative Director/Human Resources Officer/Office and Administrative Specialist Principal
Complaints or Charges	The existence and status of any complaints or charge against an employee	Public	13.43, subd. 2 (a)(4)	Administrative Director	Administrative Director/Human Resources Officer
Open/Active Employee Misconduct Investigation	Investigative notes, data, draft reports related to employment or misconduct	Confidential/ Protected Nonpublic or Private	13.393; 13.43, subd. 2 (d); 13.43,	Administrative Director/Human Resources Officer	Administrative Director/Human Resources Officer

Name of Data File or Record	Description	Classification	Statute	Responsible Designee	Employee Work Access
			subd. 8, 11		
Closed Employee Misconduct Investigation	Completed misconduct investigation that results in disciplinary action (but not data identifying employees who were sources of confidential information, which remains private data)	Public	13.43, subd. 2 (a)(5); 13.43, subd. 2 (f); 13.43, subd. 8, 11	Administrative Director/Human Resources Officer	Public
Closed Employee Misconduct Investigation	Completed misconduct investigation that does NOT result in disciplinary action	Private	13.43, subd. 2 (b)	Administrative Director/Human Resources Officer	Administrative Director/Human Resources Officer
Settlements	Terms of any agreement settling an employment dispute	Public	13.43, subd. 2 (a)(6); 13.43, subd. 10	Administrative Director/Human Resources Officer	Administrative Director/Human Resources Officer
Closed Investigation of Public Official	Completion investigation of a public official (or if a public official resigns or is terminated during investigation)	Public	13.43, subd. 2 (e) and (f)	Executive Director	Public
Worker's Compensation Records	Some information that is collected in connection with work related injuries or illness	Private/ Nonpublic	13.43, subds. 4, 18; 13.7905; 176.138	Human Resources Officer	Administrative Director/Human Resources Officer/section managers
Property Complaint Data	The identities of individuals who register complaints with government entities concerning violations of state laws or local ordinances concerning the use of real property	Confidential	13.44, subd. 1	Assistant Director, Programs and Policy/section managers	Any employee may receive a complaint.
Responses to RFB/RFP--until proposal/bid is due	Until time/date when response or bid is due, all data submitted by responder is private or nonpublic.	Private/ Nonpublic	13.591, subd. 3	Any project manager contracting with a private entity	Members of the evaluation team, as designated by the section manager
Responses to RFB/RFP--after proposal/bid is due	After response or bid is due, only name of responder is public (as to RFP) and the name and amount bid (as to RFB).	Private/ Nonpublic	13.591, subd. 3	Any project manager contracting with a private entity	Members of the evaluation team, as designated by the section manager
Responses to RFB/RFP– after bid is selected	After selection (RFB) or contract negotiation (RFP), all data of responder (except § 13.37 trade	Public	13.591, subd. 3	Any project manager	Members of the evaluation team, as designated by

Name of Data File or Record	Description	Classification	Statute	Responsible Designee	Employee Work Access
on RFB or contract is negotiated on RFP	secret data) become public. (Copyright or other protected class claims do not prevent public access.)			contracting with a private entity	the section manager
RFB/RFP Evaluative Data	Data of agency used to evaluate responses to RFB/RFP--until completion of selection, when becomes public (except § 13.37 designated trade secret data)	Protected Nonpublic	13.591, subd. 4	Any project manager contracting with a private entity	Members of the evaluation team, as designated by the section manager
Easements acquired with Outdoor Heritage Fund dollars	Acquisition data such as appraisals may remain private during negotiations but must ultimately be made public according to chapter 13. SSNs and bank account information will remain private.	Private	97A.056, subd. 13; 13.355	Easements Section Manager	Easements Section Manager, Easement Program Analyst
Easements acquired with federal partners	Easement data subject to Section 1619 of the Farm Bill will remain private. All other data is public (except SSNs and bank account information).	Private	Section 1619 of the 2008 Farm Bill; 13.355	Easements Section Manager	Easements Section Manager, Easement Program Analyst
All other easements	All data is public (except SSNs and bank account information).	Public		Easements Section Manager	Public
Grant Data, before selection	Data created for grant RFP until request is published; responses to RFP; evaluation data. After responses are opened, name, address, and amount become public.	Private/ Nonpublic/ Protected Nonpublic	13.599	Grants/All	Members of the evaluation team, as designated by the section manager
Grant Data, after selection	After selection, all data become public (except § 13.37 trade secret data)	Public	13.599	Grants/All	Members of the evaluation team, as designated by the section manager
Applicants For Appointment to the Board, before appointment; Legislative Data	All data on Applicant is private except the following are public: • name • city of residence • education and training • past employment and volunteer work • government service • awards and honors • veteran status • data provided pursuant to §15.0597 (email, telephone,	Private	13.601, subd. 3 (a); 15.097	Executive Director	Executive Director, Executive Assistant to the Board

Name of Data File or Record	Description	Classification	Statute	Responsible Designee	Employee Work Access
	felony record, gender, political party, disability, race, national origin, etc.)				
Persons Appointed to the Board, after appointment	After appointment, the following are public: • residential address • telephone number or e-mail address or both (any agency-assigned e-mail address is always public) • first and last dates of service • the existence and status of any complaints or charges against the applicant, and any final investigative report (All other appointee data is public.)	Public	13.601 subd. 3 (b) and (c); 13.43, subd. 2 (e) and (f)	Executive Director	Public
Easements, Corporate Applicants, Federal Tax ID Numbers	Entities, trusts, partnerships, corporations applying to an easement program	Protected Nonpublic		Easements Section Manager	Easements Section Manager, Easement Program Analyst
Legislative & Budget Proposals	Proposals, supporting data, and preliminary drafts until presented. Preliminary drafts remain protected nonpublic.	Protected Nonpublic	13.605	Assistant Directors/ section managers	Designated employees on an as needed basis as part of specific work assignments

Appendix C: Rights of the Public to Access Government Data

This document is required by Minnesota Statutes, section 13.025.

Right to Access Public Data

The Minnesota Government Data Practices Act (Minnesota Statutes, Chapter 13) 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 recorded information a government entity has, including paper, email, DVDs, photographs, etc.

The Data Practices Act also provides that BWSR must keep all government data in a way that makes it easy for you, as a member of the public, to access public data. You have the right to look at (inspect), free of charge, all public data that we keep. You also have the right to get copies of public data. The Data Practices Act allows us to charge for copies. You have the right to look at data, free of charge, before deciding to request copies.

How to Make a Data Request

To look at or request copies of data, make your request to the BWSR Data Practices Compliance Official (DPCO). We encourage you to use the data request form provided, but you are not required to use the form. Even if you do not use the form, we ask you to submit your request in writing.

If you choose not to use the data request form, your request should include:

- that you, as a member of the public, are making a request for data under the Data Practices Act, Minnesota Statutes, Chapter 13;
- whether you would like to look at the data, get copies of the data, or both; and
- a clear description of the data you would like to inspect or have copied.

BWSR cannot require you, as a member of the public, to identify yourself or explain the reason for your data request. However, depending on how you want us to process your request (if, for example, you want us to mail you copies of data), we may need some information about you. If you choose not to give us any identifying information, we will provide you with contact information so you may check on the status of your request. In addition, please keep in mind that if we do not understand your request and have no way to contact you, we will not be able to begin processing your request.

How We Respond to a Data Request

Upon receiving your request, we will work to process it.

- If we do not have the data, we will notify you as soon as reasonably possible.
- If we have the data, but the data are not public, we will notify you as soon as reasonably possible and state which specific law says the data are not public.
- If we have the data, and the data are public, we will respond to your request appropriately and promptly, within a reasonable amount of time by doing one of the following:
    - arrange a date, time, and place to inspect data, for free, if your request is to look at the data, or
    - provide you with copies of the data as soon as reasonably possible. You may choose to pick up your copies, or we will mail or fax them to you. If you want us to send you the copies, you will need to provide us with an address or fax number. We will provide electronic copies (such as email or CD-ROM) upon request if we keep the data in electronic format.

If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please let us know. We will give you an explanation if you ask.

The Data Practices Act does not require us to create or collect new data in response to a data request if we do not already have the data, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. (For example, if the data you request are on paper only, we are not required to create electronic documents to respond to your request.) If we agree to create data in response to your request, we will work with you on the details of your request, including cost and response time.

In addition, the Data Practices Act does not require us to answer questions that are not requests for data.

Requests for Summary Data

Summary data are statistical records or reports that are prepared by removing all identifiers from private or confidential data on individuals. The preparation of summary data is not a means to gain access to private or confidential data. We will prepare summary data if you make your request in writing and pay for the cost of creating the data. Upon receiving your written request, we will respond within ten business days with the data or details of when the data will be ready and how much we will charge.

Data Practices Contacts

BWSR Responsible Authority:

Executive Director
520 Lafayette Road North
St. Paul, MN 55155-4046

BWSR Data Practice Compliance Official:

Compliance Coordinator
520 Lafayette Road North
St. Paul, MN 55155
Telephone: 651-296-1287
Fax: 651-297-5615

Copy Costs for Members of the Public

BWSR charges members of the public for copies of government data under Minnesota Statutes, section 13.03, subd. 3(c).

- You must pay for the copies before we will give them to you.
- We do not charge for copies if the cost is less than $10.

Charges

Paper Copies (black and white, letter or legal size paper copies cost .25 cents for a one-sided copy, or .50 cents for a two-sided copy)

- For 100 or Fewer Paper Copies – .25 cents per page
- For 100 or More Paper Copies - .25 cents per page, plus other actual costs

For All Other Copies (data stored electronically, CDs, DVDs, maps, photographs, etc.)

- Actual Costs

Actual Costs

The charge for most other types of copies, when a charge is not set by statute or rule, is the actual cost of searching for and retrieving the data, and making the copies or electronically transmitting the data (e.g. sending the data by email).

In determining the actual cost of making copies, we factor in employee time, the cost of the materials onto which we are copying the data (paper, CD, DVD, etc.), and mailing costs (if any). If your request is for copies of data that we cannot reproduce ourselves, such as photographs, we will charge you the actual cost we must pay an outside vendor for the copies.

Searching, retrieving and copying costs will be based on the hourly salary rate plus the cost of benefits for the lowest-paid BWSR employee who could have completed the task. Copying costs will include the actual cost of the copies. Clients will charged in quarter-hour increments. Additionally, postage costs will be charged if the data is not picked up at the BWSR office.

At the discretion of BWSR, requestors may be required to pay up to one-half of the estimated copy cost prior to search and retrieval. Considerations include the amount of data requested, number of locations data is kept, and number of staff required to conduct searches.

Data Request Form

Note: You are not required to use this form. It is for convenience only. However, we may not be able to clarify your request or provide copies without contact information.

		Date:
Name:		
Address:		
City:	State:	Zip:
Phone Number:	Email:	

I am requesting access to data in the following way:

☐ Inspection ☐ Copies ☐ Both inspection and copies

Minnesota Statutes section 13.03, subd. 3, authorizes BWSR to charge fees to recover costs to provide copies of data. Prepayment is required prior to receiving copies of data.

These are the data I am requesting:

Describe the data you are requesting as specifically as possible. If you need more space, please use the back of this form.

Submit by mail or fax to:

Minnesota Board of Water and Soil Resources
BWSR Data Practice Compliance Official
520 Lafayette Road North
St. Paul, MN 55155
Telephone: 651-296-1287
Fax: 651-297-5615

We will respond to your request as soon as reasonably possible.

Appendix D: Requesting Government Data About You

This document is required by Minnesota Statutes, section 13.025.

Data about You

The Minnesota Government Data Practices Act (Minnesota Statutes, Chapter 13) says that data subjects have certain rights related to a government entity collecting, creating, and keeping government data about them. You are the subject of data when you can be identified from the data. Government data is a term that means all recorded information a government entity has, including paper, email, DVDs, photographs, etc.

Classification of Data about You

The Data Practices Act presumes that all government data are public unless a state or federal law says that the data are not public. Data about you are classified by state law as public, private, or confidential.
Public data: We must give public data to anyone who asks; it does not matter who is asking for the data or why.
Private data: We cannot give private data to the general public, but you have access when the data are about you. We can share your private data with you, with someone who has your permission, with our government entity staff who need the data to do their work, and as permitted by law or court order.
Confidential data: Confidential data have the most protection. Neither the public nor you can get access even when the confidential data are about you. . We can share confidential data about you with our government entity staff who need the data to do their work and to others as permitted by law or court order. We cannot give you access to confidential data.

Your Rights under the Data Practices Act

BWSR must keep all government data in a way that makes it easy for you to access data about you. Also, we can collect and keep only those data about you that we need for administering and managing programs that are permitted by law. As a data subject, you have the following rights.

Your Access to Your Data: You have the right to look at (inspect), free of charge, public and private data that we keep about you. You also have the right to get copies of public and private data about you. The Data Practices Act allows us to charge for copies. You have the right to look at data, free of charge, before deciding to request copies.

Also, if you ask, we will tell you whether we keep data about you and whether the data are public, private, or confidential.

As a parent, you have the right to look at and get copies of public and private data about your minor children (under the age of 18). As a legally appointed guardian, you have the right to look at and get copies of public and private data about an individual for whom you are appointed guardian.

Minors have the right to ask this government entity not to give data about them to their parent or guardian. If you are a minor, we will tell you that you have this right. We may ask you to put your request in writing and to include the reasons that we should deny your parents access to the data. We will make the final decision about your request based on your best interests. **Note**: Minors do not have this right if the data in question are educational data maintained by an educational agency or institution.

When We Collect Data from You: When we ask you to provide data about yourself that are not public, we must give you a notice. The notice is sometimes called a Tennessen Warning. The notice controls what we do with the data that we collect from you. Usually, we can use and release the data only in the ways described in the notice.

We will ask for your written permission if we need to use or release private data about you in a different way, or if you ask us to release the data to another person. This permission is called informed consent.

Protecting Your Data: The Data Practices Act requires us to protect your data. We have established appropriate safeguards to ensure that your data are safe. In the unfortunate event that we determine a security breach has occurred and an unauthorized person has gained access to your data, we will notify you as required by law.

When your Data are Inaccurate and/or Incomplete: You have the right to challenge the accuracy and/or completeness of public and private data about you. You also have the right to appeal our decision. If you are a minor, your parent or guardian has the right to challenge data about you.

How to Make a Request for Your Data

To look at data or request copies of data that BWSR keeps about you, your minor children, or an individual for whom you have been appointed legal guardian, make your request to the BWSR Data Practices Compliance Official (DPCO). We encourage you to use the data request form provided, but you are not required to use the form. Even if you do not use the form, we ask you to submit your request in writing.

If you choose not to use the data request form, your request should include:

- that you, as a member of the public, are making a request for data under the Data Practices Act, Minnesota Statutes, Chapter 13;
- whether you would like to look at the data, get copies of the data, or both; and
- a clear description of the data you would like to inspect or have copied.
- identifying information that proves you are the data subject, or data subject's parent/guardian if you are requesting private data.

Identification

BWSR requires proof of your identity before we can respond to your request for private data. If you are requesting data about your minor child, you must show proof that you are the minor's parent. If you are a guardian, you must show legal documentation of your guardianship. One of the following will provide proof of identity: a state driver's license, military ID, passport, or Minnesota ID.

How We Respond to a Data Request

Once you make your request, we will work to process your request. If it is not clear what data you are requesting, we will ask you for clarification.

- If we do not have the data, we will notify you within 10 business days.
- If we have the data, but the data are confidential or private data that are not about you, we will notify you within 10 business days and state which specific law says you cannot access the data.
- If we have the data, and the data are public or private data about you, we will respond to your request within 10 business days, by doing one of the following:
    - arrange a date, time, and place to inspect data, for free, if your request is to look at the data, or
    - provide you with copies of the data within 10 business days. You may choose to pick up your copies, or we will mail them to you. We will provide electronic copies upon request if we keep the data in electronic format.

After we have provided you with access to data about you, we do not have to show you the data again for 6 months unless there is a dispute or we collect or create new data about you.

If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please let us know. We will give you an explanation if you ask.

The Data Practices Act does not require us to create or collect new data in response to a data request if we do not already have the data, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. (For example, if the data you request are on paper only, we are not required to create electronic documents to respond to your request.) If we agree to create data in response to your request, we will work with you on the details of your request, including cost and response time.

In addition, we are not required under the Data Practices Act to respond to questions that are not specific requests for data.

Data Practices Contacts

BWSR Responsible Authority
Executive Director
520 Lafayette Road North
St. Paul, MN 55155-4046

BWSR Data Practice Compliance Official
520 Lafayette Road North
St. Paul, MN 55155
Telephone: 651-296-1287
Fax: 651-297-5615

Copy Costs for Data Subjects

BWSR may charge data subjects for copies of government data under the Data Practices Act, section 13.04, subd. 3(c).

- You must pay for the copies before we will give them to you.
- We do not charge for copies if the cost is less than $10.
- We do not charge to inspect data or to separate public from not public data.
- When data is about you we do not charge for search and retrieval time.

Charges

Paper Copies (black and white, letter or legal size paper copies cost .25 cents for a one-sided copy, or .50 cents for a two-sided copy)

- For 100 or Fewer Paper Copies – .25 cents per page
- For 100 or More Paper Copies - .25 cents per page, plus other actual costs

For All Other Copies (data stored electronically, CDs, DVDs, maps, photographs, etc.)

- Actual Costs

Actual Costs

The charge for most other types of copies, when a charge is not set by statute or rule, is the actual cost of searching for and retrieving the data, and making the copies or electronically transmitting the data (e.g. sending the data by email).

In determining the actual cost of making copies, we factor in employee time, the cost of the materials onto which we are copying the data (paper, CD, DVD, etc.), and mailing costs (if any). If your request is for copies of data that

we cannot reproduce ourselves, such as photographs, we will charge you the actual cost we must pay an outside vendor for the copies.

Searching, retrieving and copying costs will be based on the hourly salary rate plus the cost of benefits for the lowest-paid BWSR employee who could have completed the task. Copying costs will include the actual cost of the copies. Clients will charged in quarter-hour increments. Additionally, postage costs will be charged if the data is not picked up at the BWSR office.

At the discretion of BWSR, requestors may be required to pay up to one-half of the estimated copy cost prior to search and retrieval. Considerations include the amount of data requested, number of locations data is kept, and number of staff required to conduct searches.

Data Subject Request Form

Note: You are not required to use this form. It is for convenience only. However, we may not be able to clarify your request or provide copies without contact information.

		Date:
Name:		
Address:		
City:	State:	Zip:
Phone Number:	Email:	

For private data requestor must provide proof of identity. ID Provided:

☐ Driver's License ☐ MN I.D. ☐ Passport

I am requesting access to data in the following way:

☐ Inspection ☐ Copies ☐ Both inspection and copies

Minnesota Statutes section 13.03, subd. 3, authorizes BWSR to charge fees to recover costs to provide copies of data. Prepayment is required prior to receiving copies of data.

These are the data I am requesting:

Describe the data you are requesting as specifically as possible. If you need more space, please use the back of this form.

Submit by mail or fax to:

Minnesota Board of Water and Soil Resources
BWSR Data Practice Compliance Official
520 Lafayette Road North
St. Paul, MN 55155
Telephone: 651-296-1287
Fax: 651-297-5615

We will respond to your request as soon as reasonably possible.

Appendix E: Data Copy Costs and Worksheet

Copy Costs for Members of the Public

BWSR charges members of the public for copies of government data under Minnesota Statutes, section 13.03, subd. 3(c).

- You must pay for the copies before we will give them to you.
- We do not charge for copies if the cost is less than $10.

Charges

Paper Copies (black and white, letter or legal size paper copies cost .25 cents for a one-sided copy, or .50 cents for a two-sided copy)

- For 100 or Fewer Paper Copies – .25 cents per page
- For 100 or More Paper Copies - .25 cents per page, plus other actual costs

For All Other Copies (data stored electronically, CDs, DVDs, maps, photographs, etc.)

- Actual Costs

Actual Costs

The charge for most other types of copies, when a charge is not set by statute or rule, is the actual cost of searching for and retrieving the data, and making the copies or electronically transmitting the data (e.g. sending the data by email).

In determining the actual cost of making copies, we factor in employee time, the cost of the materials onto which we are copying the data (paper, CD, DVD, etc.), and mailing costs (if any). If your request is for copies of data that we cannot reproduce ourselves, such as photographs, we will charge you the actual cost we must pay an outside vendor for the copies.

Searching, retrieving and copying costs will be based on the hourly salary rate plus the cost of benefits for the lowest-paid BWSR employee who could have completed the task. Copying costs will include the actual cost of the copies. Clients will charged in quarter-hour increments. Additionally, postage costs will be charged if the data is not picked up at the BWSR office.

At the discretion of BWSR, requestors may be required to pay up to one-half of the estimated copy cost prior to search and retrieval. Considerations include the amount of data requested, number of locations data is kept, and number of staff required to conduct searches.

Data Copy Costs Worksheet

This Form is for BWSR Internal Use Only

Section: _____ Date: _____

Requester Name	Address	Phone
BWSR Staff Name	Address	Phone

Description	Quantity	Unit Cost	Line Total
Paper Copies		$ .25	
Employee Name & Salary Fees (List)			
Materials (List)			
Postage			
Total Cost			

Submit a copy to the Accounting Officer along with payment.
520 Lafayette Road North, St. Paul, MN 55155

List the account(s) that incurred the above expenses: _____