



Minnesota IT Services Government Data Practices Manual

MNIT Policies, Procedures and Forms

7/22/2025

Table of Contents

Introduction.....	4
The Minnesota Government Data Practices Act	4
Compliance with the Data Practices Act	4
Contracts.....	5
Government Data	5
Data Classifications	5
Role of the Administration.....	9
Role of the Chief Information Officer.....	9
Responsible authority and designated.....	10
Responsible Authority.....	10
Data Practices Compliance Official	10
Procedures to access public data.....	11
Requesting Public Data	11
Requesting Specific Types of Data	11
What to Say in Your Request	11
How We Will Respond to Your Request.....	11
If We Do Not Have Data.....	12
Possible Costs for Copies of Data – there may be a charge	12
Inspecting Data – no charge	12
Data with Commercial Value – there may be a charge	13
Summary Data – there may be a charge.....	13
Denying Access to Data.....	13
Access to Other Agencies’ Data Under IT Consolidation	13
Sample Data Request Form for Members of the Public.....	14
Rights of subjects’ data.....	15
Subject of Government Data.....	15
Summary of Rights of Individuals Who Are the Subjects of Government Data.....	15
Who May Exercise the Rights of the Individual?	16
Controls on the Collection / Storage of Data on Individuals	16
How to Obtain MNIT Information About You	16

Identification Issues	17
Additional Information on Data Subject Requests	18
Access to Other Agencies' Data Under IT Consolidation	18
Sample Data Request Form for Data Subjects	19
Further Requests	20
Challenging the Accuracy of Data	20
Granting Access to Others	21
What is the Connection Between a Tennessee Warning Notice and an Informed Consent?	21
Sample Consent for Release of Information Form	22
The Tennessee Warning Notice.....	24
Minnesota Statutes section 13.04, subdivision 2.....	24
Procedures to limit the collection and use of private	25
Limitations on Collection and Use of Data	25
Data Protection.....	25
Fees.....	26
For 100 or Fewer Paper Copies of Public Data – 25 Cents Per Page.....	26
Most Other Types of Copies – Actual Cost.....	26

Introduction

This policy and information document is, among other things, intended to provide direction and procedures for access to and/or copies of government data maintained or collected by Minnesota IT Services (f/k/a Office of Enterprise Technology and d/b/a MNIT). This document satisfies requirements under Minnesota Statutes section 13.05.

This document is also intended to provide guidance to Minnesota IT Services (MNIT) employees who respond to requests for MNIT data; any departure from this guidance must be authorized by the MNIT Data Practices Compliance Official. All responses to requests for MNIT data must be coordinated through the MNIT Data Practices Compliance Official.

The Minnesota Government Data Practices Act

The Minnesota Government Data Practices Act (MGDPA or Data Practices Act), which is Chapter 13 of Minnesota Statutes, is a state law that controls how government data is collected, created, stored (maintained), used and released (disseminated). Briefly, the Act regulates:

- What information can be collected.
- Who may see or have copies of the information.
- Classification of specific types of government data.
- Duties of government personnel in administering the provisions of the Act.
- Procedures for access to the information.
- Civil penalties for violation of the Act.
- Charging of fees for copies.

Compliance with the Data Practices Act

The law applies to state agencies in Minnesota, including Minnesota IT Services. State-level entities include the University of Minnesota, Minnesota State Colleges and Universities (MnSCU) and state-level offices, departments, commissions, officers, bureaus, divisions, boards, authorities, districts and agencies.

The Data Practices Act applies to political subdivisions, including counties, cities, school districts, special districts, boards, commissions, districts and authorities created by law, local ordinance or charter provision. Although townships are political subdivisions, the Data Practices Act does not apply to all townships.

Statewide systems are subject to the Data Practices Act. A statewide system is a record keeping or data administering system that is established by federal law, state statute, administrative decision or agreement, or joint powers agreement, and that is common to any combination of state agencies and/or political subdivisions.

Community action agencies organized pursuant to the Economic Opportunity Act of 1964 also are subject to the Data Practices Act. Persons or entities licensed or funded by, or under contract to, a government entity are subject to the Data Practices Act to the extent specified in the licensing, contract or funding agreement.

Contracts

Generally, if MNIT enters into a contract with a person or entity and data is involved, the contracting party shall administer the data consistent with the Data Practices Act. If MNIT enters into a contract with a private person or entity to perform any of its functions, MNIT will include terms in the contract that make it clear that all of the data created, collected, received, stored, used, maintained or disseminated by the private person or entity in performing those functions is subject to the requirements of the Data Practices Act, and that the private person must comply with those requirements as if it were a government entity. The remedies in section 13.08 of the Data Practices Act apply to the private person or entity.

Government Data

Government data is all data kept in any recorded form by government entities in Minnesota. As long as data is recorded in some way by a government entity, it is government data, no matter what physical form it is in, or how it is stored or used. Government data may be stored on paper forms/records/files, in electronic form, on audio or video tape, on charts, maps, etc. Simply put, data is:

- any piece of information,
- collected, created, maintained or disseminated,
- regardless of physical form or storage medium.

It is important to remember that government data is regulated at the level of individual items or elements of data, so that any given document, record or file contains many data elements.

Government data does not include mental impressions of government employees that did not come from recorded data. That is, if a thought only exists in the mind of a government employee, there is no obligation to create data to document that thought in response to a data request. Thus, if the data do not exist or have been properly disposed of, there is still no obligation to create the data from a mental impression in response to a request.

Data Classifications

The Data Practices Act sets out a system of data classification that defines who can access each classification of data. In general, it classifies all government data as public unless a specific state statute (including a provision of the Data Practices Act) or federal law classifies the data as not public. Government entities must determine what types of data they maintain and what data classifications apply to the data. If no law can be identified that classifies the data as not public, then the data is presumed to be public and available to anyone upon request.

There are two types of data: data on individuals (data which an individual is the subject) and data not on

individuals (data about something other than an individual, such as a business).

There are six basic classifications of data under the Data Practices Act:

- Public (data on individuals) – can be disclosed to anyone for any purpose; for example, names and job titles of MNIT employees.
- Private (data on individuals) – can be disclosed only to the subject of the data, to individuals within the government entity whose work assignments reasonably require access to the data, with statutory authority, and with the subject of the data’s permission; for example, names of MNIT employees receiving workers’ compensation benefits.
- Confidential (data on individuals) – cannot even be disclosed to the subject of the data; for example, information involved in the preparation of a pending civil legal action.
- Public (data not on individuals) – can be disclosed to anyone for any purpose; for example, invoices and purchase orders (note that the vendor contract should be reviewed prior to releasing such data).
- Nonpublic (data not on individuals) – can be disclosed only to individuals within the government entity whose work assignments reasonably require access to the data, with statutory authority; for example, certain financial information about businesses.
- Protected Nonpublic (data not on individuals) – available only to government entities with a legal right to know it; for example, state agency legislative and budget proposals until the budget is presented to the Legislature (except preliminary drafts remain nonpublic).

The following table illustrates the Data Practices Act’s data classifications:

Table 1: Data Classifications

Data on Individuals	Meaning of Classification	Data not on Individuals
Public	Data that is available to anyone for any reason.	Public
Private	Data that due to state or federal law is not available to the public but is available to the data subject and those authorized by the data subject. (This data is also available to those whose work assignments require access and other entities authorized by law.)	Nonpublic
Confidential	Data that due to state or federal law is not available to the public or the data subject. (This data is available to those whose work assignments require access and other entities authorized by law.)	Protected Nonpublic

The Data Practices Act classifies many types of government data in sections 13.15 through 13.90. Various sections of Chapter 13 list other Minnesota Statutes that classify government data as not public, or that place restrictions on access to government data.

Using state employees and the work of state agencies, the following are examples of data classifications.

Examples of Employee Information that is Public:

- Name
- Salary
- Value and nature of fringe benefits
- Expense reimbursements
- Education and training
- Existence and status of complaints against employee
- Terms of buy-out agreements
- Final disposition of disciplinary action
- Work location
- Work phone number
- Payroll time sheets
- Employee email address
- Employee identification number

Examples of Other Public Information:

- Certain budget information
- Invoices and purchase orders (note that the vendor contract should be reviewed prior to releasing such data)

Examples of Employee Information that is Private:

- Social Security number
- Birth date
- Home phone number
- Home address
- Health related documents and data in a court file, including administrative courts

Fraud Data

In 2025, the Minnesota Legislature passed new provisions that govern the release of data concerning fraud in public programs. Under the new Minnesota Statutes section 13.357, fraud is defined as “an intentional or deliberate act to deprive another of property or money or to acquire property or money by deception or other unfair means.” The section provides specific acts that are considered fraud about which data may be shared.

The data sharing authorization provides that any government entity may now disclose data “relating to suspected or confirmed fraud in public programs” to any other government entity or federal or law enforcement agency. This data can be shared *regardless of its classification* so long as access to the data would promote the protection of public resources and the integrity of public programs *or* if access to the data would

aid in the law enforcement process. This means that data, even if private or confidential, may be disclosed between government and law enforcement entities if the data relates to actual or suspected fraud so long as the requirements are met.

If we withhold payment for a program participant because of actual or suspected fraud, then data relating to evidence of fraud becomes public at the time that the withholding period ends unless that data is protected as nonpublic under either state or federal law. Note that transferring data between agencies and entities may change the underlying classification of that data depending on how it is classified by the recipient entity.

Role of the Administration

Pursuant to Minnesota Statutes section 13.05, subdivision 4, the Commissioner of the Minnesota Department of Administration is given the authority to approve new uses and dissemination of private and confidential data on individuals. Section 13.06 gives to the commissioner certain powers with regard to approving temporary classifications of data.

Role of the Chief Information Officer

Pursuant to Minnesota Statutes section 16E.01, subdivision 3(a) (7), Minnesota IT Services is required to “facilitate the cooperative development of and ensure compliance with standards and policies for information and telecommunications technology systems and services and electronic data practices and privacy within the executive branch”.

Responsible authority and designated data practices compliance official

The Data Practices Act requires Minnesota government entities to designate the individuals who have official responsibilities under the statute. The following have been designated at Office of Minnesota IT Services (MNIT):

- Responsible Authority
- Data Practices Compliance Official

Responsible Authority

The Responsible Authority is the state official who has administrative authority to carry out the duties of the Data Practices Act. At MNIT, the Responsible Authority is:

Tarek Tomes, Commissioner and Chief Information Officer
200 Centennial Office Building
658 Cedar Street St. Paul, MN 55155

However, please make all requests for data to the Data Practices Compliance Official, shown below.

Data Practices Compliance Official

The Data Practices Compliance Official is a designated person to whom persons should place data requests with. Additionally, persons may direct questions regarding problems in obtaining access to data or other data practices problems. At MNIT, the Data Practices Compliance Official is:

Katie Pauk, MNIT Data Practices Compliance Official
200 Centennial Office Building
658 Cedar Street
St. Paul, MN 55155
Email: Katie.Pauk@state.mn.us.
Phone: 651-802-1771

If you have questions or concerns about a data practices issue or would like to make a request for data, please contact Katie Pauk at the above mailing address, phone number or email address. Please see the following pages for additional information on how to request data.

Procedures to access public data

All government data collected, created, received, maintained or disseminated by a government agency in Minnesota is public unless otherwise classified by law.

The Data Practices Act requires government entities to establish public access procedures to ensure that requests for government data are received and complied with appropriately and promptly.

Requesting Public Data

If you want copies of or access to public data, put your request in writing and direct it to MNIT's Data Practices Compliance Official identified on page 10 of this manual. You may submit your request by email, interoffice mail or regular mail. For your convenience, a data request form is included on page 13. You may use/copy this form and write your request on it.

Requesting Specific Types of Data

You may request specific types of data or data elements, ask for specific documents or portions of documents, and/or ask for entire records, files or data bases. You do not have to give a reason for requesting public data and you do not have to give your name; however, some information may be needed depending on how you pay for copies or if copies are mailed, emailed or faxed. Please clarify when making a request whether you would like to inspect the data, receive copies, or both.

The Data Practices Act does not require us to answer questions that are not requests for data. The Data Practices Act also 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.

What to Say in Your Request

In your request, you should say that you are making a data request under the Data Practices Act. Tell us as clearly as you can what types of data or information you want to inspect or copy. If we are not sure of exactly what information you are requesting, we will ask you to clarify your request.

How We Will Respond to Your Request

If you are not the subject of the data you are requesting, our response will depend on things like how much information you are requesting, what the information is, whether the information is public and how many staff we have available to respond. We will respond within a reasonable time period and if possible within ten

business days. 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 for you 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 and after receiving prepayment (if \$50 or greater). 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 can 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.

If We Do Not Have Data

If we do not have the data you request, we will notify you in writing as soon as reasonably possible. The law does not require us to create data that we do not have.

Possible Costs for Copies of Data – there may be a charge

The Data Practices Act provides that we may charge you for providing copies. Minnesota Statutes section 13.03, subdivision 3, authorizes MNIT to charge a fee to recover our costs to provide copies of data, including (but not limited to) costs associated with searching, compiling, copying, mailing or otherwise shipping the data, as well as a reasonable fee for data with a commercial value. However, the actual costs of providing copies of the data will only be charged when more than 100 pages of copies are requested (if double-sided, both sides are counted). For 100 or fewer copies, MNIT charges 25 cents per page. For more information, please see [MNIT's fee schedule on page 25](#). If the cost is \$50 or greater, MNIT requires prepayment prior to providing the requested copies.

Inspecting Data – no charge

You have the right to inspect (see/look at) all public data at reasonable times and places and at no cost (with the exception of enhanced data, see below). You have a right to inspect public data that we have stored in electronic format. In this case, we may provide you access to a computer terminal so that you can access and view the data. Inspecting may also include remote access by you so that you can download or print copies on your own computer equipment. However, if you request that the data be enhanced, we may charge a fee.

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. Please note that if we have notified you that responsive data that you would like to inspect is available for inspection, and you do not inspect the data within five business days of the notification, we may suspend further response or processing for the request until you inspect the data that has been made available.

Data with Commercial Value – there may be a charge

If you request copies of public data that have commercial value, we may charge you a fee to recover our actual development costs for the data. This would be in addition to the fees outlined in the fee schedule.

Summary Data – there may be a charge

Summary data includes summaries of private or confidential data where no individual is identified. Summary data is public.

You have the right to see and get copies of summary data MNIT has already prepared. An example of summary data would be a statistical record or report such as the number of MNIT employees by race, age and gender.

MNIT may prepare summary data at the request of any person, if the request is in writing and the requestor pays the cost of preparing the data. MNIT requires prepayment of this cost if \$50 or greater.

MNIT will respond to summary data requests within a reasonable amount of time, if possible, ten business days with the data or details of when the data will be ready and how much we will charge.

Please note that MNIT reserves the right to refuse requests to prepare summaries of public data. There is no requirement in the Data Practices Act to create summary data from existing public data.

Denying Access to Data

If the data you request is classified as nonpublic, protected nonpublic, confidential and/or private data on others, MNIT will inform you of this in writing as soon as reasonably possible and tell you which state or federal law classifies the data as nonpublic, protected nonpublic, confidential and/or private.

Access to Other Agencies' Data Under IT Consolidation

Since the creation of the Office of Enterprise Technology (OET) (now Office of Minnesota IT Services or MNIT) in 2005, a number of individual agency technology systems have been consolidated into single enterprise systems managed by MNIT. In addition, in 2011 a new law consolidated and transferred all executive branch state agencies' information technology (IT) service delivery to OET (Laws of Minnesota 2011, First Special Session chapter 10, article 4). The State Chief Information Officer, however, is not the "responsible authority" under the Data Practices Act for other agencies' data residing on MNIT managed technology equipment and thus such requests should not be made to MNIT. Upon receiving such a request, MNIT will inform the requesting party that MNIT is not the responsible authority under the Data Practices Act for responding to the request and provide contact information for the appropriate agency's responsible authority, designee or data practices compliance official.

Sample Data Request Form for Members of the Public

Minnesota IT Services

Instructions: Please complete front and back of this form and submit it to:

Katie Pauk, MNIT Data Practices Compliance Official
200 Centennial Office Building
658 Cedar Street
St. Paul, MN 55155
Email: Katie.Pauk@state.mn.us
Phone 651.802.1771

Note: You do not have to provide any of the contact information below. However, if you want us to mail or email you copies of data, we will need some type of contact information. We may also need some contact information from you depending on how you would like to pay for copies and other costs. If we do not understand your request and need to get clarification from you, without contact information we will not be able to begin processing your request until you contact us.

Date of request:

Name of requestor:

Address 1:

Address 2:

Phone:

Email:

I am requesting access to data in the following way:

Note: inspection is free but MNIT charges for copies when the cost is over \$10.00.

In-person Inspection Paper Copies Electronic Copies Sent via Email

I am requesting the following data pursuant to the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13:

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

Rights of subjects' data

The Data Practices Act establishes specific rights for individuals who are the subjects of government data, and establishes controls on how entities collect, store, use, and release data about individuals. The legislature established these rights and controls because the decisions that government entities make, when using information about those individuals, can have a great effect on their lives.

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

Subject of Government Data

A subject of government data is an individual about whom a government entity stores or maintains data. Such data will be classified as either public, private or confidential.

Summary of Rights of Individuals Who Are the Subjects of Government Data

The Data Practices Act provides you with certain rights (Minnesota Statutes section 13.04). These rights include, but are not limited to the following provisions:

- You have the right to receive a Tennessee warning when a government entity asks you to provide private or confidential data about yourself (see summary on page 23).
- You have the right to know whether a government entity maintains data about you and how they are classified.
- You have the right to view, at no cost, all public and private data maintained about you.
- You have the right to have public and private data explained to you.
- You have the right to receive copies of public data and private data about yourself; however, you may be charged a reasonable fee for copies.
- You have the right not to have private or confidential data about you disclosed to the public unless authorized by law or you give consent to release.
- You have the right to challenge the accuracy and completeness of any public or private data about yourself, appeal a Responsible Authority's determination about your challenge to the Commissioner of Administration, and have an explanation about your disagreement included with the data.

Who May Exercise the Rights of the Individual?

Minnesota Rules, part 1205.0200, subpart 8, defines an individual as a living human being. Pursuant to section 13.02, subdivision 8, of the Data Practices Act, every individual is presumed competent to exercise all of the rights established by the Data Practices Act.

In the case of individuals who are under the age of 18, the Data Practices Act defines “individual” to include a parent or guardian, or someone who is acting as a parent or guardian in the absence of a parent or guardian. This means that a minor is presumed to be competent to exercise her/his rights under the Data Practices Act and so are her/his parent(s) or guardian(s).

A government entity must presume that a parent may exercise the rights of the minor unless the responsible authority is provided with evidence that a court order specifically directs otherwise. Such court orders include those relating to divorce, separation or custody, and the termination of parental rights. Any other legally binding instrument may bar a parent from exercising the minor’s rights.

Controls on the Collection / Storage of Data on Individuals

State government entities may collect and store public, private and/or confidential data on individuals only if necessary to administer/manage a program authorized by state law or local ordinance or mandated by the federal government.

How to Obtain MNIT Information About You

To look at data, or request copies of data that MNIT keeps about you, your minor children, or an individual for whom you have been appointed legal guardian, make a written request. Make your request for data to MNIT’s Data Practices Compliance Official identified on page 10 of this manual. You may make your written request by mail or email, using the data request form on page 18. If you choose to not use the data request form, your written request should include all of the following:

- A statement that you are making a request under the Data Practices Act (Minnesota Statutes, Chapter 13), as a data subject, for data about you.
- An indication of whether you would like to inspect the data, have copies of the data, or both.
- A clear description of the data you would like to inspect or have copied.
- Identifying information that proves you are the data subject or the data subject’s parent/guardian.

Before private data is released to you (the data subject), MNIT requires you to provide identification so that we know you are the individual subject of the data and that we have authority to release it to you. See below for additional information.

Identification Issues

MNIT requires your identity to be authenticated before we can respond to your request for 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.

The following constitute proof of identity:

- An adult individual must provide a valid photo ID, such as a:
 - State driver's license
 - Military ID
 - Passport
 - Minnesota ID
 - Minnesota tribal ID
- A minor individual must provide a valid photo ID, such as a:
 - State driver's license
 - Military ID
 - Passport
 - Minnesota ID
 - Minnesota Tribal ID
 - Minnesota school ID
- The parent or guardian of a minor must provide a valid photo ID and either:
 - A certified copy of the minor's birth certificate or
 - A certified copy of documents that establish the parent or guardian's relationship to the child, such as
 - A court order relating to divorce, separation, custody, foster care
 - A foster care contract
 - An affidavit of parentage
- The legal guardian for an individual must provide a valid photo ID and a certified copy of appropriate documentation of formal or informal appointment as guardian, such as:
 - Court order(s)
 - Valid power of attorney

Note: Individuals who do not exercise their data practices rights in person must provide a notarized letter or certified copy of a valid photo ID. Parents or guardians of a minor must also provide the additional certified copy of the minor's birth certificate or other document, as described above.

Additional Information on Data Subject Requests

For more information related to how we respond to requests, costs/fees, and related issues, please see pages 10-12 and 25-26. When reviewing these pages, please note that unlike public data requests, data subject requests differ in some ways, including, but not limited to:

- They require the requesting party to identify himself/herself (and provide proof of identity).
- They must be responded to by the government entity within 10 business days.
- Data subject requests use only the “actual costs” method for determining fees associated with requests for copies. Actual costs for data subjects do not include search and retrieval costs.

Access to Other Agencies’ Data Under IT Consolidation

Since the creation of the Office of Enterprise Technology (OET) (now Minnesota IT Services or MNIT) in 2005, a number of individual agency technology systems have been consolidated into single enterprise systems managed by MNIT. In addition, in 2011 a new law consolidated and transferred all executive branch state agencies’ information technology (IT) service delivery to OET (Laws of Minnesota 2011, First Special Session chapter 10, article 4). The State Chief Information Officer, however, is not the “responsible authority” under the Data Practices Act for other agencies’ data residing on MNIT managed technology equipment and thus such requests should not be made to MNIT. Upon receiving such a request, MNIT will inform the requesting party that MNIT is not the responsible authority under the Data Practices Act for responding to the request and provide contact information for the appropriate agency’s responsible authority, designee or data practices compliance official.

Sample Data Request Form for Data Subjects

Office of Minnesota IT Services

Instructions: Please complete front and back of this form and submit it to:

Katie Pauk, MNIT Data Practices Compliance Official
200 Centennial Office Building
658 Cedar Street
St. Paul, MN 55155
Email: Katie.Pauk@state.mn.us
Phone: 651-802-1771

Note: To request data as a data subject, you may be asked to authenticate your identity, which may require a notarized letter, a certified copy of a photo ID, or showing us a valid photo ID, such as a driver's license, military ID, or passport. Parents, guardians of minors, and legal guardians of individuals must show additional documentation specified in this manual (see Identification Issues on page 16).

Date of request:

Name of data subject:

Parent/Guardian name (if applicable):

Address 1:

Address 2:

Phone:

Email:

I am requesting access to data in the following way:

Note: inspection is free but MNIT charges for copies when the cost is over \$10.00.

In-person Inspection Paper Copies Electronic Copies Sent via Email

I am requesting the following data pursuant to the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13:

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

For Internal Use Only—MNIT Staff

Verification Identity Authenticated? Yes No

Verified by: Name _____ Signature _____

Further Requests

If you have reviewed data about yourself already, MNIT is not required to show you the data again for six months unless:

- We create or collect more data on you.
- You are challenging the accuracy or completeness of the data or are appealing the results of such a challenge.

Challenging the Accuracy of Data

You have the right to challenge the accuracy and/or completeness of public and private data that MNIT has or maintains about you. If you are a minor, your parent or guardian has the right to challenge data about you. If you believe we have public or private data about you which is inaccurate or incomplete, you can file a data challenge with MNIT. You may challenge only accuracy and completeness of data.

Accurate means the data are reasonably correct and free from error. Complete means that the data describe all of the subject's transactions with the entity in a reasonable way.

To challenge the accuracy and/or completeness of data, you must communicate in writing (letter or email message) to the Responsible Authority and the Data Practices Compliance Official identified on page 9. State that you are challenging the accuracy and/or completeness of data that MNIT maintains about you.

You should identify the specific data being challenged, describe why or how the data is inaccurate or incomplete, and state what you want MNIT to do to make the data accurate or complete. Upon receipt of your challenge, MNIT will review the data. Within 30 business days, we will determine if the data is inaccurate or incomplete. If we agree that challenged data is inaccurate or incomplete, we will make the changes requested and try to notify anyone who has received the data in the past.

If we do not agree that the challenged data is inaccurate or incomplete, we will notify you of this. If we determine that challenged data is accurate and/or complete, and you disagree with us, you have the right to submit a written statement of disagreement to us. The form of your statement of disagreement is of your choosing, and must be included with the disputed data whenever the disputed data is accessed or released. You should send your statement to the Responsible Authority and the Data Practices Compliance Official identified on page 9.

Once the above steps have been exhausted, you have the right to appeal our determination to the Commissioner of the Department of Administration. You must exercise the right to appeal within 60 calendar days of the date we gave you written notice of the right to appeal our determination. If we did not give you written notice of this right, you will have 180 days within which to file an appeal. For more information about filing an appeal, see Minnesota Rules, part 1205.1600. We may provide private data to the Commissioner in order for them to respond to your appeal, and the data maintains the same classification with the Commissioner as when maintained by us. The Commissioner may also disclose private data within the appeal record to the Office of Administrative Hearings.

Granting Access to Others

You can give permission to others to access private data about you by completing and signing an informed consent form. Minnesota Rules 1205.1400, subpart 3, requires that individuals giving informed consent have sufficient mental capacity to understand the consequences of their decision to give consent. Minnesota Rules 1205.1400, subpart 4, requires that a valid informed consent must:

- Be voluntary and not coerced.
- Be in writing.
- Explain why the new use or release is necessary.
- Include any known consequences for giving informed consent.

A sample consent form which meets the above criteria is on the following page.

Additionally, labor organizations and the Public Employment Relations Board have the right to request personnel data (including personnel files) to the extent necessary to conduct elections, investigate and process grievances, and implement the provisions of chapters 179 and 179A. If the request comes from an exclusive representative, the personnel data must be provided regardless of its classification under any other provision of chapter 13.

What is the Connection Between a Tennesen Warning Notice and an Informed Consent?

When a government entity collects private or confidential data from an individual about the individual, such as a photograph of an employee, the entity must give the individual a Tennesen warning notice (Minnesota Statutes section 13.04, subdivision 2). The Tennesen warning notice must include how the entity intends to use the data and which outside entities or persons are authorized to have the data. Once the entity gives the notice, the entity may use or release the data in the ways described in the notice.

After giving a Tennesen warning and collecting private data from an individual, a government entity may wish to use the data differently than it described, or may wish to release the data to an outside entity (government or non-government) or person other than it described. In either of these situations, the government entity would need to obtain informed consent from the individual.

Sample Consent for Release of Information Form

Office of Minnesota IT Services

Instructions: Please complete front and back of this form and submit it to:

Katie Pauk, MNIT Data Practices Compliance Official
200 Centennial Office Building
658 Cedar Street
St. Paul, MN 55155
Email: Katie.Pauk@state.mn.us
Phone: 651.802.1771

Note: Consenting data subjects may be asked to authenticate their identity, which may require a notarized letter, a certified copy of a photo ID, or showing us a valid photo ID, such as a driver's license, military ID, or passport. Parents, guardians of minors, and legal guardians for individuals must show additional documentation specified in this manual (see *Identification Issues* on page 16).

Contact Information

Date of request:

Name of data subject:

Parent/Guardian name (if applicable):

Address 1:

Address 2:

Phone:

Email:

Authorization and Disclosure

Type in your information here:

I, [Click here to enter text](#), authorize [Click here to enter text](#) to disclose the following information about me:

Identify as specifically as possible - the reports, record names or types of data/information or records that will be released to the following individual(s) and/or entities:

Name of individual(s) or entities to receive the data/information: [Click here to enter text](#)

Please send this information to:

Mailing address (Street/City/State/Zip): [Click here to enter text](#)

Email: [Click here to enter text](#)

Fax: [Click here to enter text](#)

Purpose of data/information: [Click here to list any uses for the data/information or restrictions on uses, if any.](#)

I understand that data/information about me is protected private data under the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13, and cannot be disclosed by Minnesota IT Services (f/k/a Office of Enterprise Technology and d/b/a MNIT) without my written consent unless otherwise provided for by state or federal law. I understand that by signing this Consent for Release of Information Form, I am authorizing MNIT to release to the person(s) and/or entities and their representatives' data/information which would otherwise be private and accessible only to me and to MNIT. I understand that although the data/information are classified as private at MNIT, the classification/treatment of the data at [Insert name of other person/entity](#) depends on laws or policies that apply to that other person/entity. I release and forever discharge MNIT and its representatives (e.g., agents, officers, contractors, and employees) from any liability for any damage that may result from furnishing the data/information identified above, including any and all claims and demands arising out of or in connection with the data/information. I also understand that I may revoke this consent at any time and that this consent expires as specified below, or if not specified, within one year of the date of my signature below.

Specific date, event or condition upon which this consent expires, if any: [Select date here.](#) [Click here to describe event or condition.](#)

Data subject authorizing release:

Signature _____ Date _____

Parent/Guardian (if needed):

Signature _____ Date _____

For Internal Use Only—MNIT Staff

Verification Identity Authenticated? Yes No

Verified by: Name _____ Signature _____

The Tennessean Warning Notice

Minnesota Statutes section 13.04, subdivision 2

The notice must be given when:

- An individual
- Is asked to supply
- Private or confidential data
- Concerning self

All four conditions must be present to trigger the notice requirements.

The notice does not need to be given when:

1. Law enforcement officers are investigating a crime.
2. The data subject is not an individual.
3. The subject offers information that has not been requested by the entity.
4. The information requested from the subject is about someone else.
5. The entity requested or received information about the subject from someone else.
6. The information requested from the subject is public data about that subject.

Statements must be included to inform the individual:

1. Why the data are being collected from the individual and how the entity intends to use the data.
2. Whether the individual may refuse or is legally required to supply the data.
3. Any known consequences to the individual of either supplying or refusing to supply the data.
4. The identity of other persons or entities known to be authorized by law to have access to the data (always indicate that the data may be shared upon court order or accessed by the legislative auditor or the state auditor).

Consequence of giving the notice is:

- Private or confidential data on individuals may be collected, stored, used and released as described in the notice without liability to the entity.

Consequences of giving an incomplete notice, or of not giving the notice, are:

- Private or confidential data on individuals cannot be collected, stored, used or released for any purposes other than those stated in the notice unless:
 1. The individual subject of the data gives informed consent.
 2. The Commissioner of Administration gives approval.
 3. A state or federal law subsequently authorized or required the new use or release.

Procedures to limit the collection and use of private or confidential data and data protection

Limitations on Collection and Use of Data

Private or confidential data on an individual shall not be collected, stored, used, or disseminated by MNIT for any purposes other than those stated to the individual at the time of collection in accordance with Minnesota Statutes section 13.04, with some exceptions:

- Data collected prior to August 1, 1975 (prior to the effective date of the Tennessee Warning notice requirement).
- When subsequent laws change the rules regarding the data.
- When the Commissioner of the Minnesota Department of Administration specifically approves.

Data Protection

Under the Data Practices Act, the State Chief Information Officer is required to:

- Establish procedures to assure that all data on individuals is accurate, complete and current for the purposes for which it was collected.
- Establish appropriate security safeguards for all records containing data on individuals.

To comply with these requirements, MNIT has the following:

- A Data Practices Compliance Official.
- This data practices manual.
- Training on data practices and privacy.

In the unfortunate event that MNIT determines a security breach has occurred and an unauthorized person has gained access to your data, we will notify you as required by law.

Fees

As explained on page 11, Minnesota Statutes section 13.03, subdivision 3, authorizes MNIT to charge a fee to recover its costs to provide copies of public data, including (but not limited to) costs associated with searching, compiling, copying, mailing or otherwise shipping the data, as well as a reasonable fee for data with a commercial value.

MNIT does not charge for requests less than \$10.00. If the cost is \$50 or greater, MNIT requires prepayment prior to providing the requested copies.

For 100 or Fewer Paper Copies of Public Data – 25 Cents Per Page

The “actual costs” of providing copies of the data will be charged only when more than 100 pages of copies are requested by a member of the public (if double-sided, both sides are counted). For 100 or fewer pages of black and white, letter or legal-size paper copies, MNIT charges 25 cents for a one-sided copy, or 50 cents for a two-sided copy.

Most Other Types of Copies – Actual Cost

Requests by a member of the public. The charge for most other types of copies (public and private data), 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). More specifically, the following costs may be included, as long as they are reasonable:

- Staff time required to retrieve documents.
- Staff time required to sort and label documents.
- Staff time to remove staples and copy documents.
- Materials (for example, paper, toner, disks, tapes, etc.).
- Special costs associated with making copies of electronic data.
- Mailing costs.

The Data Practices Act does not permit the following costs:

- Administrative costs unrelated to copying.
- Cost for simply inspecting, accessing or viewing data.
- Overhead costs.
- Purchase, maintenance or normal operating expenses of a copier, printer or computer.
- Records storage.
- Sales tax.

- Staff time required to separate public from not public data.
- Staff time required to provide information about the data to the requester (explain content and meaning of data).

The costs for copies of electronic data, for example, are based on the actual cost of, among other things, searching and retrieving the data.

The cost of employee time to search for data, retrieve data, and make copies is based on the lowest paid employee who is able to execute the search and retrieval.

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.

Requests by a data subject. A government entity may charge the actual cost of making copies of data but may not charge for search and retrieval when a request is made by a data subject. The “actual costs” method is used even when there are 100 or less copy pages.