DEPARTMENT OF CORRECTIONS

Policy:	**106.210**
Title:	**Providing Access to and Protecting Government Data**
Effective Date:	**11/19/18**

PURPOSE: To comply with the Minnesota Government Data Practices Act (MGDPA) by maintaining policy and procedures for providing members of the public access to government data kept by the Department of Corrections (DOC) and protecting the rights of subjects of data collected, used, and released by the DOC.

APPLICABILITY: All employees

DEFINITIONS:

Confidential data on individuals – data not made public by statute or federal law applicable to the data and not accessible to the individual subject of the data.

Data breach – the unauthorized acquisition of data maintained by the department that compromises the security and classification of the data. Unauthorized acquisition means a person has obtained, accessed, or viewed data without the informed consent of the data subject or without statutory authority and with the intent to use the data for nongovernmental purposes..

Data not on individuals – data in which no individual is or can be identified as the subject of the data, e.g., statistical records and reports.

Data on individuals – data in which any individual is or can be identified as the subject of the data.

Data practices compliance official – staff person designated by the responsible authority to receive and respond to questions and concerns about data practices problems, including problems in obtaining access to data the DOC keeps.

Data practices designee – any person designated by a responsible authority to be in charge of individual files or systems containing government data and designated to receive and respond to requests for data. For Minnesota Department of Corrections' data practices designees, see Minnesota DOC – Data Practices Designees (attached).

Government data – all data collected, received, created, maintained, or disseminated by a government agency regardless of its physical form, storage media, or conditions of use.

Private data – data that is available only to the subject of the data; or persons authorized to receive the data either by law or by the subject of the data.

Protected not public data – data is not disclosed because disclosure could jeopardize the security of the data.

Public data on individuals – data maintained by the DOC available to anyone for any reason, including, but not limited to, summary data on individuals in which the identities of the individuals is not ascertainable.

Responsible authority – the person ultimately responsible for the collection, use, and dissemination of all agency data and for all data practices decisions, and for compliance with the MGDPA and the rules related to it. For the DOC, this is the commissioner.

PROCEDURES:

A. Designation of Data Practices Responsibilities

1. The director of policy and legal services may designate a data practices compliance official and staff in each facility or work unit as data practices designees.

2. The responsible authority posts annually on the DOC website the list of staff positions designated as the data practices compliance official and data practices designees.

3. All staff persons who collect, access, or respond to requests for data must comply with this policy and, if they are not certain about statutory requirements for collecting, accessing, or releasing data, must contact the data practices designee for their facility or business unit.

B. Collection and Use of Data

The DOC may collect and use data not on individuals for any reason, but it may collect and use data on individuals only when a state or federal law allows or requires doing it. When collecting and using private or confidential data on individuals, the DOC must protect the rights of the subjects of the data to receive effective notice and to have the data used for the purpose it was collected.

1. Right to Notice

Before collecting private or confidential data about employees, offenders, or others, the DOC must provide the individual with notice, sometimes called a "Tennessen" notice.

a) The Tennessen notice must include information about:

(1) why the DOC is collecting the data;

(2) how the DOC plans to use the data;

(3) the law that requires the individual to give the DOC the data and what might happen (consequences) if the individual does not give the data; and

(4) what other people or entities have the legal right to know about, see, or have copies of the data.

b) DOC staff are not required to provide a Tennessen Notice when an individual gives information not requested; the information requested is about someone else; the information is public data about the individual; or the information is being collected by a DOC law enforcement officer investigating a crime.

c) DOC staff must explain anything in the notice if the individual asks for an explanation.

d) A Tennessen Notice should be in writing whenever practical, and receipt of the notice acknowledged in writing by the data subject. The notice need not be in writing or signed to be effective, however. If a data subject declines to acknowledge receipt of the notice in writing, other verification of notice may be used such as written certification by the person presenting the notice. When a Tennessen notice is given over the phone, the DOC staff person who talks to the individual must give the notice orally and give or send a copy in writing for the individual to sign as soon as possible.

2. Use of Data

After a DOC staff person gives an individual notice and the individual provides private or confidential data, the DOC may use the data only in the ways stated in the notice except:

a) if, after the notice is given and the data collected, a federal, state or local law is enacted that authorizes or requires use or release of the data in a different way, the DOC may comply with the new law;

b) if no law has been enacted that authorizes or requires use of the data for the new purpose, and the DOC cannot notify the subject of the data, the DOC may ask the commissioner of the Minnesota Department of Administration to approve the new use and, if the commissioner approves, the DOC may use or release the data in the new way;

c) if it collected private or confidential data about the individual before August 1, 1975, the DOC may use, keep and release the data for the reasons it collected it. It also can ask the commissioner of administration for permission to use, keep or release the data to protect public health, safety or welfare; or

d) if a court orders it to release private or confidential data about the individual, the DOC must release the data. A data practices designee who needs assistance in interpreting the court order should consult with the data practices compliance official.

C. Ensuring Accuracy and Completeness of Data

Individuals who are the subjects of data may challenge the accuracy or completeness of data about themselves.

1. Challenge

A challenge to the accuracy or completeness of data on an individual must be in writing and sent by mail to the DOC's Data Practices Compliance Official, Department of Corrections, 1450 Energy Park Drive, Suite 200, St. Paul, MN 55108; or by fax to 651-603-6770. The written challenge must:

a) State that the individual is challenging the accuracy and completeness of data the DOC maintains about the individual;

b) Identify clearly what data the individual is challenging, for example, make it clear whether the individual is challenging a specific word, sentence, date, time, or name;

c) Explain clearly why or how the data is inaccurate or incomplete;

d) State clearly what the individual thinks should be done to make the data accurate or complete; and

e) Include a mailing address, fax number, or e-mail address to which the response should be sent.

2. Review and Response

Within 30 days, the DOC data practices compliance official must review a challenge to the accuracy of data to decide whether all, some, or none of the data is inaccurate or incomplete, and respond in writing to the individual's challenge.

a) If the DOC data practices compliance official agrees with all or part of the individual's challenge, the DOC data practices compliance official must direct staff

to correct the inaccurate or incomplete data and try to notify anyone who has received the data in the past.

b) If the DOC data practices compliance official does not agree with all or part of the individual's challenge, the DOC data practices compliance official will tell the individual the official believes the data are accurate and complete. When responding to the individual's challenge, the DOC data practices compliance official must tell the individual about the right to appeal the decision within 60 days. If the DOC data practices compliance official does not tell the individual about the right to appeal the decision, the individual has 180 days to file the appeal.

3. Statement of Disagreement or Appeal

If the individual disagrees with the decision on disputed data, the individual may submit a statement of disagreement to the DOC or appeal the DOC's determination to the commissioner of the department of administration.

a) If the individual submits a statement of disagreement with the DOC's determination on the accuracy of the data, the DOC data practices compliance official must direct staff to include the individual's statement of disagreement whenever the disputed data is released to anyone else.

b) The instructions for filing an appeal are posted on the DOC website.

D. Authorized Access to Data

All members of the public, including DOC employees, have the right to inspect, free of charge, any government data the DOC keeps or to receive copies of data if they are authorized to have access to the data and pay the cost for providing it. The DOC publishes on its website information on how members of the public can request access to or copies of data and information explaining the rights of subjects of data. The DOC's data practices designees, under the direction of the data practices compliance officer and responsible authority, determine who is authorized to access data in compliance with the MGDPA.

1. Public Data

All data the DOC has is public unless state or federal law classifies otherwise. Anyone who requests it is authorized to have access to public data.

2. Private Data on Individuals

Only the subject of the data, persons authorized by the subject of the data (if authorization is permitted by law), or persons otherwise authorized by law may have access to private data on individuals.

a) Authorized by Subject of Data

(1) The subject of private data may authorize access to the data by signing and dating a document that identifies the person who is authorized to have access to the data, the data to which the person may have access, and the time period during which the person may have access.

(2) An individual may, but is not required to, use the Release of Information form available on the department's website.

b) Authorized by Law

(1) Employees of the DOC may have access to private data about individuals if it is reasonably necessary for them to perform their assigned duties.

(2) If the subject of the data is deceased, the legal personal representative of the deceased or, if there is no personal representative, the spouse, parent or child of the deceased person may have access to or authorize the release of private data.

(3) If the subject of the data is a juvenile, the parents or guardians of the juvenile may have access to private data on the juvenile unless the juvenile has asked that the data not be shared and it is determined that nondisclosure is in the best interest of the juvenile.

(a) If a minor does not want the DOC to give the minor's parents access to private data, the minor must write to the DOC Data Practices Compliance Official, Policy & Legal Services Unit, 1450 Energy Park Drive, Suite 200, St. Paul, MN 55108. The letter must explain why the minor does not want the DOC to release the information to the minor's parents and must be signed and dated.

(b) In deciding whether to honor the minor's request, the DOC must consider: whether there is a law that requires it to give the data to the minor's parents or guardians; whether the minor has a good reason for asking the DOC not to release the data; whether giving parents or guardians the data would cause the minor to be harmed in any way; whether the minor understands what will happen if the DOC does not release the data; and whether it is in the best interest of the minor for the DOC not to give the data to the parents or guardians.

3. Confidential and Protected Nonpublic Data

Only DOC employees whose work assignments require access or those permitted access by law are authorized to access data on individuals or not on individuals that is made "not public" by state or federal law.

E. <u>Providing Access to Data</u>

1. Requests for Access to Data

Individuals may request access to specific documents, files, records or types of data the DOC keeps, or may request access to the public and private data about the individual the DOC keeps.

a) Individuals must request access to data in writing, either by mailing, emailing, or faxing the request to the appropriate data practices designee during normal office hours (8:30 a.m. – 4:30 p.m. Monday-Friday).

b) Requests that relate to one of DOC's facilities or field services offices should be sent directly to the person listed for that facility or field office on the list of Minnesota Department of Corrections Data Practices Designees available on the DOC website.

c) Individuals making requests for data may, but are not required to, use the Data Practices Request form attached to this policy. Individuals who request data do not have to identify themselves or explain why they want the requested information, but must:

(1) state they are making a data request under the Minnesota Government Data Practices Act (MGDPA);

(2) identify clearly what information they want to see;

(3) respond to questions from the data practices designee or compliance official to help clarify what information is being requested; and
(4) if they are requesting copies of data, provide a fax number, e-mail address, or mailing address to which the requested data may be sent.

2. Referral of Data Practices Requests:

a) When the data practices designee receives a data request from a representative of the media, the designee must promptly inform the communications director about the request and communicate with the media representative through the DOC communications office.

b) When the data practices designee receives a data request related to any pending or active litigation, the data practices designee must promptly refer the request to the facility litigation coordinator or the director of policy and legal services. The director of policy and legal services determines how the request is handled. Subpoenas are not data practices requests and they should be referred to the facility or business unit manager.

c) When the data practices designee receives a data request from a legislator or legislative staff member, the designee must promptly inform the legislative liaison of the request. The data practices designee responds to the request and provides the legislative liaison with a copy of the response.

d) When the data practices designee receives a data request for data held by more than one facility or business unit, he or she must inform the designee for the other involved facility or business unit; and inform the requester that the requester may receive responses from the other facility or business unit.

3. Response to Requests for Data

When a request for data is received, the DOC data practices designees must:

a) Verify the identity of the person, if the person is requesting access to private data;

(1) When the subject of private data requests it, the DOC accepts a state driver's license, a military ID, a passport, a Metricula Consular, a Minnesota ID, or a Minnesota tribal ID as proof of identity. Staff may present an employee identification card/number.

(2) When someone authorized by the subject of the data requests access to private data, the DOC accepts a valid authorization from the subject of the data and a state driver's license, a military ID, a passport, a Metricula Consular, a Minnesota ID, or a Minnesota tribal ID as proof of identity.

(3) When the parent or guardian of a minor who is the subject of data requests access to private data, the DOC accepts a state driver's license, a military ID, a passport, a Metricula Consular, Minnesota ID, or a Minnesota tribal ID as proof of identity; and the minor's birth certificate naming the individual as a parent or a court order designating the individual as legal guardian.

b) Respond to requests for public data immediately, if possible, or as soon as reasonably possible;

c) Respond to requests from subjects of data for public or private data about themselves immediately, if possible, or within 10 working days; and/or

d) Notify the individual who requested the data that the DOC:
   (1) does not have the requested data; or
   (2) has the data and arrange to make it available or deliver it, whenever possible, in electronic form; or
   (3) has the data but not in the form the person who requested it wants but can provide it to them and they can convert it to any other form; or
   (4) has the data, but will need to deliver it in installments as it becomes available; or
   (5) needs more time to identify, retrieve, or copy the requested data and when the data will be available; or
   (6) has the data but the data is not "public" data, identify both the classification of the requested data and the specific law that classifies the data, and explain whether and how the person can get access to the data ; and
   (7) provides an estimate or invoice for whatever costs are incurred to retrieve, duplicate, and deliver the data.

4. Costs for Providing Data

The MGCPA authorizes government agencies to charge for providing data in hard copy or digital format. The DOC data practices designee prepares an invoice for costs based on the statutorily allowed fee structures by requestor. All individuals who request access to data may:

a) Make arrangements to inspect the data, free of charge, at the DOC facility or office that has the data; or

b) Pre-pay to receive the data according to the following:
   (1) If the data subject, pre-pay the costs of providing the data, which includes time for making and certifying copies and materials; or

   (2) If not the data subject, pre-pay per-page or actual costs based on the following:
      (a) Paper copies at $0.25 per single-sided page or $0.50 per double-sided page for 100 or fewer copies (letter/legal size paper); or
      (b) Actual costs for requests exceeding 100 pages or other types of copies (e.g. electronic data, photographs, or other media). Actual costs include:
         - Staff time required to retrieve and copy the data, a task assigned to the lowest salaried employee appropriate to do the work;
         - If the individual asks to have copies faxed, the fee will not include long distance phone charges; and
         - If the individual requests a certified copy of a document, the cost of staff time to certify the document.

5. Providing Access for Review of Private Data

If a person requests the opportunity to review the requested data, the DOC data practices designee must make the data available without charge as soon as possible or within 10 business days.

a) Because the MGDPA requires the DOC to protect private data about the individual, a DOC staff person will be with the individual during inspection of the data.

b) After the individual has inspected the data, the DOC is not required to allow the individual to have access to the data again for six months, unless it collects or creates more information about the individual before six months have passed or the individual has challenged the accuracy of any of the data, or is appealing the results of that challenge.

c) If the individual requesting the data has questions about it, the DOC data practices designee must explain the data in a way the individual can understand.

6. Documentation of Requests for Data
DOC data practices designees will keep a log of all requests for data that includes the date the request was received; the name of the person who requested data, if the person provided a name; what document, if any, was provided to verify the identity of the person requesting the data; a description of the data that was provided; and the date on which it was provided.

F. Protecting the Security of Data
All DOC employees are required to comply with the safeguards for data on individuals and retention practices in compliance with the MGDPA, ACA Standards, and Minnesota Historical Society Guidelines.

1. Employee Access
DOC employees must not access private or confidential data unless access to the data is reasonably required for the employees to perform their assigned duties and are responsible for protecting the security of the data as is appropriate for the classification of the data.

a) Supervisors must approve access to electronic databases or systems that store private or confidential data only if an employee has a current business need for access to the data.

(1) When access to databases containing private or confidential data is requested for a new or reassigned employee, supervisors must sign off on the access form provided by MNIT.

(2) When an employee with access to databases containing private or confidential data separates from employment or vacates a position requiring such access, the supervisor must submit an electronic transaction request to human resources (HR) and HR will notify MNIT of the separation.

(3) When an employee's job duties change such that access is no longer needed, the supervisor must notify MNIT.

b) Copies of approved access requests must be retained electronically or in the employee's supervisory file.

c) DOC employees must take reasonable steps to preserve the security of private or confidential data to which they have access, including, but not limited to:
(1) Locking computers and/or office spaces when unattended;
(2) Disclosing private or confidential data only when authorized to do so;
(3) Storing private or confidential data only on department devices;
(4) Taking the necessary reasonable steps to secure such data or devices from theft, loss, or unauthorized access;

(5) Refraining from downloading software unless approved by the department and MNIT;
(6) Securing all password-enabled devices with a strong password;
(7) Saving all electronic documents important to the department's business on secure, backed-up networks; and
(8) Using secure print/copy functions when making hard copies of data.

2. Consequences for improper access to or use of data
Any employee who is determined to have tampered with or removed any private or confidential data; divulged private or confidential data to unauthorized persons or for unauthorized purposes; or accessed private or confidential data for unauthorized purposes will be subject to disciplinary action and/or referred for prosecution.

3. Determining whether a data breach has occurred
a) A breach in the security of data occurs when a person, who has no reasonable work-related need to access private or confidential data, views or takes the data with **intent** to use it for nongovernmental purposes.

b) Good faith acquisition or access to government data by an employee, contractor, or agent to fulfill job responsibilities is not a breach, even if it results in accidental access to unauthorized data.

c) Following discovery of any potential breach in the security of data, the facility, field office, or business unit data practices designee or other assigned managerial level staff must immediately investigate the likelihood the incident meets the definition of a data breach.

4. Disclosure of a Data Breach
a) If it is determined that a breach has occurred identify anyone whose data may have been improperly disclosed or accessed.

b) Prepare a notice, see Data Breach Notice Template (attached) that includes the following information:
(1) There may have been a breach of (type of data);
(2) That an investigation will be conducted to determine whether there was a breach; and
(3) That a report will be issued after the investigation is complete and how the person may request a copy of the report when it is finished.

Send the notice as soon as possible to each individual by 1st class mail, an electronic notice, or, if sending the notice would cost more than $250,000, post the notice conspicuously on the DOC website and notify major media outlets that reach the Minnesota public.

c) Conduct an investigation and determine the scope of the potential breach, how to restore the security of the data, the number of individuals whose data was actually accessed, whether discipline of an employee (through a separate staff investigation) occurred, the name of each employee determined to be responsible, and the final disposition of any discipline.

d) Write a report that includes all of the information from the investigation listed above; send a copy of the report to any individual who requested it and to the

DOC's chief financial officer, who will determine whether the data was accessed or used for unlawful purposes, and if so, notify the legislative auditor.

G. Inventory of Not Public Data

The DOC data practices compliance official, with the assistance of data practices designees, maintains and updates an inventory of all not public data on individuals currently collected, stored, used, or disseminated by the DOC that identifies the federal or state statute that authorizes the programs or functions for which data or types of data are collected, or that authorizes the actual collection, storage, use, or dissemination of data or types of data. This inventory will be available to members of the general public, upon request

INTERNAL CONTROLS:

Data practices designees and the data practices compliance official:

A. maintain and update the data inventories for their respective facilities, business unit, field districts, or division; and

B. maintain a record of all requests for data received and responses.

ACA STANDARDS: 2-CO-1C-23; 2-CO-1E-01, 2-CO-1E-06 through 2-CO-1E-08, 4-4067, 4-4095, 4-4098, 4-4099, 1-ABC-1C-15, 1-ABC-1E-01, 1-ABC-1E-04, 1-ABC-3E-07, 1-ABC-1E-08, 3-3066, 3-3101, 3-3029, 2-7041, and 2-7070.

REFERENCES: Minn. Stat., Ch. 13
Minn. Rules, Ch. 1205 (Department of Administration Data Practices Rules)

REPLACES: Policy 106.210, "Providing Access to and Protecting Government Data,"7/5/16. All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS: How to Request Public Data (On DOC Public Website)
Request for Government Data (On DOC Public Website)
Release of Information Authorization (On DOC Public Website)
Rights of Data Subjects (On DOC Public Website)
Data Breach Notice template (106.210D)

APPROVALS:

Deputy Commissioner, Facility Services
Deputy Commissioner, Community Services
Assistant Commissioner, Operations Support
Assistant Commissioner, Facility Services