Policy for Ensuring the Security of Not Public Data City of Dayton Effective September 23, 2025 Updated September 2025

Policy for Ensuring the Security of Not Public Data

Legal requirement

The adoption of this policy by the City of Dayton satisfies the requirement in Minnesota Statutes, section 13.05, subd. 5, to establish procedures ensuring appropriate access to non-public data. By incorporating employee access to non-public data in Admin's Data Inventory (required by Minnesota Statutes, section 13.025, subd. 1), in the individual employee's position description, or both, Admin's policy limits access to non-public data to employees whose work assignment reasonably requires access.

Please direct all questions regarding this policy to the City of Dayton's Data Practices Compliance Official (DPCO):

Amy Benting
abenting@daytonmn.gov
12260 S Diamond Lake Road
Dayton, MN 55327

Procedures implementing this policy
Data inventory
Under the requirements in Minnesota Statutes, section 13.025, subd. 1, the City has prepared a Data Inventory which identifies and describes all non-public data on individuals maintained by the City. To comply with the requirement in section 13.05, subd. 5, the City has also modified its Data Inventory to represent the employees who have access to non-public data.
In the event of a temporary duty as assigned by a manager or supervisor, an employee may access certain non-public data, for as long as the work is assigned to the employee.
In addition to the employees listed in the Cities Inventory, the Responsible Authority, the Data Practices Compliance Official (DPCO), may have access to *all* not public data maintained by the City if necessary for specified duties. Any access to non-public data will be strictly limited to the data necessary to complete the work assignment.

Employee position descriptions

Position descriptions may contain provisions identifying any non-public data accessible to the employee when a work assignment reasonably requires access.

Data sharing with authorized entities or individuals

State or federal law may authorize the sharing of non-public data in specific circumstances. Non-public data may be shared with another entity if federal or state law allows or mandates it. Individuals will have notice of any sharing in applicable Tennessen warnings (*see* Minnesota Statutes, section 13.04) or the City will obtain the individual's informed consent. Any sharing of non-public data will be strictly limited to the data necessary or required to comply with the applicable law.

Ensuring that not public data are not accessed without a work assignment

Within Dayton, DCPO may assign tasks by employees or by job classification. If a department maintains not public data that all employees within its department do not have a work assignment allowing access to the data, the department will ensure that the non-public data are secure. This policy also applies to departments that share workspaces with other departments within City where not public data are maintained.

Recommended actions for ensuring appropriate access include:

•Assigning appropriate security roles, limiting access to appropriate shared network drives, and implementing password protections for non-public electronic data

•Password protecting employee computers and locking computers before leaving workstations

•Securing not public data within locked workspaces and in locked file cabinets

•Shredding not public documents before disposing of them

Penalties for unlawfully accessing not public data

City will utilize the penalties for unlawful access to non-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.

CITY OF DAYTON
HENNEPIN AND WRIGHT COUNTIES, MINNESOTA

RESOLUTION 61-2025

A RESOLUTION DESIGNATING THE RESPONSIBLE AUTHORITY, COMPLIANCE OFFICIAL, AND DEPARTMENT DESIGNEES PURSUANT TO THE MINNESOTA GOVERNMENT DATA PRACTICES ACT

WHEREAS, the City of Dayton is a government entity that is subject to the Minnesota Government Data Practices Act, Minn. Stat., Ch. 13 (the "Act"), and related Parts of the Minnesota Rules lawfully promulgated by the Commissioner of Administration to implement the Act; and

WHEREAS, pursuant to Minnesota Statutes § 13.02, subd. 16, the City Council is required to designate an individual as the City's Responsible Authority, who is the person responsible for the collection, use, and dissemination of any set of data on individuals, government data, or summary data by the City, and all other duties and obligations imposed on a Responsible Authority by the Act; and

WHEREAS, pursuant to Minnesota Statutes § 13.05, subd. 13, the City Council or the Responsible Authority is required to designate a City employee to act as the City's Data Practices Compliance Official, who serves as the individual to whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices problems; and

WHEREAS, pursuant to Minnesota Statutes § 13.02, subd. 6, the City Council or the Responsible Authority may identify one or more Designees, who are each a person designated to be in charge of individual files or systems containing government data and to receive and comply with requests for government data.

NOW, THEREFORE, BE IT RESOLVED, by the City Council of the City of Dayton, Minnesota, designates the following individuals:

1. The Responsible Authority for the City of Dayton is:

   City Clerk/Assistant City Administrator Amy Benting
   Dayton City Hall
   12260 South Diamond Lake Road
   Dayton, MN 55327
   abenting@daytonmn.gov
   Phone: 763-427-4589
   Fax: 763-427-3708

2. The Data Practices Compliance Official for the City of Dayton is:

   City Administrator Zach Doud
   Dayton City Hall
   12260 South Diamond Lake Road
   Dayton, MN 55327
   zdoud@daytonmn.gov