Policy for Ensuring the Security of Not Public Data

Legal requirement

The adoption of this policy by the Douglas County Board of Commissioners, on September 16th, 2014, satisfies the requirement in Minnesota Statutes, section13.05, subd. 5, to establish procedures ensuring appropriate access to not public data.

By incorporating employee access to not public data in Douglas County's Data Inventory (required by Minnesota Statutes, section 13.025, subd. 1), in the individual employee's position description, or both, Douglas County's policy limits access to not public data to employees whose work assignment reasonably requires access.

Please direct all questions regarding this policy to the Douglas County Data Practices Compliance Official (DPCO):

Heather Schlangen, Douglas County Coordinator Director
heathers@co.douglas.mn.us
Phone: 320-762-3858
821 Cedar Street
Alexandria, MN 56308

Procedures implementing this policy

Preparation of a Data Inventory

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, Douglas County Department Heads will prepare a Data Inventory which **identifies and describes all not public data on individuals** maintained by each Douglas County Department. To comply with the requirement in section 13.05, subd. 5, Douglas County Department Heads will add to the Data Inventory **the employees who have access to not public data**.

In the event of a temporary duty as assigned by a supervisor, an employee may access certain not public data, for as long as the work is assigned to the employee.

In addition to the employees listed in Douglas County Data Inventory, the Responsible Authority (RA), the Data Practices Compliance Official (DPCO), Department Heads, and the Douglas County General Counsel may have access to all not public data maintained by Douglas County if necessary for specified duties. Any access to not public data will be strictly limited to the data necessary to complete the work assignment.

Employee position descriptions

Position descriptions will contain provisions identifying any not public data accessible to the employee when a work assignment reasonably requires access.

Standard language to be included in job descriptions:

Other duties as assigned section: If a new work assignment requires access to not public data, the incumbent is permitted to access not public data for the work assignment purposes only. Any access to not public data must be strictly limited to the data necessary to complete the work assignment and after the assignment is completed, the employee's work assignment no longer requires access.

Access to Not Public Data
The incumbent may encounter not public data in the course of these duties. Any access to not public data should be strictly limited to accessing the data that are necessary to fulfill the employment responsibility. While data are being accessed, incumbent should take reasonable measures to ensure the not public data are not accessed by individuals without a work reason. Once the work reason to access the data is reasonably finished, incumbent must properly store the not public data according to the provisions Ch. 13.

Data sharing with authorized entities or individuals

State or federal law may authorize the sharing of not public data in specific circumstances. Not public data may be shared with another entity if a 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 Douglas County 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.

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

Within Douglas County, departments may assign tasks by employee 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 not public data are secure. This policy also applies to departments that share workspaces with other departments within Douglas County 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 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.

Penalties for unlawfully accessing not public data
Douglas County 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, referring the matter to the appropriate prosecutorial authority that may pursue a criminal misdemeanor charge.

Updated: 7/17/2019 HS
Reviewed: 7/21/2022 HS