Policy for Ensuring the Security of Not Public Data

Legal requirement

The adoption of this policy by the Department of Administration (Admin) satisfies the requirement in Minnesota Statutes, section 13.05, subd. 5, to establish procedures ensuring appropriate access to not public data. By incorporating employee access to not 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 not public data to employees whose work assignment reasonably requires access.

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

Chris McNulty
chris.mcnulty@state.mn.us
Phone: 651.201.2772
201 Administration Building
50 Sherburne Avenue
St. Paul, MN 55155

Procedures implementing this policy

Data inventory

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, Admin has prepared a Data Inventory which identifies and describes all not public data on individuals maintained by Admin. To comply with the requirement in section 13.05, subd. 5, Admin has also modified its Data Inventory to represent the employees who have access to not public data.

In the event of a temporary duty as assigned by a manager or 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 Admin's Data Inventory, the Responsible Authority, the Data Practices Compliance Official (DPCO), Admin's Senior Leadership Team, and the Agency General Counsel may have access to *all* not public data maintained by Admin 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 may contain provisions identifying any not 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 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 Admin 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 Admin, divisions may assign tasks by employee or by job classification. If a division maintains not public data that all employees within its division do not have a work assignment allowing access to the data, the division will ensure that the not public data are secure. This policy also applies to divisions that share workspaces with other divisions within Admin 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

Admin 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.