STATE OF MINNESOTA
Office of Minnesota Secretary of State
Steve Simon

August 1, 2024

I, Steve Simon, Secretary of State of Minnesota, do hereby approve and adopt the attached policy entitled Policy for Ensuring the Security of Not Public Data as of this date, August 1, 2024, by my signature affixed below.

Steve Simon
Secretary of State

Veterans Service Building, Suite 210 | 20 W 12th Street | Saint Paul, MN 55155
Phone: 651-201-1324 or 1-877-600-8683 | Fax: 651-215-0682 | MN Relay Service: 711
E-mail: secretary.state@state.mn.us | Web site: www.sos.mn.gov

Policy for Ensuring the Security of Not Public Data

Legal requirement

The adoption of this policy by the Office of the Secretary of State (OSS) 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 OSS's Data Inventory (required by Minnesota Statutes, section 13.025, subd. 1), in the individual employee's position description, or both, OSS'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 OSS's Data Practices Compliance Official (DPCO):

Justin R. Erickson
justin.erickson@state.mn.us
Phone: 651.201.6895
Fax: 651.296.9073
Veterans Service Building
20 West 12th Street, Suite 210
St. Paul, MN 55155

Procedures implementing this policy

Data inventory

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, OSS has prepared a Data Inventory which identifies and describes all not public data on individuals maintained by OSS. To comply with the requirement in section 13.05, subd. 5, OSS 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 OSS's Data Inventory, the Responsible Authority, the Data Practices Compliance Official (DPCO), OSS's Senior Leadership Team, the General Counsel and other counsel may have access to *all* not public data maintained by OSS 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 OSS 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

Employees within the divisions of OSS have access to all of the not public data held with respect to that division; the employees within a division have work assignments inherently requiring that they work with all the data of the division. Employees in a division may also be required by assignment to work with data held by other divisions, either because they have been temporarily assigned to do tasks of another division or because their job tasks require contact with the data of other divisions.

Divisions are physically segregated within OSS, and computer systems discretely serving different divisions are also separate modules, with appropriate security.

Penalties for unlawfully accessing not public data

OSS 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.