

# **Winona County Soil and Water Conservation District**

## **Policy for Ensuring the Security of Not Public Data**

### **Legal requirement:**

The adoption of this policy by the Winona County Soil and Water Conservation District (SWCD) 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 SWCD's Data Inventory (required by Minnesota Statutes, section 13.025, subd. 1), in the individual employee's position description, or both, SWCD'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 SWCD's Data Practices Compliance Official (DPCO):

Karin Sonneman  
Winona County Attorney,  
[ksonneman@co.winona.mn.us](mailto:ksonneman@co.winona.mn.us)  
171 West 3<sup>rd</sup> Street  
Winona, Minnesota 55987

### **Procedures implementing this policy:**

#### **Data inventory**

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, the SWCD has prepared a Data Inventory which identifies and describes all not public data on individuals maintained by SWCD. To comply with the requirement in section 13.05, subd. 5, SWCD 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 SWCD's Data Inventory, the Responsible Authority, the Data Practices Compliance Official (DPCO), other staff members may have access to all not public data maintained by SWCD 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 Tennessee warnings (see Minnesota Statutes, section 13.04) or SWCD 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**

SWCD, may assign tasks by employee or by job classification. If the SWCD maintains not public data that all employees within SWCD do not have a work assignment allowing access to the data, the SWCD will ensure that the not public data are secure. This policy also applies to areas of SWCD that share workspaces with other entities 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:**

SWCD 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.

Adopted: July 2020