# CITY OF LAKEVILLE
# Policy for Ensuring the Security of Not Public Data
**August 2019**

## Legal requirement

The adoption of this policy by the City of Lakeville (Lakeville) 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 Lakeville's Data Inventory (required by Minnesota Statutes, section 13.025, subd. 1), in the individual employee's position description, or both, Lakeville'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 City of Lakeville's Responsible Authority and Data Practices Compliance Official:

Ann Orlofsky
aorlofsky@lakevillemn.gov
952-985-4404
20195 Holyoke Avenue
Lakeville, MN 55044

## Procedures implementing this policy

### Data Inventory

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, Lakeville has prepared a Data Inventory which identifies and describes all not public data on individuals maintained by Lakeville. To comply with the requirement in section 13.05, subd. 5, Lakeville 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 Lakeville's Data Inventory, the Responsible Authority, Data Practices Compliance Official, City Administrator, Human Resources Manager and Information Systems Manager may have access to all not public data maintained by Lakeville 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

All employees are required to adhere to Minnesota Statute Chapter 13, the Government Data Practices Act. 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 Lakeville 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 Lakeville, departments 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 not public data are secure. This policy also applies to departments that share work spaces with other departments within Lakeville 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 work stations
- 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**

Lakeville 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, which may pursue a criminal misdemeanor charge.