City of Northfield, Minnesota	Policy Number: 1.07
ADMINISTRATIVE POLICY	Adopted: 10/7/2014 – Motion 2014-187
APPROVE THE POLICY FOR ENSURING THE SECURITY OF NOT PUBLIC DATA	Revised:

City of Northfield
Policy for Ensuring the Security of Not Public Data

Legal requirement

The adoption of this policy by the City of Northfield (City) satisfies the requirement in Minn. Stat. § 13.05, subd. 5, to establish procedures ensuring appropriate access to not public data. By incorporating employee access to not public data into the City's Data Inventory (required by Minn. Stat. § 13.025, subd. 1), in the individual employee's position description, or both, the City'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's Data Practices Compliance Official:

Deb Little, City Clerk
Deb.Little@ci.northfield.mn.us
Phone: 507.645.3001
Fax: 507.645.3055
Northfield City Hall
801 Washington St.
Northfield, MN 55057

Procedures implementing this policy

Data inventory

Under the requirement in Minn. Stat. § 13.025, subd. 1, the City has prepared a Data Inventory, which identifies and describes all not public data on individuals maintained by the City. To comply with the requirement in Minn. Stat. § 13.05, subd. 5, the City will also include in its Data Inventory the position titles of 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 the City's Data Inventory, the Responsible Authority, the Data Practices Compliance Official, the City Administrator, senior management employees, and the City Attorney may have access to all not public data maintained by the City 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 Minn. Stat. § 13.04) or the City 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 the City, departments may assign tasks by employee or by job classification. If a department maintains not public data that all employees within such 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 the City 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

The City will utilize the penalties for unlawful access to not public data as provided for in Minn. Stat. §13.09, if necessary. Penalties include suspension, dismissal, or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge. All City employees should also refer to the City's employee handbook for specific policies related to data, security and related penalties.