CITY OF ROCHESTER
ORGANIZATIONAL POLICY

SECURITY OF NOT-PUBLIC DATA

Purpose

The purpose of this policy is to outline expectations regarding the appropriate access to not-public data by public employees. "Not-public data" is defined as any government data classified by law as confidential, private, non-public, or protected non-public. Common examples of not-public data may include the name of a person who has signed up for a City newsletter, some law enforcement data, and certain personnel data.

City employees are required to sign a Data Practices Policy Acknowledgement Form indicating they have reviewed and understand the contents of this policy. Employee access to not-public data is limited to those individual whose work responsibilities reasonably requires access to the data.

Legal Requirement

The adoption of this policy by the City of Rochester (City) satisfies the requirement in Minnesota Statute §13.05, Subdivision 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 Minnesota Statute §13.025, subd. 1), this policy limits access to not-public data to employees whose work assignment reasonably requires access.

All questions regarding this policy should be directed to the City's Data Practices Compliance Official:

Aaron Reeves, City Clerk, Email: areeves@rochestermn.org
Phone: 507-328-2900, Fax: 507-328-2901
City of Rochester, 201 4th Street SE, Rochester, MN 55904

Data Inventory

A data inventory has been created and maintained by the City which identifies and describes all not-public data on individuals. As part of this inventory, a list of not-public data is maintained along with position titles of employees who have access to this data. In the event a temporary duty is assigned by a supervisor to another employee, that individual may access to certain not-public data, for as long as the work is assigned to the employee.

In addition to the employees listed in the 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.

Data Sharing with Authorized Entities or Individuals

State or federal law may authorize or mandate sharing of not-public data in specific circumstances. Individuals will have notice of information shared in applicable Tennessen Warnings 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 applicable law.

Ensuring Not-public Data Are Not Accessed Without A Work Assignment

Within the City, department supervisors may assign tasks by employee or by job classification. When no employees within a department have work assignments that allow access to specific not-public data, steps will be taken to ensure the security of that data. 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[1]

Employees who violate this policy may be subject to disciplinary action up to and including termination of employment. In addition, violations may be referred to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

Adopted March 2, 2015

[1] The City may utilize the penalties for unlawful access to not public data as provided in Minnesota Statute §13.09.