II. Data Inventory

Policy for Ensuring the Security of Not Public Data

Legal Requirement

The adoption of this policy by the City of Vadnais Heights ("City") 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 the City's Data Inventory (required by Minnesota Statutes, section 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.

Procedures Implementing This Policy

Data Inventory

Under the requirement in Minnesota Statutes, section 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 section 13.05, subd. 5, the City 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 the City's Data Inventory, the Responsible Authority, the Mayor, City Council, and City Attorney, Data Practices Compliance Official (DPCO), 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* Minnesota Statutes, section 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, divisions may assign tasks by employee or by job classification. If a division maintains not public data that all employees within its division do not have a work assignment allowing access to the data, the division will ensure that the not public data are secure. This policy also applies to divisions that share workspaces with other divisions 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 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.

Notice to Individuals; Investigation Report

The City will disclose any breach of the security of the data following discovery or notification of the breach. Written notification will be made to any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person, informing the individual that a report will be prepared under paragraph (b), how the individual may obtain access to the report, and that the individual may request delivery of the report by mail or e-mail. The disclosure will be made in the most

expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement agency; or (2) any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

Upon completion of an investigation into any breach in the security of data and final disposition of any disciplinary action, including exhaustion of all rights of appeal under any applicable collective bargaining agreement, the responsible authority will prepare a report on the facts and results of the investigation. If the breach involves unauthorized access to or acquisition of data by an employee, contractor, or agency of the City, the report will include:

(1) A description of the type of data that were accessed or acquired;

(2) the number of individuals whose data was improperly accessed or acquired;

(3) if there has been final disposition of disciplinary action, the name of each employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing duties under Minn. Stat. Ch. 5B; and

(4) The final disposition of any disciplinary action taken against each employee in response.

Coordination With Consumer Reporting Agencies

If the City discovers circumstances requiring notification under Minn. Stat. § 13.055 of more than 1,000 individuals at one time, the City must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

Security Assessments

At least annually the City will conduct a comprehensive security assessment of any personal information maintained by the City. For the purposes of this subdivision, personal information is defined under Minn. Stat. § 325E.61, subdivision 1, paragraphs (e) and (f).