Policy for Controlling Access to Not Public Data on Individuals by City Employees, Appointed Officials and Elected Officials

Purpose:

While providing services to the public, the City of Owatonna (“City”) frequently receives, creates, or acquires data which is classified by the Minnesota Data Practices Act (*MDPA") as "Not Public Data on Individuals." To protect the security of the subjects of this not public data, the City has adopted this policy governing access to such data.

Applicability:

This policy is applicable to all City employees, all appointed officials including members of Council-created commissions and committees, and any elected officials including State and County elected officials and the City Council. This policy is also applicable to all City vendors and consultants.

Definitions:

"Breach of the security of the data" means unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data. Good faith acquisition of or access to government data by an employee, contractor, or agent of a government entity for the purposes of the entity is not a breach of the security of the data, if the government data is not provided to or viewable by an unauthorized person, or accessed for a purpose not described in the procedures required by Minnesota Statues Section 13.05, subdivision 5. For purposes of this paragraph, data maintained by a government entity includes data maintained by a person under a contract with the government entity that provides for the acquisition of or access to the data by an employee, contractor, or agent of the government entity.

“Data on individuals" means all government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual.

"Individual" means a natural person.

“Not public data” means any government data classified by statute, federal 1aw, or temporary classification as confidential, private, nonpublic, or protected nonpublic.

“Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

(1) Social security number;
(2) Driver’s license number or Minnesota identification card number; or

(3) Account number or credit or debit card number; in combination with any required security code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Unauthorized acquisition" means that a person has obtained, accessed or viewed government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

"Unauthorized person" means any person who accesses government data without a work assignment that reasonably requires access or regardless of the person's work assignment, for a purpose not described in the procedures required by Minnesota Statue Section 13.05, subdivision 5.

Permitted Access to Not Public Data by City Employees and Officials:

Persons employed by the City, any City contactors and consultants, and any appointed or elected officials are permitted access to not public data only while engaged on a work assignment that reasonably requires access to that data.

Types of Not Public Data on Individuals and Anticipated City Employee Access:

See attached Data Inventory table as Exhibit A.

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 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:

When the City Administrator or Department Head assigns a work task to an employee that requires access to not public data on an individual, the City Administrator or Department Head will inform the employee which data are not public and that the data may not be disclosed to anyone else including other City employees.

When the City Administrator or Department Head determines that not public data must be provided to County or State employees or to appointed or elected officials of the City, County or State, the City Administrator or Department Head shall inform the appointed or elected official which data are not public and that the data may not be disclosed to anyone else.

Actions to ensure only appropriate access to not public data include: (1) limiting access to appropriate shared network drives and implementing password protections for not public electronic data; (2) password protect employee and officials' computers and locking computers

before leaving work stations; (3) securing hard copies of not public data in locked cabinets; (4) shredding not public data prior to disposal, and (5) no work related pictures on personal cameras or phones.

Notice of a Breach:

If the City becomes aware of an unauthorized acquisition of not public data, City Staff shall take the following actions:

1. Send a Notice to the 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.
2. The Notice shall be in substantial form as the attached form on Exhibit B and sent via First Class mail or email.
3. The City shall conduct an investigation into any breach in the security of data.
4. After finishing the investigation, the City shall have a report prepared on the facts and results of the investigation. This report shall be made available to the subject of the data by U.S. mail or email.
5. In compliance with Minnesota Statutes Section 13.055 subd. 2(b), the report must include at minimum:
    a. A description of the type of data that were accessed or acquired;
    b. The number of individuals whose data was improperly accessed or acquired;
    c. If an employee has been disciplined for the improper access and there has been a final disposition of that discipline as defined in Minnesota Statutes Section 13.43, the name of the employee responsible for the unauthorized access or acquisition and the final disposition of discipline.
    d. If a contractor or agent of the government entity is responsible for the unauthorized access, whether the City has changed how it does business with that contractor.

Annual Security Assessment:

The City staff shall annually conduct a security assessment of any personal information maintained by the City.

Penalty for Violation of this Policy:

Violation of this policy by a City employee is just cause for suspension without pay or termination. Minnesota Statute Section 13.09 provides that anyone who willfully violates this policy or applicable Minnesota Statutes or whose conduct constitutes the knowing unauthorized acquisition of not public data is guilty of a misdemeanor.