THE CITY OF DULUTH MINNESOTA Policy & Procedure	**DATA ACCESS POLICY – SECURITY OF NOT PUBLIC DATA** **Supercedes:** N/A **Date Approved:** June 13, 2016 **Approved:**	Page 1 of 2

Legal Requirement

The City hereby establishes the following written procedures to ensure appropriate employee access to not public data as required by Minnesota Statutes Sections 13.05, Subdivision 5, and 13.025, Subdivision 1-2 (2015). Access to not public data shall be limited to employees whose work assignment reasonably requires access.

Data Inventory and Access

The City has adopted the Minnesota General Records Retention Schedule for Minnesota Cities (City Council Resolution 12-0437R) ("Retention Schedule" or "Data Inventory"). Access to government data is generally governed by the City Records Management Policy approved December 29, 2014. The Data Inventory generally describes all not public data on individuals maintained by the City. The Data Inventory and Records Management Policy specify type(s) of not public data accessible to employees in each City Department(s). Within each City Department, access to not public data shall be limited to employees whose work assignment(s) reasonably requires access. In addition, job descriptions maintained by the City Human Resources Office may contain provisions identifying additional not public data accessible to certain employees when a work assignment reasonably requires access.

In addition to the employees in the Departments listed in the City's Data Inventory and Records Management Policy, the Responsible Authority (Minnesota Statutes Section 13.02, Subdivision 16), his/her Designee (Minnesota Statutes Section 13.02, Subdivision 6), the Data Practices Compliance Official (Minnesota Statutes Section 13.05, Subdivision 13), the Mayor, the Chief Administrative Officer, and the City Attorney's Office may have access to *all* not public data maintained by the City when reasonably necessary for their duties. However, access to not public data will be strictly limited to the data necessary to complete their duties.

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. 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 is Not Accessed without a Work Assignment

City Department Directors and/or Division Managers may assign tasks by employee or by job classification. If a Department/Division maintains not public data that all employees within that Department/Division do not have a work assignment allowing access to the data, the Department Director and/or Division Manager will ensure that the not public data is secure. This also applies to City Departments/ Divisions that share workspaces with other City Departments/Divisions where not public data are maintained.

Actions for ensuring appropriate access include, but are not limited to:

- 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; and
- Shredding not public documents before disposing of them.

Penalties for Unauthorized Access of Not Public Data

The City will utilize administrative discipline and will report criminal activity to law enforcement officials.