 <p><b>DULUTH</b> MINNESOTA POLICY &amp; PROCEDURE</p>	<p><b>DATA ACCESS POLICY – SECURITY OF NOT PUBLIC DATA</b>  Supersedes: June 13, 2019                      Date Approved: August 1, 2025</p>	
	<p>Approved: <i>Mark Stelly</i></p>	<p>Page 1 of 2</p>

### **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 13.025, 13.03 and 13.05. Access to not public data shall be limited to persons 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 governed by the Minnesota Government Data Practices Act and the City Records Management Policy approved December 29, 2014. The Data Inventory and Records Management Policy specifies 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.


### **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, 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 outside agencies where not public data are maintained.

 <p>POLICY &amp; PROCEDURE</p>	<p>DATA ACCESS POLICY – SECURITY OF NOT PUBLIC DATA Supersedes: June 13, 2019      Date Approved: August 1, 2025</p>	
	<p>Approved: <i>Mark Steley</i></p>	<p>Page 2 of 2</p>

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**

Violations of this policy can subject the person to discipline, up to and including termination. Violation of the Minnesota Government Data Practices Act can subject the person to an action for damages, administrative penalties or criminal charges.