CITY OF VIRGINIA
Data Protection Policy

City of Virginia
Data Protection Policy

The Government Data Practices Act presumes that all government data are public unless a state or federal law says that the data are not public. Data are classified by state law as public, private, or confidential. See below for some examples.

Public data

We must give public data to anyone who asks. It does not matter who is asking for the data or why the person wants the data.

EXAMPLE OF PUBLIC DATA: *Name of an applicant for a City License*

Private data

We cannot give private data to the general public, but the subject may have access to private data when the data is about them. We can share private data with that subject, with someone who has their permission, with our government entity staff who have a work assignment to see the data, and to others as permitted by law or court order.

EXAMPLE OF PRIVATE DATA: *Subscription list for entity's periodic publications*

Confidential data

Confidential data have the most protection. Neither the public nor the subject can get access. We can share confidential data with our government entity staff who have a work assignment to see the data, and to others as permitted by law or court order.

EXAMPLE OF CONFIDENTIAL DATA - *MS 13.41, Subd. 3. Board of Peace Officer Standards and Training active investigative data relating to the investigation of complaints against any licensee*

Accuracy and Currency of Data

- All employees will be requested, and given appropriate forms, to provide updated personal information to the appropriate staff person, which is necessary for tax, insurance, emergency notification, and other personnel purposes. Other people who provide private or confidential information will also be encouraged to provide updated information when appropriate.
- Department heads should periodically review forms used to collect data on individuals to delete items that are not necessary and to clarify items that may be ambiguous.
- All records must be disposed of according to the city's records retention schedule.

Data Safeguards

- Private and confidential information will be stored in files or databases which are not readily accessible to individuals who do not have authorized access and which will be secured during hours when the offices are closed.
- Private and confidential data must be kept only in city offices, except when necessary for city business.
- Only those employees whose job responsibilities require them to have access will be allowed access to files and records that contain private or confidential information. These employees will be instructed to:
    - not discuss, disclose, or otherwise release private or confidential data to city employees whose job responsibilities do not require access to the data,
    - not leave private or confidential data where non-authorized individuals might see it, and
    - shred private or confidential data before discarding.
    - When a contract with an outside party requires access to private or confidential information, the contracting party will be required to use and disseminate the information consistent with the Act. The city may include in a written contract the language contained on the sample contract provision page.

Challenge to Data Accuracy

An individual who is the subject of public or private data may contest the accuracy or completeness of that data maintained by the city. The individual must notify the city's responsible authority in writing describing the nature of the disagreement. Within 30 days, the responsible authority or designee must respond and either:

1. correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual, or
2. notify the individual that the authority believes the data to be correct.

An individual who is dissatisfied with the responsible authority's action may appeal to the Commissioner of the Minnesota Department of Administration, using the contested case procedures under Minnesota Statutes Chapter 14. The responsible authority will correct any data if so ordered by the Commissioner.

Disclosure of Data Breach

If the security and classification of government data held by the City of Virginia are compromised by such a breach by the city or its contractor, the city shall notify the subject of the data upon discovery or notification of the breach, as per Minn. Stat. § 13.055.

Questions about the Data Practices Policies in Virginia

Any questions regarding the City of Virginia's Data Practices Policies and compliance can be directed to the Britt See-Benes, Responsible Authority or the Thomas Butorac, City Attorney at (218) 748-7500.