Minnesota Government Data Practices Act

Guidelines and Procedures

Updated 2022

City of Minnetrista
Data Practices Procedures
Table of Contents

City of Minnetrista
Data Practices Procedures
List of Exhibits

DATA PRACTICES PROCEDURES

1.0 Introduction. These procedures are adopted to comply with the requirements of the Minnesota Government Data Practices Act (the "Act"), specifically Minnesota Statutes (abbreviated herein as "M.S." or "Minn. Stat."), Sections 13.03, Subd. 2 and 13.05, Subd. 5 and 8. It is the intent of the City of Minnetrista ("City") to remain in compliance with the Act. These procedures shall be supplemented by the requirements of the Act as needed and if any procedure contained herein is inconsistent with those requirements, as they may be amended, the specific provisions of the Act shall be controlling.

2.0 Responsible Authority. The City Clerk is the Responsible Authority and Compliance Official responsible for the collection, use and distribution of government data and is accountable for City compliance with the Minnesota Government Data Practices Act. The Responsible Authority has authorized certain other City employees to collect, maintain, disseminate, and otherwise assist in complying with the Act ("Designees"). These Designees are listed on attached Exhibit 1. The Responsible Authority shall provide training to Designees and staff at such times and in such a manner as the designated Responsible Authority determines is appropriate to inform them of their obligations under the Act. The designated Responsible Authority shall also be authorized to amend or supplement the Exhibits attached to these procedures as needed to further the intent of these procedures and the City's compliance with the Act. For the purposes of carrying out these procedures, the term Responsible Authority shall include Designees unless the context in which it is used indicates a different intent.

3.0 Access to Public Data. All information maintained by the City is public unless there is a specific statutory designation which gives it a different classification. Categories of classification are as follows:

Data on Individuals*	**Data on Decedents**	**Data not on Individuals***
M.S. § 13.02, subd. 5	M.S. § 13.10, subd. 1	M.S. § 13.02, subd. 4
Public	**Public**	**Public**
Accessible to anyone	Accessible to anyone	Accessible to anyone
M.S. § 13.02, subd. 15	M.S. § 13.02, subd. 15	M.S. § 13.02, subd. 14
Private	**Private****	**Nonpublic**
Accessible to the data subject; Not accessible to the public	Accessible to the representative of the decedent; Not accessible to the public	Accessible to the data subject; Not accessible to the public
M.S. § 13.02, subd. 12	M.S. § 13.10, subd. 1(b)	M.S. § 13.02, subd. 9
Confidential	**Confidential****	**Protected Nonpublic**
Not accessible to the data subject; Not accessible to the public	Not accessible to the representative of the decedent; Not accessible to the public	Not accessible to the data subject; Not accessible to the public
M.S. § 13.02, subd. 3	M.S. § 13.10, subd. 1(a)	M.S. § 13.02, subd. 13

* "Individual" is defined at Minn. Stat. 13.02, subd. 8. Individual means a living human being. It does not mean any type of entity created by law, such as a corporation.

** Private and confidential data on decedents become public data 10 years after the death of the data subject and 30 years after the creation of the data.

3.1 People Entitled to Access. Any person has the right to inspect or view public data and/or to have an explanation of the meaning of the data. The person does not need to state his or her name or give the reason for the request unless a statute specifically authorizes the City to request such information. The Responsible Authority may ask a person to provide identifying or clarifying information for the sole purpose of facilitating access to the data. Examples of when identifying information may be requested include, but are not limited to, obtaining a mailing address when the person has requested that copies be mailed or requesting identification when copies have been paid for by check. Additionally, any person has the right to obtain a copy of public data except in the case of copyrighted materials in the possession of the City for which the City does not have express written permission to reproduce. (Exhibit 9)

3.1A Copyrighted Documents. Copyrighted public documents may be shown to anyone but shall not be reproduced or photocopied without express written permission from the copyright holder.

3.1A1 The Responsible Authority reserves the right to refuse to provide copies of copyrighted data in accordance with the copyright law of the United

States (Title 17, United States Code) which governs the making of photocopies or other reproductions of copyrighted material.

3.1A2 Public documents created by the City and its officials and employees on behalf of the City do not qualify for copyright protection and shall be available for viewing and reproduction in accordance with the Act. In certain cases, the City may enforce a copyright or acquire a patent for a computer software program or components of a program created by the City. In such cases, the data shall be treated as trade secret information.

3.2. Form of Request. The request for public data may be verbal or written. The Responsible Authority or designee may require a verbal request to be made in writing whenever a written request will assist the Responsible Authority or designee in performing his or her duties. (Exhibit 3).

3.3 Identification of Requesting Party. The Responsible Authority may not require the requesting party to provide identification to view public documents unless contact information is required in order to clarify the request. The Responsible Authority must verify the identity of the requesting party as a person entitled to reproductions when reproductions of copyrighted public data are requested. Identity can be established through personal knowledge, presentation of photo identification, comparison of the data subject's signature on a consent form with the person's signature in City records, or other reasonable means.

3.4 Form of Copies. Where public data is maintained in a computer storage medium, the Responsible Authority shall provide copies of the public data in electronic form upon request, provided a copy can reasonably be made in that form. The Responsible Authority is not required to provide the data in an electronic format or program that is different from the format or program in which the Responsible Authority maintains the data. The Responsible Authority may charge a fee for the actual cost of providing the copy.

3.5 Accessibility of Records. Upon request by an individual, records must be made available within a reasonable time period to persons with disabilities in a manner consistent with state and federal laws prohibiting discrimination against persons with disabilities. Reasonable modifications must be made in any policies, practices and procedures that might otherwise deny equal access to records to individuals with disabilities. This requirement does not apply to (1) technology procured or developed prior to January 1, 2013, unless substantially modified or substantially enhanced after January 1, 2013 or (2) records that cannot be reasonably modified to be accessible without an undue burden as defined in Minnesota Statutes, Section 16E.015, subdivision 4 to the public entity or (3) except as otherwise provided in Minnesota Statutes, Chapter 16E.

3.6 Time Limits. Requests will be received and processed only at Minnetrista City Hall during normal business hours. If copies cannot be made at the time of the request, copies must be supplied as soon as reasonably possible. Whenever possible, the Responsible Authority will immediately allow the requesting person to inspect the public data. When providing an immediate response to the requester, it should not interfere with the City's efficient operations. The Responsible Authority may require that the requesting person make an appointment or return at a later time to inspect or to pick up copies of the

requested data. When public data on individuals is requested by the individual data subject and an immediate response is not possible, the authorized City employee will provide the data within 10 days of the date of the request, excluding Saturdays, Sundays, and legal holidays.

3.7 Fees. Anyone may inspect or view public data for any reason without charge. Fees may be charged only if the requesting person asks for a copy or electronic transmittal of the data. Fees will be charged according to the City's current fee schedule and may not include time necessary to separate public from non-public data. A summary of fees generally associated with data requests is contained in Exhibit 2.

4.0 Access to Private and Confidential Data on Individuals. Information about individual people is classified by law as public, private, or confidential. A list of the private and confidential information maintained by the City is contained in Appendix A.

4.1 People Entitled to Access.

4.1A Public information about an individual may be shown or given to anyone for any reason.

4.1B Private information about an individual may be shown or given to:

4.1B1 The individual, but only once every six months, unless a dispute has arisen, or additional data has been collected or created.

4.1B2 A person who has been given access by the express written consent of the data subject.

4.1B3 People, or another responsible authority, who are authorized access by the federal, state, or local law or court order.

4.1B4 People about whom the individual was advised at the time the data was collected. The identity of those people must be part of the Tennessen warning described below.

4.1B5 People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

4.1C Confidential information may not be given to the subject of the data, but may be given or shown to:

4.1C1 People who are authorized access by federal, state, or local law or court order.

4.1C2 People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

4.2 Form of Request. Any individual may request data verbally or in writing. Data will be released depending on whether or not the City has stored the data requested and whether the data is classified as public, private, or confidential. All requests to see private or confidential information must be made in writing in order to verify identity. The Responsible Authority will provide a form (Exhibit 3) to document the requesting party's identity, the information requested, and the City's response; however, any individual may request data verbally or in writing as long as the request is accompanied by documentation of the requesting party's identity and a detailed description of the information requested.

4.3 Identification of Requesting Party. The Responsible Authority must verify the identity of the requesting party as a person entitled to access when private or confidential data is requested. Identity can be established through personal knowledge, presentation of photo identification, comparison of the data subject's signature on a consent form with the person's signature in City records, or other reasonable means.

4.4 Time Limits. Requests will be received and processed at Minnetrista City Hall only during normal business hours. Access to the data will be provided as soon as is reasonably possible. Data requested by the individual data subject will be provided within ten days of the date of the request, excluding Saturdays, Sundays, and legal holidays if an immediate response is not possible.

4.5 Fees. Fees will be charged in the same manner as for public information and are summarized in Exhibit 2.

4.6 Summary Data. The term "summary data" refers to statistical records and reports derived from data on individuals, but which does not identify an individual by name or reveal any other characteristic that could uniquely identify an individual. Summary data derived from private or confidential data is public. The Responsible Authority will prepare summary data upon request if the request is in writing and the requesting party pays for the cost of preparation. The Responsible Authority must notify the requesting party about the estimated costs and collect these costs before preparing or supplying the summary data. This should be done within 10 days after receiving the request. If the summary data cannot be prepared within 10 days, the Responsible Authority must notify the requester of the anticipated time schedule and the reason for the delay.

Summary data may be prepared by "blacking out" personal identifiers, cutting out portions of the records that contain personal identifiers, creating a spreadsheet, programming computers to delete personal identifiers, or other reasonable means.

The Responsible Authority may ask an outside agency or person to prepare the summary data if: (1) the specific purpose is given in writing; (2) the agency or person agrees not to disclose the private or confidential data; and (3) the Responsible Authority determines that access by this outside agency or person will not compromise the privacy of the private or confidential data. (Exhibit 4)

4.7 Records of Minors and Incapacitated Persons as defined in Minnesota Statutes, Section 524.5-102, subdivision 6. The following applies to private *(*not confidential) data about people under the age of 18 and about those persons who are incapacitated as defined by Minnesota Statutes, Section 524.5-102, subdivision 6.

4.7A Parent / Guardian Access. In addition to minors and incapacitated persons as defined above who may have access to private data, a parent may have access to private information about a minor or incapacitated person. For the purposes of these procedures, a "Parent" shall include guardians and individuals acting as parents or guardians in the absence of parents or guardians. A parent is presumed to have this right unless the minor has requested the Responsible Authority to withhold the data and withholding the data would be in the best interest of the minor, or unless the Responsible Authority has been given evidence that there is a state law, court order, or other legally binding document, that restricts the parent's exercise of this right.

4.7B Notice to Minor and Incapacitated Persons. Before requesting private data from minors or incapacitated persons, City personnel must notify the minors and incapacitated persons that they may request that the information not be given to their parent(s) or guardian(s). (Exhibit 5)

4.7C Denial of Parent or Guardian Access. The Responsible Authority may deny parent or guardian access to private data when the individual requests this denial and the Responsible Authority determines that withholding the data would be in the best interest of the individual. The request from the individual must be in writing, stating the reasons for the request. In determining the best interest of the individual, the Responsible Authority will consider:

4.7C1 Whether the individual is of sufficient age and maturity to explain the reasons and understand the consequences,

4.7C2 Whether denying access may protect the individual from physical or emotional harm,

4.7C3 Whether there are reasonable grounds to support the individual's reasons, and

4.7C4 Whether the data concerns medical, dental, or other health services provided under Minnesota Statutes, Sections 144.341 to 144.347. If so, the data may be released only if failure to inform the parent or guardian would seriously jeopardize the health of the individual. The Responsible Authority may also deny parental access without a request from the minor or incapacitated person under any state or federal laws that allows or requires denial of parental or guardian access.

5.0 Access to Private and Confidential Data on Decedents. Private data on decedents means data which, prior to the death of the data subject, were classified by statute, federal law, or temporary classification as private data. Confidential data means data which, prior to the death of the data subject, were classified by statute, federal law, or temporary classification as confidential data. A list of the private and confidential information maintained by the City is contained in Appendix A. Information about individuals who are deceased will be treated the same as data that is about individuals who are living except that private and confidential data on decedents will become public data ten years after the death of the data subject and 30 years after the creation of

the data in accordance with Minnesota Statutes, Section 13.10, subdivision 2. An individual is presumed dead if either 90 years have elapsed since the creation of the data or 90 years have elapsed since the individual's birth, whichever is earlier, except that an individual is not presumed to be dead if the Responsible Authority has information readily available to it indicating the individual is still living.

5.1 People Entitled to Access.

5.1A Public information about a decedent may be shown or given to anyone.

5.1B Private information about a decedent may be shown or given to:

5.1B1 The representative of the decedent may exercise the rights that the decedent could have exercised as a living individual. A "representative of the decedent" means a personal representative of the estate of the decedent during the period of administration, or if no personal representative has been appointed or after discharge, the surviving spouse, any child of the decedent, or, if there is no surviving spouse or children, the parents of the decedent.

5.1B2 A person who has been given access by the express written consent of the decedent prior to their expiration or by the express written consent of the legal representative of the decedent.

5.1B3 People who are authorized access by the federal, state, or local law or court order.

5.1B4 People about whom the decedent or legal representative was advised at the time the data was collected. The identity of those people must be part of the Tennessen warning described below.

5.1B5 People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

5.1C Confidential information may not be given to the legal representative of the decedent, but may be given or shown to:

5.1C1 People who are authorized access by federal, state, or local law or court order.

5.1C2 People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

5.2 Form of Request. Any individual may request data verbally or in writing. Data will be released depending on whether or not the City has stored the data requested and whether the data is classified as public, private, or confidential. All requests to see private or confidential information must be made in writing in order to verify identity. The Responsible Authority will provide a form (Exhibit 3) to document the requesting party's

identity, the information requested, and the City's response; however, any individual may request data verbally or in writing as long as the request includes documentation of the requesting party's identity and a detailed description of the information requested.

5.3 Identification of Requesting Party. The Responsible Authority must verify the identity of the requesting party as a person entitled to access when private or confidential data is requested. Identity can be established through personal knowledge, presentation of photo identification, comparison of the data subject's signature on a consent form with the person's signature in City records, or other reasonable means.

5.4. Time Limits. Requests will be received and processed at Minnetrista City Hall only during normal business hours. The response must be immediate, if possible, or within 10 business days, if an immediate response is not possible.

5.5 Fees. Fees will be charged in the same manner as for public information and are summarized in Exhibit 2.

5.6 Summary Data. The term summary data refers to statistical records and reports derived from data on individuals, but which does not identify an individual by name or any other characteristic that could uniquely identify an individual. Summary data derived from private or confidential data is public. The Responsible Authority will prepare summary data upon request if the request is in writing and the requesting party pays for the cost of preparation. The Responsible Authority must notify the requesting party about the estimated costs and collect these costs before preparing or supplying the summary data. This should be done within 10 days after receiving the request. If the summary data cannot be prepared within 10 days, the Responsible Authority must notify the requester of the anticipated time schedule and the reason for the delay.

Summary data may be prepared by "blacking out" personal identifiers, cutting out portions of the records that contain personal identifiers, creating a spreadsheet, programming computers to delete personal identifiers, or other reasonable means.

The Responsible Authority may ask an outside agency or person to prepare the summary data if (1) the specific purpose is given in writing (2) the agency or person agrees not to disclose the private or confidential data, and (3) the Responsible Authority determines that access by this outside agency or person will not compromise the privacy of the private or confidential data. (Exhibit 4)

6.0 Access to Data Not On Individuals. Information not about individuals is classified by law as public, nonpublic, and protected nonpublic. Information that is not about individuals will generally be treated the same as data about individuals. Nonpublic and protected nonpublic information, except for security information, becomes public either ten years after it was created by the City or ten years after the data was received or collected by the City unless the Responsible Authority reasonably determines that if the information was made public or made available to the data subject that the harm to the public or the data subject would outweigh the benefit to the public or the data subject.

6.1 People Entitled to Access.

6.1A Public information not about an individual may be shown to anyone. Copyrighted documents will not be reproduced or photocopied without express written permission from the copyright holder.

6.1B Nonpublic information not about an individual may be shown or given to:

6.1B1 An authorized representative of the subject entity of the data, but only once every six months, unless a dispute has arisen, or additional data has been collected.

6.1B2 A person who has been given access by the express written consent of the authorized representative of the entity which is the subject of the data.

6.1B3 People who are authorized access by federal, state, or local law or by court order.

6.1B4 People about whom the legal representative of the subject entity was advised at the time the data was collected. The identity of those people must be part of the Tennessen warning described below.

6.1B5 People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

6.1C Protected Nonpublic information may not be given to the legal representative of the entity, but may be given or shown to:

6.1C1 People who are authorized access by federal, state, or local law or court order.

6.1C2 People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

6.2 Form of Request. Any individual may request data verbally or in writing. Data will be released depending on whether or not the City has stored the data requested and whether the data is classified as public, nonpublic, protected nonpublic or is copyrighted.

All requests to view or receive a reproduction of nonpublic or protected nonpublic information must be made in writing in order to verify identity. All requests to receive a reproduction of copyrighted public, nonpublic or protected nonpublic information must be made in writing in order to determine if the request for copyrighted material qualifies for release under copyright law of the United States (Title 17, United States Code.) The Responsible Authority will provide a form (Exhibit 3) to document the requesting party's identity, the information requested, and the City's response; however, any individual may request data verbally or in writing as long as the request includes documentation of the requesting party's identity and a detailed description of the information requested.

6.3 Identification of Requesting Party. The Responsible Authority must verify the identity of the requesting party as a person entitled to access when non-public or protected nonpublic data is requested. The Responsible Authority must also verify the identity of the requesting party as a person entitled to access when copies of copyrighted private, non-public, or protected nonpublic data is requested. Identity can be established through personal knowledge, presentation of photo identification, comparison of the data subject's signature on a consent form with the person's signature in City records, or other reasonable means.

6.4 Time Limits. Requests will be received and processed at Minnetrista City Hall only during normal business hours. The response must be immediate, if possible, or within 10 business days, if an immediate response is not possible.

6.5 Fees. Fees will be charged in the same manner as for public information and are summarized in Exhibit 2.

6.6 Summary Data. The term summary data refers to statistical records and reports derived from data on individuals, but which does not identify an individual by name or any other characteristic that could uniquely identify an individual. Summary data derived from private or confidential data is public. The Responsible Authority will prepare summary data upon request if the request is in writing and the requesting party pays for the cost of preparation. The Responsible Authority must notify the requesting party about the estimated costs and collect these costs before preparing or supplying the summary data. This should be done within 10 days after receiving the request. If the summary data cannot be prepared within 10 days, the Responsible Authority must notify the requester of the anticipated time schedule and the reason for the delay.

Summary data may be prepared by "blacking out" personal identifiers, cutting out portions of the records that contain personal identifiers, creating a spreadsheet, programming computers to delete personal identifiers, or other reasonable means.

The Responsible Authority may ask an outside agency or person to prepare the summary data if: (1) the specific purpose is given in writing; (2) the agency or person agrees not to disclose the private or confidential data; and (3) the Responsible Authority determines that access by this outside agency or person will not compromise the privacy of the private or confidential data. (Exhibit 4)

7.0 Temporary Classification. If the Responsible Authority determines information not expressly classified by law should be protected, the Responsible Authority may apply to the Commissioner of Administration for permission to classify information as private, confidential, nonpublic, or protected nonpublic for its own use and for the use of other governmental entities on a temporary basis. The application and the classification of the information shall be in accordance with Minnesota Statutes, Section 13.06.

8.0 Denial of Access. If the Responsible Authority determines that the requested data is not accessible to the requesting party, the Responsible Authority must inform the requesting party verbally at the time of the request or in writing as soon after that as possible. The Responsible Authority must give the specific legal authority, including statutory section, for withholding the

data. The Responsible Authority must place a verbal denial in writing upon request. This must also include the specific legal authority for the denial.

9.0 Collection of Data on Individuals. The collection and storage of information about individuals will be limited to that necessary for the administration and management of the programs specifically authorized by the state legislature, City Council, or federal government.

9.1 Tennessen Warning. When an individual is asked to supply private or confidential information about the individual, the City employee requesting the information must give the individual a Tennessen warning.

9.1A This Tennessen warning must contain the following:

9.1A1 The purpose and intended use of the requested data,

9.1A2 Whether the individual may refuse or is legally required to supply the requested data,

9.1A3 Any known consequences from supplying or refusing to supply the information, and

9.1A4 The identity of other persons or entities authorized by state or federal law to receive the data.

9.1B A Tennessen warning is not required when:

9.1B1 An individual is requested to supply investigative data to a law enforcement officer;

9.1B2 The data subject is not an individual (e.g., the data subject is a corporation or partnership);

9.1B3 The data subject offer information that has not been requested by the City;

9.1B4 The information requested from the individual is about someone else;

9.1B5 The City receives information about the subject from someone else; or

9.1B6 The information requested from the subject is classified as public data.

9.1C A Tennessen warning may be on a separate form (Exhibit 9) or may be incorporated into the form which requests the private or confidential data.

9.1D Collection of Data on Individuals through the Use of the City's Computer. When an individual gains access to government information or services through the City's computer, the City may create, collect, or maintain electronic access data or use its computer to install a cookie on an individual's computer. The City must inform individuals gaining access to the City's computer

of the creation, collection, or maintenance of electronic access data or the City's use of cookies before requiring the individual to provide any data about the individual to the City. As part of that notice, the City must inform the individual how the data will be used and disseminated. Notwithstanding an individual's refusal to accept a cookie on their computer, the City must allow the individual to gain access to data or information, transfer data or information, or use government services by means of the City's computer. The provisions of this section do not apply to a cookie temporarily installed by the City on a person's computer during a single session on or visit to the City's web site if the cookie is installed only in a computer's memory and is deleted from the memory when the web site browser or application is closed.

9.2 Data Quality Procedures. The City is required to establish procedures to ensure that data on individuals are accurate, complete, and current. The Responsible Authority shall work with employees that collect, use, or disseminate data on individuals to implement the following procedures:

9.2A At the time that data is collected from the individual data subject, the individual should be advised of his or her right to review and contest the accuracy or completeness of public or private data concerning him/herself.

9.2B An individual data subject should be encouraged to review his/her file for accuracy, completeness, and currency.

9.2C Whenever possible and practical, collect data about an individual from the individual subject of the data rather than from third parties (e.g., birthdate, address, etc.). (This directive does not prohibit employees from collecting data from third parties.)

9.2D Design forms to collect objective types of data elements whenever possible, rather than data which calls for an opinion or conclusion or other subjective entry. Forms for the collection of data on individuals should request only necessary data.

9.2E Department heads should periodically review forms used to collect data on individuals. Data elements that are not necessary or that lend themselves to ambiguity or subjectivity should be removed and the forms redesigned.

9.2F Department heads should periodically conduct quality/validity checks on sample case files that contain data on individuals.

10.0 Data Accuracy and Completeness.

10.1 Challenge to Data Accuracy or Completeness. An individual who is the subject of public or private data may contest the accuracy or completeness of that data maintained by the City of which they are the subject. "Accurate" means the data are reasonably correct and free from error. "Complete" means the data describe all of the subject's transactions with the City in a reasonable way.

To challenge the accuracy or completeness of data, the individual must notify the City's Responsible Authority in writing describing the nature of the disagreement. The statement should describe why or how the data are inaccurate or incomplete and should also state what the individual wants the City to do to make the data accurate or complete. 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 Responsible Authority believes the data to be correct. Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data. The Responsible Authority should provide the data subject with a written statement that informs the data subject of the right to appeal and should also provide a copy of Minnesota Rules, Part 1205.1600.

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

10.2 Challenge to Data Accuracy or Completeness. All City employees will be requested, and given appropriate forms, to annually provide updated personal information to the Responsible Authority, as necessary for tax, insurance, emergency notification, and other personnel purposes. Other individuals who provide private or confidential information will also be encouraged to provide updated information when appropriate.

10.3 Review. City department managers 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.

11.0 Policy for Ensuring the Security of Not Public Data.

11.1 Legal Requirement. The adoption of this Section by the City satisfies the requirement in Minnesota Statutes, Section 13.05, subdivision 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 in the individual employee's position description, or both, the City's policy limits access to not public data to employees whose work assignment require reasonable access. Please direct all questions regarding this Section to the Responsible Authority.

11.2 Data Inventory. Under the requirement in Minnesota Statutes, Section 13.025, subdivision 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 set forth in Minnesota Statutes, Section 13.05, subdivision 5, the City has also modified its Data Inventory to represent the employees who have access to not public data.

11.3 Data Safeguards.

11.3A Not public data will be stored by the City in files or databases which are not readily accessible to individuals who do not have authorized access and will be secured during hours when the offices are closed.

11.3B Not public data must be kept only in City offices, except when necessary for City business.

11.3C The City will assign appropriate security roles to its employees, limit employee access to appropriate shared network drives and implement password protections for not public electronic data.

11.3D Only those City employees whose job responsibilities require them to have access will be allowed access to City files and records that contain not public data. Employee position descriptions will contain provisions identifying any not public data accessible to the employee when a work assignment reasonably requires access. If a City employee does not have a work assignment allowing access to the not public data, the City will ensure that the not public data are secure. The City's employees will be instructed to:

11.3D1 Release or disclose not public data only to those persons, within and outside of the City, who are authorized by law to have access to the data;

11.3D2 Not leave not public data where unauthorized individuals might see it;

11.3D3 Password protect their computers and lock their computers before leaving work stations;

11.3D4 Secure not public data within locked work spaces and in locked file cabinets; and

11.3D5 Shred not public data before disposing of them.

In the event of a temporary duty assigned to a City employee, the employee may access certain not public data for as long as the work is assigned to the employee.

11.4 Data Sharing with Authorized Entities or Individuals.

11.4A When a contract with an outside party requires access to not public data, the contracting party will be required to use and disseminate the information consistent with the Act. The City must include in a written contract the language contained in Exhibit 10 or substantially similar language.

11.4B In addition to the employees listed in the City's data inventory (see Appendix A), the Responsible Authority, the City's criminal prosecutor, the City Attorney, the City Engineer, and the City Building Inspector 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.

11.4C 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 it 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.

11.5 Penalties for Unlawfully Accessing Not Public Data. The City will utilize penalties for unlawful access by its employees 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.

EXHIBIT 1

LIST OF DESIGNEES

The Minnesota Government Data Practices Act establishes a system for compilation and distribution of data gathered by government agencies. All data collected and maintained by the City of Minnetrista ("City") is presumed public and is accessible to the public for both inspection and copying, unless classified as Private, Confidential, Nonpublic or Protected Nonpublic in accordance with Federal law, State Statute, or a temporary classification.

The City of Minnetrista has appointed the following position to administer this system.

Responsible Authority and Compliance Official:

Dawn Motzko
City Clerk
City of Minnetrista
7701 County Road 110 W
Minnetrista, MN 55364
(952) 241-2518
dmotzko@ci.minnetrista.mn.us

Positions appointed as designees in system administration are as follows

Allie Polsfuss
Director of Administration
City of Minnetrista
7701 Co. Rd. 110 W
Minnetrista, MN 55364
(952) 241-2510
apolsfuss@ci.minnetrista.mn.us

Paul Falls
Director of Public Safety
City of Minnetrista
7651 County Road 110 W
Minnetrista, MN 55364
(952) 241-2554
pfalls@ci.minnetrista.mn.us

Other persons responsible for the maintenance and dissemination of City records are as apparent or assigned.

EXHIBIT 2

Copy Costs

100 or fewer black and white paper copies, letter or legal size – one-sided	25 cents per page
100 or fewer black and white paper copies letter legal size – two-sided	50 cents per page
Over 100 pages of photocopies	Actual cost*
Electronic copies	Actual cost*
All other types of copies	Actual cost*

* the "actual cost" means the cost of any media (paper, CD ROMs, DVDs, cassette tapes, etc.), mailing costs, employee time to prepare copies[1], costs of reproduction that cannot be done by the City (such as microfilm duplication, oversized photocopies, certain color photocopies, etc.), and employee time to search for and retrieve data for copying (but if the requestor is the data subject, search and retrieval time will not be charged).

"Actual cost" does not include: employee time spent to separate public from not public data; operating expenses of the copier (such as electricity, wear, and tear, etc.); costs not related to copying such as preparing a cover letter or invoice; returning data to off-site storage; sorting, retrieving, or verifying accuracy if not necessary for copying; sales tax; accounting functions; and costs related to inspection.

[1] Employee time will be calculated based on the wages/salary (including benefits) of the lowest-paid City employee who is able to complete the task.

EXHIBIT 3

Minnesota Government Data Practices Act

DATA REQUEST FORM

A. To be Completed by Requester (Please Print)

Name (Last, First, MI) Email Address

Street Address Phone Number

City, State, Zip

Signature Date

Detailed description of the information requested: (Include complete addresses, names, and dates whenever possible. Attach additional sheets if necessary.)

_____

_____

_____

B. Completed by the City of Minnetrista Handled by:_____

Information classified as:
Public ❑ Non-Public ❑ Private ❑ Protected Non-Public ❑ Confidential ❑ Copyrighted ❑

Action:
❑ Approved ❑ Approved in part (Explain Below) ❑ Denied (Explain Below)

Remarks or basis for denial including Minnesota Statute:

_____

_____

_____

Charges:
❑ None
❑ Photocopy:
_____ Pages x _____ cents = _____
❑ Special Rate: _____
Explanation _____
❑ Other: _____
Explanation _____

Identity Verified for Private Information:
❑ Identification: Driver's License, Etc.
❑ Comparison with Signature on File
❑ Personal Knowledge
❑ Other _____

Authorized Signature: _____ Date: _____

EXHIBIT 4

GOVERNMENT DATA ACCESS AND NONDISCLOSURE AGREEMENT

1. **AUTHORIZATION.** The City of Minnetrista (the "City") hereby authorizes _____, (the "Authorized Party") access to the following government data: _____
_____

2. **PURPOSE.** Access to this government data is limited to the objective of creating summary data for the following purpose:
_____
_____

3. **COST.** (Check all that apply):

___ The Authorized Party has been requested by the City to prepare summary data and will be paid in accordance with City policy. The estimated total is: $_____

_____ is the person who requested the summary data and agrees to bear the City's costs associated with the preparation of the data which has been estimated to be $_____.

_____
Signature of Requestor Date

4. **SECURITY.** The Authorized Party agrees that it and any employees or agents under its control must protect the privacy interests of individual data subjects in accordance with the terms of this Agreement. The Authorized Party agrees to remove all unique personal identifiers which could be used to identify any individual from data classified by state or federal law as not public which is obtained from City records and incorporated into reports, summaries, compilations, articles, or any document or series of documents.

Data contained in files, records, microfilm, or other storage media maintained by the City are the City's property and are not to leave the City's custody. The Authorized Party agrees not to make reproductions of any data or remove any data from the site where it is provided, if the data can in any way identify an individual. No data which is not public, and which is irrelevant to the purpose stated above will ever be disclosed or communicated to anyone by any means.

The Authorized Party warrants that the following named individual(s) will be the only person(s) to participate in the collection of the data described above:

Complete name (printed) Title (printed)

5. **LIABILITY FOR DISCLOSURE.** The Authorized Party is liable for any unlawful use or disclosure of government data collected, used, and maintained in the exercise of this agreement and is classified as not public under state or federal law. The Authorized Party understands that it may be subject to civil or criminal penalties under those laws. The Authorized Party agrees to defend, indemnify, and hold the City, its officials, and employees harmless from any liability, claims, damages, costs, judgments, or expenses, omission of the Authorized Party's failure to fully perform in any respect all obligations under this Agreement.

6. **INSURANCE.** In order to protect itself as well as the City, the Authorized Party agrees at all times during the term of this Agreement to maintain insurance covering the Authorized Party's activities under this Agreement. The insurance will cover $1,500,000 per claimant for personal injuries and/or damages and $1,500,000 per occurrence. The policy must cover the indemnification obligation specified above.

7. **ACCESS PERIOD.** The Authorized Party may have access to the information described above from _____ to _____.

8. **ACCESS RESULTS.** A copy of all reports, summaries, compilations, articles, publications, or any document or series of documents that are created from the information provided under this Agreement must be provided to the City. The Authorized Party may retain one copy of the summary data created for its own records but may not disclose it without City permission, except in defense of claims brought against it.

AUTHORIZED PARTY:_____

By:_____ Date: _____

Title (if applicable): _____

REQUESTOR OF SUMMARY DATA:_____

By: _____ Date: _____

Title (if applicable): _____

CITY OF MINNETRISTA:

By: _____ Date: _____

Its: _____

EXHIBIT 5

NOTICE TO PERSONS UNDER AGE 18

Some of the information you are asked to provide is classified as private under State law. You have the right to request that some or all of the information not be given to one or both of your parents/legal guardians. Please complete the form below if you wish to have information withheld.

Your request does not automatically mean that the information will be withheld. State law requires the City to determine if honoring the request would be in your best interest. The City is required to consider:

* Whether you are of sufficient age and maturity to explain the reasons and understand the consequences,

* Whether denying access may protect you from physical or emotional harm,

* Whether there are reasonable grounds to support your reasons, and

* Whether the data concerns medical, dental, or other health service provided under Minnesota Statutes, Sections 144.341 to 144.347. If so, the data may be released only if failure to inform the parent would seriously jeopardize your health.

NOTICE GIVEN TO:_____

DATE:_____

BY:

_____

(name) (title)

REQUEST TO WITHHOLD INFORMATION

I request that the following information:

_____

_____

be withheld from: _____

For these reasons:

_____

_____

_____

Date:_____ Print name: _____

Signature: _____

EXHIBIT 6

CONSENT TO RELEASE PRIVATE DATA

I, _____, authorize the City of Minnetrista ("City") to release
(Print name)

the following private data about me:

_____

_____

to the following person(s) or entity (ies):

_____

_____

The person(s) or entity (ies) receiving the private data may use it only for the following purpose or purposes:

_____

_____

This authorization is dated_____and expires on_____.

I understand that my records are protected under state privacy regulations and cannot be disclosed without my written consent unless otherwise provided for by law. I also understand that I may cancel this consent at any time prior to the information being released and that in any event this consent automatically expires 90 days after signing. By signing this document, I give my full and voluntary consent to the City to release the above-listed data to the persons identified in this release, and I waive any and all claims against the City for the disclosure of private data about me in accordance with this document.

_____
Signature

_____
Signature of parent or guardian
(if data subject is under 18 years of age)

IDENTITY VERIFIED BY:

- ☐ **Witness: x_____**
- ☐ **Identification: Driver's License, State ID, Passport, other:_____**
- ☐ **Comparison with signature on file**
- ☐ **Other:_____**

Responsible Authority/Designee: _____

EXHIBIT 7

CONSENT TO RELEASE COPYRIGHTED DATA

I, _____, certify that I have the authority to authorize the City of Minnetrista to release the following copyrighted data of which I am the copyright holder:

_____

_____

To the following person or people:

_____

_____

The person or people receiving the copyrighted data may use it only for the following purpose or purposes:_____

This authorization is dated _____ and expires on _____.
**The expiration cannot exceed one year from the date of the authorization.*

I, the undersigned, agree to give up and waive all claims that I might have against the City, its agents, and employees for releasing data pursuant to this request.

_____

Printed Name Title

_____

Complete Address Phone

_____

Notarized Signature Date

STATE OF MINNESOTA)
) ss.
COUNTY OF_____)

On this _____ day of _____, 20_____, before me, a Notary Public within and for said County, personally appeared _____, known to me to be the person described in and who executed the foregoing instrument and acknowledged that they executed the same as their free act and deed.

_____

Notary Public

My Commission Expires On: _____

EXHIBIT 8

SAMPLE DATA PRACTICES ADVISORY

(Tennessen Warning)

Some or all of the information that you are asked to provide on the attached form is classified by State law as either private or confidential. Private data is information that generally cannot be given to the public but can be given to the subject of the data. Confidential data is information that generally cannot be given to either the public or the subject of the data.

Our purpose and intended use of this information is:

_____

_____

You ___ are/ ___ are not legally required to provide this information.

If you refuse to supply the information, the following may happen:

_____

_____

_____

Other persons or entities authorized by law to receive this information are:

_____

_____

_____

_____

EXHIBIT 9

City of Minnetrista
Tennessen Warning Form

It is the City of Minnetrista's responsibility to inform potential employees of their privacy rights. Please carefully read the Tennessen Warning provided below. Sign and date the form and return it with your application. Your signature indicates that you have received information regarding your rights as they pertain to the Minnesota Government Data Practices Act.

In accordance with the Minnesota Government Data Practices Act, the City of Minnetrista is required to inform you of your rights as they relate to the private information collected from you. Private data is information that is available to you, but not to the public. Minnesota Statutes, Sections 13.04 and 13.43 are two statutes that govern what affects you as an applicant for employment at the City of Minnetrista. All data collected by the City in relation to your employment application is considered private except for the following:

1. Your veteran's status;
2. Relevant test scores;
3. Your job history;
4. Your education and training; and
5. Your work availability

Your name is considered to be private information; however, if you are selected to be interviewed as a finalist, your name becomes public information.

The data supplied by you may be used for such other purposes as may be determined to be necessary in the administration of personnel policies, rules, and regulations of the City of Minnetrista. Furnishing social security numbers is voluntary for applicants to the City of Minnetrista, but refusal to supply other requested information would mean that your application for employment might not be considered.

Private data is available only to you, to appropriate city employees, and others as provided by state and federal laws who have a bona fide need for the data. Public data is available to anyone requesting it and consists of all data furnished in the application for employment that is not designated in this notice as private data.

The information you give about yourself is needed to identify you and to assist the City of Minnetrista in determining your suitability for the position for which you are applying.

I have read and understand the information given above regarding the Minnesota Government Data Practices Act.

_____ _____

Applicant Signature Date

EXHIBIT 10

SAMPLE CONTRACT PROVISION

Data Practices Compliance. Contractor will have access to data collected or maintained by the City to the extent necessary to perform Contractor's obligation under this contract. Contractor acknowledges that, pursuant to Minnesota Statutes, Section 13.05, subdivision 11, all of the data created, collected, received, stored, used, maintained, or disseminated by Contractor in performing the contract are subject to the requirements of the Minnesota Government Data Practices Act (the "Act"), Minnesota Statutes, Chapter 13. Contractor is required to comply with the requirements of the Act as if it were a government entity. Contractor acknowledges that the remedies provided in Minnesota Statutes, Section 13.08 apply to Contractor with respect to such data. Contractor will notify the City of all requests for data that Contractor receives. Contractor agrees to defend and indemnify the City from any claim, liability, or damage that result from Contractor's violation of the Act or this section of the contract. Upon termination of this contract, Contractor agrees to return data to the City as requested by the City. The obligations of this section of the contract, including the obligation to defend and indemnify the City, shall survive the termination of this Contract, and shall continue so long as the data exists.

EXHIBIT 11

Building Permit/Plans
DATA PRACTICES ADVISORY

You may be required to submit building plans with your building permit application so that the City of Minnetrista can determine whether or not your building permit application should be approved. If you do not submit plans when they are required, your building permit will not be approved. The Minnesota Government Data Practices Act establishes a presumption that all government data are public and are accessible by the public for both inspection and copying unless there is a federal law, a state statute, or a temporary classification of data that provides that certain data are not public. Minnesota Statutes, Section 13.01 defines "government data" as being all data collected, created, received, maintained, or disseminated by the City.

The Government Data Practices Act allows building plans to be classified as nonpublic ONLY if they contain the following information:

> Security information defined by Minnesota Statutes, Section 13.37 as being "government data the disclosure of which the responsible authority determines would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury."
>
> AND / OR
>
> Trade Secret information defined by Minnesota Statutes, Section 13.37 as being "government data, including a formula, pattern, compilation, program, device, method, technique or process (1) that was supplied by the affected individual or organization, (2) that is the subject of efforts by the individual or organization that are reasonable under the circumstances to maintain its secrecy, and (3) that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use."

Building plans submitted to the City are generally public information. If the plans are copyrighted, they will be made available for viewing by the public but will not be allowed to be copied unless a release is obtained by the City from the copyright holder. If you believe that your building plans qualify for the classification of nonpublic data as described above, you must provide documentation verifying your claim. The Responsible Authority for the City of Minnetrista will determine whether the plans qualify for nonpublic data classification within 10 business days of the request. If you do not agree with the determination of the Responsible Authority, you may file an application for a temporary classification of nonpublic data with the Commissioner of Administration.

Building plans and related documents submitted to the City are presumed to be public and by submitting them to the City and by signing this document you are expressly giving permission to the City to make copies for the City's use and to make available to the public upon request unless you indicate otherwise as follows:

_____ The building plans I have submitted are **COPYRIGHTED** under and protected by the Federal Copyright Act and I do not give permission for them to be copied for release to the public. However, I understand the plans are considered public information under Minnesota law and may be viewed by the public.

_____ The building plans I have submitted contain **TRADE SECRET INFORMATION** as defined by Minn. Stat. § 13.37, subd. 1 (a) and are to be treated as protected nonpublic data. I understand I must provide an explanation (below) to support my claim that the information I am providing constitutes trade secret information under law.

_____ The building plans I have submitted contain **SECURITY INFORMATION** as defined by Minn. Stat. § 13.37, subd. 1 (a) and are to be treated as protected nonpublic data. I understand I must provide an explanation (below) to support my claim that the information I am providing constitutes security information under law.

Explanation:

_____
_____
_____
_____
_____

_____	_____
Name of Applicant (Please Print)	Date
_____	_____
Signature of Applicant	Property address
_____	_____
Contact Address	Contact phone
_____	
Email address	

APPENDIX A

NONPUBLIC, PRIVATE & CONFIDENTIAL DATA MAINTAINED BY THE CITY OF MINNETRISTA

This list of data types is divided into the following categories: General, Administration, Community and Real Property, Personnel, and Public Safety. The categories are provided only for convenience in locating types of data; inclusion in any particular category is not intended to indicate an exclusive location for that data type. (For example, data listed under Personnel may be physically located in more than one City department.)

GENERAL

Applications for Election or Appointment
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.601, subd. 3
DESCRIPTION OF DATA: Data on applicants collected by the City from the applicant's application is private, except the following is public: name, city of residence, education and training, employment history, volunteer work, awards and honors, and prior government service or experience. Once appointed, the following is public: residential address and either telephone number or email where the appointee may be reached, or both at the request of the appointee.

Audit Data (provided by State Auditor)
CLASSIFICATION(S): Protected Nonpublic/Confidential
GOVERNING STATUTE: Minn. Stat. § 6.715, subd. 5
DESCRIPTION OF DATA: Data relating to an audit, examination or investigation performed by the State Auditor. Data provided by the State Auditor for purpose of review and verification must be protected from unlawful disclosure.

Business Data
CLASSIFICATION(S): Private/Nonpublic/Public
GOVERNING STATUTE: Minn. Stat. § 13.591
DESCRIPTION OF DATA: Data submitted to the City by a business requesting financial assistance or benefits financed by public funds are private or nonpublic data. The data becomes public when public financial assistance is provided or the business receives a benefit from the City, except that business plans, income and expense projections not related to the financial assistance provided, customer lists, income tax returns, and design, market and feasibility studies not paid for with public funds remain private or nonpublic.

City Attorney Records
CLASSIFICATION(S): Confidential
GOVERNING STATUTE: Minn. Stat. § 13.393

DESCRIPTION OF DATA: The use, collection, storage, and dissemination of data by the City Attorney are governed by statutes, rules, and professional standards concerning discovery, production of documents, introduction of evidence, and professional responsibility. Data which is the subject of attorney-client privilege is confidential. Data which is the subject of the "work product" privilege is confidential.

Civil Investigative Data
CLASSIFICATION(S): Confidential/Protected Nonpublic/Not public/Public
GOVERNING STATUTE: Minn. Stat. § 13.39
DESCRIPTION OF DATA: Data collected as part of an active investigation undertaken to commence or defend pending civil litigation, or which are retained in anticipation of pending civil litigation are classified as protected nonpublic data pursuant to Minn. Stat. § 13.02, subd. 13, in the case of data not on individuals and confidential pursuant to Minn. Stat. § 13.02, subd. 3, in the case of data on individuals. This does not include disputes where the sole issue is the City's timeliness in responding to a data request.

Council Meetings Having Data Classified as Nonpublic
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13D.05
DESCRIPTION OF DATA: Any portion of a meeting must be closed if expressly required by other law or if the following types of data are discussed: data that would identify alleged victims or reporters of criminal sexual conduct, domestic abuse, or maltreatment of minors or vulnerable adults; active investigative data as defined in section 13.82, subd. 7, or internal affairs data relating to allegations of law enforcement personnel misconduct collected or created by a state agency, statewide system, or political subdivision; or educational data, health data, medical data, welfare data, or mental health data that are not public data under section 13.32, 13.3805, subd. 1, 13.384, or 13.46, subd. 2 or 7.

Elected Officials Correspondence
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.601, subd. 2
DESCRIPTION OF DATA: Correspondence between individuals and elected officials is private data on individuals but may be made public by either the sender or the recipient.

Financial Disclosure Statements
CLASSIFICATION(S): Public
GOVERNING STATUTE: Minn. Stat. § 13.601, subd. 1.
DESCRIPTION OF DATA: Financial disclosure statements of elected or appointed officials which, by requirement of the City, are filed with the City, are public data on individuals.

Grants
CLASSIFICATION(S): Nonpublic/Private
GOVERNING STATUTE: Minn. Stat. § 13.599

DESCRIPTION OF DATA: Data created by state agency providing grants and persons/agencies that apply for or receive grants.

Identity of Employees Making Complaints
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 181.932, subd. 2; 13.7905, subd. 5(b)
DESCRIPTION OF DATA: The identity of an individual who reports to any governmental body or law enforcement official a violation or suspected violation by the individual's employer of any federal or state law or rule is private data on individuals if it meets the requirements of Minn. Stat. § 181.932, subd. 2.

Internal Competitive Response
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. §§ 13.591, subd. 5, 13.37.
DESCRIPTON OF DATA: A bid or proposal to provide government goods or services that is prepared by the staff of a government entity in competition with bids or proposals solicited by the same government entity from the private sector or a different government entity from the private sector are classified as private or nonpublic until completion of the selection process or completion of the evaluation process at which time the data are public with the exception of trade secret data as defined and classified in Minnesota Statutes, Section 13.37.

Internal Auditing Data
CLASSIFICATION(S): Confidential/Private/Protected Nonpublic/Public
GOVERNING STATUTE: Minn. Stat. § 13.392
DESCRIPTION OF DATA: Data, notes, and preliminary drafts of reports created, collected, and maintained by the internal audit offices of the city or by person performing audits for the City and relating to an audit or investigation; data on an individual supplying information for an audit or investigation, under specified circumstances.

Judicial Data
CLASSIFICATION(S): Confidential/Private/Protected Nonpublic/Public
GOVERNING STATUTE: Minn. Stat. § 13.03, subd. 4(e)
DESCRIPTION OF DATA: Judicial branch data disseminated to the City has the same classification in the hands of the City as it had in the hands of judicial branch entity providing it.

Personal Contact and Online Account Information
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.356, 13.04, subd. 2.
DESCRIPTION OF DATA: Data on an individual collected, maintained, or received by the City for notification purposes or as part of a subscription list for the City's electronic periodic publications as requested by the individual are classified as private data on individuals. This data includes telephone numbers, e-mail addresses, internet user names and passwords, Internet protocol addresses, and any other similar data related to the

individual's online account or access procedures. This data may only be used for the specific purpose for which the individual provided the data. This data also does not include data submitted for purposes of making a public comment.

Pleadings
CLASSIFICATION(S): Public
GOVERNING STATUTE: Minn. Stat. § 13.03, subd. 12
DESCRIPTION OF DATA: Pleadings in a lawsuit by or against the City.

Requests for Proposals
CLASSIFICATION(S): Private/Nonpublic/Not public/Public
GOVERNING STATUTE: Minn. Stat. §§ 13.591, subd. 3(b), 13.37.
DESCRIPTION OF DATA: Data submitted by a business to the City in response to a request for proposals, as defined in Minn. Stat. § 16C.02, subd. 12, are private or nonpublic until the time and date specified in the solicitation that proposals are due, at which time the name of the responder becomes public. All other data in a responder's response to a request for proposals are private or nonpublic data until completion of the evaluation process. After a government entity has completed the evaluation process, all remaining data submitted by all responders are public with the exception of trade secret data as defined and classified in Minn. Stat. § 13.37. A statement by a responder that submitted data are copyrighted or otherwise protected does not prevent public access to the data contained in the response. If all responses to a request for proposals are rejected prior to completion of the evaluation process, all data, other than the names of the responders, remain private or nonpublic until a resolicitation of the requests for proposal results in completion of the evaluation process or a determination is made to abandon the purchase. If the rejection occurs after the completion of the evaluation process, the data remain public. If a resolicitation of proposals does not occur within one year of the proposal opening date, the remaining data become public.

Sealed Bids
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.37
DESCRIPTION OF DATA: Sealed bids, including the number of bids received, prior to opening are classified as nonpublic data with regard to data not on individuals and as private data with regard to data on individuals.

Security Information
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.37
DESCRIPTION OF DATA: Data which, if the Responsible Authority determines if disclosed would be likely to substantially jeopardize the security of information possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury, is classified as nonpublic data with regard to data not on individuals and as private data with regard to data on individuals. This includes checking account numbers, crime prevention block maps and lists of

volunteers who participate in community crime prevention programs and the volunteers' home and mailing addresses, telephone numbers, e-mail or other digital addresses, Internet communication services account information or similar account information, and global positioning system locations. If the City denies a data request based on a determination that the data are security information, upon request, the City must provide a short description explaining the necessity for the classification.

Service Cooperative Claims Data
CLASSIFICATION(S): Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.203
DESCRIPTION OF DATA: Claims experience and all related information received from carriers and claims administrators participating in a group health or dental plan, including any long-term disability plan, offered through Minnesota service cooperatives to Minnesota political subdivisions and survey information collected from employees and employers participating in these plans and programs, except when the executive director of a Minnesota service cooperative determines that release of the data will not be detrimental to the plan or program, are classified as nonpublic data not on individuals.

Social Security Numbers
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.355
DESCRIPTION OF DATA: Social Security numbers of individuals are private data on individuals, except to the extent that access to the Social Security number is specifically authorized by law.

Social Security Numbers on Mailings
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.355, subd. 3
DESCRIPTION OF DATA: The City may not mail, deliver, or cause to be mailed or delivered an item that displays a Social Security number on the outside of the item or if it is visible without opening the item.

Trade Secret Information
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.37
DESCRIPTION OF DATA: Data, including a formula, pattern, compilation, program, device, method, technique or process: (1) that was supplied by the affected individual or organization; (2) that is the subject of efforts by the individual or organization that are reasonable under the circumstances to maintain its secrecy; and (3) that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use are nonpublic data with regard to data not on individuals and as private data with regard to data on individuals.

Utility Disconnection Data

CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.681, subd. 6
DESCRIPTION OF DATA: Data on customers provided to the City by a utility regarding disconnection of gas or electric service are private data on individuals or nonpublic data.

ADMINISTRATION

Absentee Ballots
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.37 and 13.607, subd. 7 and 203B.12, subd. 7
DESCRIPTION OF DATA: Sealed absentee ballots before opening by an election judge are private and nonpublic. Names of voters submitting absentee ballots may not be made available for public inspection until the close of voting on Election Day.

Assessor's Data
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.51
DESCRIPTION OF DATA: Data contained on sales sheets received from private multiple listing service organizations is private where the contract with the organizations requires the City to refrain from making the data available to the public. The following data collected by the City from individuals or business entities concerning income properties are private or nonpublic: (a) detailed income and expense figures; average vacancy factors; verified net rentable areas or net usable area, whichever is appropriate; anticipated income and expenses; projected vacancy factors; and lease information. Income information on individuals collected and maintained by the City to determine eligibility of property for class 4d under Minn. Stat. § 273.128 and 273.13, is private data on individuals.

Candidates for Election to City Council
CLASSIFICATION(S): Public/Private
GOVERNING STATUTE: Op. Atty.Gen. No. 852, October 6, 2006; Advisory Opinion No. 05-036; Minn. Stat. § 13.607, subd. 8 and 204B.06, subd. 1b
DESCRIPTION OF DATA: Data created, collected, or maintained about an individual candidate for election to the City Council is public. An affidavit of candidacy must state an address of residence and telephone number. The candidate may request that the address be classified as private data by certifying that a police report has been submitted or an order for protection has been issued in regard to the safety of the candidate or candidate's family, or that the candidate's address is otherwise private pursuant to Minnesota law.

Computer Access Data
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.15
DESCRIPTION OF DATA: Data created, collected, or maintained about a person's access to the City's computer system for the purpose of: (1) gaining access to data or information; (2) transferring data or information; or (3) using government services are private data on individuals or nonpublic data. This data does not include a cookie temporarily installed by

the City on a person's computer during a single session or visit to the City's web site if the cookie is installed only in a computer's memory and is deleted from the memory when the web site browser or web site application is closed.

Deferred Assessment Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.52
DESCRIPTION OF DATA: Data collected pursuant to Minnesota Statutes, Section 435.193, which indicates the amount or location of cash or other valuables kept in the homes of applicants for deferred assessment are private data.

Federal Contracts Data
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.35
DESCRIPTION OF DATA: All data collected and maintained by the City when required to do so by a federal agency as part of its contract with the City are classified as either private or nonpublic depending on whether the data are data on individuals or data not on individuals.

Homestead Applications
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.4965, subd. 3, 273.124, subd. 13
DESCRIPTION OF DATA: Social Security numbers, affidavits, or other proofs of entitlement to homestead status that are submitted by property owners or their spouses are private data on individuals. The data may be disclosed to the Commissioner of Revenue or, under limited circumstances, the County Treasurer.

Municipal Bonds Register Data
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. §§ 13.202, subd. 12, 475.55, subd. 6
DESCRIPTION OF DATA: Data with respect to the ownership of municipal obligations are nonpublic data or private data on individuals.

Municipal Electric Utility Customer Data
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.685
DESCRIPTION OF DATA: Data on customers of municipal electric utilities are private data on individuals or nonpublic data.

Municipal Self-insurer Claims
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.202, subd. 9(a), 471.617, subd. 5
DESCRIPTION OF DATA: Data about individual claims or total claims made by an individual under a self-insured health benefit plan of a municipality are private.

Registered Voter Lists
CLASSIFICATION(S): Confidential/Public
GOVERNING STATUTE: Minn. Stat. §§ 13.607, subd. 6; 201.091
DESCRIPTION OF DATA: The information contained in the master list of registered voters may only be made available to public officials for purposes related to election administration, jury selection, and in response to a law enforcement inquiry concerning a violation of or a failure to comply with any criminal statute or state or local tax statute.

Social Recreational Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.548
DESCRIPTION OF DATA: For individuals enrolling in recreational or other social programs: name, address, telephone number, any other data that identifies the individual, and any data which describes the health or medical condition of the individual, family relationships, living arrangements, and opinions as to the emotional makeup or behavior of an individual are classified as private.

Solid Waste Collector Customer Lists
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. §§ 13.7411, subd. 4 (c), 115A.93, subd. 5
DESCRIPTION OF DATA: Customer lists provided to the City by solid waste collectors.

COMMUNITY AND REAL PROPERTY

Appraisal Data
CLASSIFICATION(S): Confidential/Protected Nonpublic/Public
GOVERNING STATUTE: Minn. Stat. § 13.44, subd. 3
DESCRIPTION OF DATA: Estimated or appraised values of property that are made by the City or by an independent appraiser acting for the City for the purpose of selling or acquiring land through purchase or condemnation are classified as confidential data on individuals or protected nonpublic data. However, this data becomes public at the discretion of the City Council, determined by majority vote of the City's governing body. Appraised values of property that are made by appraisers working for fee owners or contract purchasers who have received an offer to purchase their property from a government entity are classified as private data on individuals or nonpublic data. Appraisal data made confidential or nonpublic become public when the data are submitted to a court appointed condemnation commissioner, the data are presented in court in condemnation proceedings, or the parties enter into an agreement for the purchase and sale of the property.

Award Data
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.48

DESCRIPTION OF DATA: Financial data on business entities submitted to the City for the purpose of presenting awards to business entities for achievements in business development or performance are private data on individuals or nonpublic data.

Benefit Data
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.462
DESCRIPTION OF DATA: Data on individuals collected or created when an individual seeks information about becoming, is or was an applicant for or a recipient of benefits or services provided under any housing, home ownership, rehabilitation and community action agency, Head Start, or food assistance programs administered by the City are private data on individuals with the exception of the names and addresses of applicants for and recipients of the benefits, which are classified as public data on individuals.

Property Complaint Data
CLASSIFICATION(S): Confidential
GOVERNING STATUTE: Minn. Stat. § 13.44, subd. 1
DESCRIPTION OF DATA: Data that identifies individuals who register complaints concerning violations of state laws or local ordinances concerning the use of real property are classified as confidential data.

Planning Questionnaires
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.59
DESCRIPTION OF DATA: Names and addresses of individuals and businesses and the legal descriptions of property owned by individuals and businesses, when collected in surveys of individuals conducted by the City for the purposes of planning, development, and redevelopment.

Redevelopment Data
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.59
DESCRIPTION OF DATA: Names and addresses of individuals and the legal descriptions of property owned by individuals, when collected in surveys of individuals conducted by the City or a housing and redevelopment authority for the purposes of planning, development, and redevelopment are classified as private data. Names and addresses of businesses and the legal descriptions of business properties and the commercial use of the property to the extent the disclosure of the use would identify a particular business are nonpublic data.

PERSONNEL

Applicant Information
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.43.
DESCRIPTION OF DATA: Generally, all data about people who are or were an employee, an applicant for employment, a volunteer, or an independent contractor is private with the following exceptions which are public:

- Veteran status
- Relevant test scores
- Rank on eligibility list
- Job history
- Education and training
- Work availability
- Name, after being certified as eligible for appointment to a vacancy or when considered a finalist for a position of public employment (which occurs when the person has been selected to be interviewed by the appointing authority)
- Names of applicants for appointment to and members of an advisory board or commission.

Applicants to a Public Body
CLASSIFICATION(S): Public
GOVERNING STATUTE: Minn. Stat. § 13.601
DESCRIPTION OF DATA: Generally, all data about people who are or were an applicant to or an appointed member of a public body is private with the following exceptions which are public:

- Name
- City of Residence
- Education and Training
- Employment History
- Volunteer Work
- Awards and Honors
- Prior Government Service

Appointed (Not Elected) Members to a Public Body
CLASSIFICATION(S): Public
GOVERNING STATUTE: Minn. Stat. § 13.601
DESCRIPTION OF DATA: Generally, all data about people who are or were an appointed, not elected, to a public body is private, with the following exceptions which are public:

- Name
- City of Residence
- Education and Training
- Employment History
- Volunteer Work

- Awards and Honors
- Prior Government Service
- Residential Address
- Either a telephone number or electronic mail address where the appointee can be reached, or both, at the request of the appointee

Employee Assistance Information
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.43, subd. 7
DESCRIPTION OF DATA: Employee assistance program data, such as training, assessment, counseling, and referral services for employees and their dependents, are private data on individuals.

Employee Data Generally
CLASSIFICATION(S): Confidential/Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.43.
DESCRIPTION OF DATA: Generally, all data about current and former City employees, volunteers, and independent contractors are private with the following exceptions which are public:

- Name
- Actual gross salary
- Salary Range
- Contract fees
- Actual gross pension
- Value and nature of employer paid fringe benefits
- Basis for and the amount of added remuneration, including expense reimbursement, in addition to salary
- Job title
- Job description
- Education and training background
- Previous work experience
- Date of first and last employment
- The existence and status (but not nature) of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action
- Final disposition of any disciplinary action, with specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body
- Terms of any agreement settling any dispute arising from the employment relationship, including a "buyout" agreement
- Work location
- Work telephone number
- Badge number
- Honors and awards received

- Payroll time sheets or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other non-public data.

Employee Drug and Alcohol Tests
CLASSIFICATION(S): Confidential/Private
GOVERNING STATUTE: Minn. Stat. § 13.43, subd. 5c), 181.954, subd. 2 and 3
DESCRIPTION OF DATA: Test results and other information acquired in an employee drug and alcohol testing process are private data on individuals.

Employment and Training Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.47
DESCRIPTION OF DATA: Data on individuals collected, maintained, used, or disseminated because an individual applies for, is currently enrolled in, or has been enrolled in employment and training programs funded with federal, state, or local resources are private data on individuals.

Examination Data
CLASSIFICATION(S): Private/Confidential
GOVERNING STATUTE: Minn. Stat. § 13.34
DESCRIPTION OF DATA: Data consisting solely of testing or examination materials or scoring keys used solely to determine individual qualifications for appointment or promotion, the disclosure of which would compromise the objectively or fairness of the testing or examination process are classified as nonpublic, except pursuant to court order.

Harassment
CLASSIFICATION(S): Confidential/Private
GOVERNING STATUTE: Minn. Stat. § 13.43 subd. 8
DESCRIPTION OF DATA: When there is a harassment complaint against an employee, the employee may not have access to data that would identify the complainant or other witnesses if the data would threaten the personal safety of the complainant or witness or subject the complainant or witness to harassment. However, summary information will be provided to the employee in order for him/her to prepare for a disciplinary proceeding that has been initiated.

Human Rights Data
CLASSIFICATION(S): Confidential/Private/Protected Nonpublic/Public
GOVERNING STATUTE: Minn. Stat. §§ 13.552, 363A.28 and 363A.35
DESCRIPTION OF DATA: Data maintained by the human rights department of the city, including: investigative data in an open case file; the name and address of the charging party or respondent, factual basis of the allegations, and statute or ordinance under which the charge is brought; investigative data in a closed case file.

Labor Relations Information
CLASSIFICATION(S): Private/Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.37
DESCRIPTION OF DATA: Management positions on economic and non-economic items that have not been presented during the collective bargaining process or interest arbitration, including information specifically collected or created to prepare the management position is classified as nonpublic data with regard to data not on individuals and as private data with regard to data on individuals.

Personnel and Employment Data
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.43.
DESCRIPTION OF DATA: Certain government data on individuals maintained because the individual is or was an employee of or an applicant for employment by, performs services on a voluntary basis for, or acts as an independent contractor with the City are public as set forth in Minn. Stat. § 13.43, subd. 2. All other personnel data is private data on individuals but may be released pursuant to a court order. Data pertaining to an employee's dependents are private data on individuals.

Protection of Employee or Others
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.43 subd 11
DESCRIPTION OF DATA: If it is reasonably necessary to protect an employee from harm to self or to protect another person who may be harmed by the employee, information that is relevant to the safety concerns may be released to (1) the person who may be harmed or to the person's attorney when relevant to obtaining a restraining order, (2) a prepetition screening team in the commitment process, or (3) a court, law enforcement agency or prosecuting authority.

Salary Benefit Survey Data
CLASSIFICATION(S): Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.435
DESCRIPTION OF DATA: Salary and personnel benefit survey data purchased from consulting firms, nonprofit corporations or associations or obtained from employers with the written understanding that the data shall not be made public are classified as nonpublic data.

Undercover Law Enforcement Officer
CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.43 subd. 5
DESCRIPTION OF DATA: All personnel data about an undercover law enforcement officer is private until no longer assigned to those duties. Then, the officer is subject to the same rules applicable to other employees unless the law enforcement agency determines that revealing the data would threaten the officer's safety or jeopardize an active investigation.

Public Safety Peer Counseling and Critical Incident Stress Management Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.43, subd. 9, 181.9731, 181.9732
DESCRIPTION OF DATA: Data acquired by a peer support counselor in public safety peer counseling or data acquired by a critical incident stress management team member providing critical incident stress management services. "Public safety peer counseling" means a session or sessions led by a peer support counselor held for an emergency service provider (peace officers, correctional officers, probation officers, supervision agents, firefighters, rescue squad members, dispatchers, hospital or emergency medical clinic personnel, a person who provides emergency medical services for a Minnesota licensed ambulance service, forensic science professional, or other person involved with public safety emergency services, either paid or volunteer) who experienced an occupation-related trauma, illness, or stress develop skills and strategies to better understand, cope with, and process emotions and memories tied to the trauma, illness, or stress. This includes group sessions led by a peer support counselor, one-to-one contact with a peer support counselor, and meetings with a peer support counselor to obtain referrals to appropriate mental health or community support services. "Critical incident stress management services" means consultation, risk assessment, education, intervention, and other crisis intervention services provided by a critical incident stress management team or critical incident stress management team member to an emergency service provider affected by a critical incident. The data shall not be disclosed to third parties as it is classified as private data. Exceptions include when disclosure: (1) is necessary to prevent harm to self by the recipient of the services or to prevent the person from harming someone else; (2) is required by mandatory reporting laws; (3) is authorized by the person who received services and the person provides written consent; (4) is authorized by the living spouse or estate administrator of a deceased person who received services; or (5) is required under limited circumstances related to testimony.

PUBLIC SAFETY

Arson Investigation
CLASSIFICATION(S): Confidential/Public
GOVERNING STATUTE: Minn. Stat. §§ 13.6905, subd. 26, 299F.055 and 299F.056
DESCRIPTION OF DATA: Data received pursuant to the Arson Reporting Immunity Law, Minn. Stat. § 299F.052 to 299F.057 by an authorized person or insurance company shall be confidential data until its release is required pursuant to a criminal or civil proceeding

Child Abuse Report Records
CLASSIFICATION(S): Confidential/Private
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 6 (b), 13.82, subd. 8 and 9 and 626.556, Minnesota Statutes Chapter 260E
DESCRIPTION OF DATA: Active or inactive investigative data that identify a victim of child abuse or neglect reported under Minnesota Statutes, Section 626.556 are private data on individuals. Active or inactive investigative data that identify a reporter of child abuse or

neglect under Minnesota Statutes, Section 626.556 are confidential data on individuals, unless the subject of the report compels disclosure under Minnesota Statutes, Section 626.556, subd. 11. Investigative data that become inactive under Minnesota Statutes, Section 626.556, subd. 7 (a) or (b) and that relate to the alleged abuse or neglect of a child by a person responsible for the child's care, as defined in Minnesota Statutes, Section 626.556, subd. 2 are private data. Various child maltreatment classifications and requirements re-organized under Minnesota Statutes Chapter 260E.

Civil Commitment Data
CLASSIFICATION(S):
GOVERNING STATUTE: Minn. Stat. § 253B.185, subd. 1(b)
DESCRIPTION OF DATA: Notwithstanding any provision of Chapter 13, a county attorney considering the civil commitment of a person may obtain records and data from the City upon request and without a court order.

Corrections and Detention Data
CLASSIFICATION(S): Confidential/Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.85
DESCRIPTION OF DATA: Data on individuals created, collected, used or maintained because of their lawful confinement or detainment in state reformatories, prisons and correctional facilities, municipal or county jails, lockups, work houses, work farms and all other correctional and detention facilities are classified as private to the extent that the release of the data would either: (a) disclose medical, psychological or financial information or personal information not related to their lawful confinement or detainment or (b) endanger an individual's life. Corrections and detention data are confidential to the extent that the data would (a) endanger an individual's life, (b) endanger the effectiveness of an investigation authorized by statute relating to the enforcement of rules or law, (c) identify a confidential informant, or (d) clearly endanger the security of any institution or its population.

Crime Victim Notice of Release
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 5 (a), 611A.06
DESCRIPTION OF DATA: All identifying information regarding a crime victim, including a victim's request for notice of release and a notice of release made pursuant to Minnesota Statutes, Section 611A.06 is classified as private data on individuals.

Criminal Gang Investigative Data System
CLASSIFICATION(S): Confidential
GOVERNING STATUTE: Minn. Stat. §§ 13.6905, subd. 14, 299C.091
DESCRIPTION OF DATA: Data in the criminal gang investigative data system are confidential data on individuals as defined in Minnesota Statutes, Section 13.02, subd. 3, but are accessible to law enforcement agencies and may be released to the criminal justice agencies.

Criminal History Data

CLASSIFICATION(S): Private/Public
GOVERNING STATUTE: Minn. Stat. § 13.87
DESCRIPTION OF DATA: Criminal history data maintained by agencies, political subdivisions and statewide systems are classified as private, pursuant to Minnesota Statutes, Section 13.02, subd. 12, except that the data created, collected, or maintained by the Bureau of Criminal Apprehension that identify an individual who was convicted of a crime, the offense of which the individual was convicted, associated court disposition and sentence information, controlling agency and confinement information are public data for 15 years following the discharge of the sentence imposed for that offense. Data maintained in the integrated search service is private. An individual who is the subject of the data may only be provided with (1) a list of government entities that provided public or private data about the individual and (2) data that describes what is maintained about the individual at each government entity on the list.

Criminal History Data – Discharge / Dismissal of Crime
CLASSIFICATION(S): Not Public
GOVERNING STATUTE: Minn. Stat. § 13.871
DESCRIPTION OF DATA: Data in criminal discharge and dismissal records is classified under Minn. Stat. § 609.3751, subd. 5.

Corrections and Detention Data
CLASSIFICATION(S): Private/Confidential/Public
GOVERNING STATUTE: Minn. Stat. § 13.85
DESCRIPTION OF DATA: Data on individuals created, collected, used, or maintained because of their lawful confinement or detainment in a correctional or detention facility, including a municipal jail or lockup is classified under Minn. Stat. § 13.85.

Domestic Abuse Data
CLASSIFICATION(S): Confidential/Public
GOVERNING STATUTE: Minn. Stat. § 13.80
DESCRIPTION OF DATA: Data on individuals collected, created, received, or maintained by the Police Department pursuant to the Domestic Abuse Act, Minn. Stat. § 518B.01 are classified as confidential data, pursuant to Minn. Stat. § 13.02, subd. 3, until a temporary court order made pursuant to Minn. Stat. § 518B.01, subd. 5 or 7 is executed or served upon the data subject who is the respondent to the action.

E-Charging Data
CLASSIFICATION(S): Private/Nonpublic, Confidential /Protected Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.871, subd. 11 and 299C.41.
DESCRIPTION OF DATA: Credentialing data is private or nonpublic data. Auditing data and workflow and routing data are classified as provided by other law.

EMT or First Responder Misconduct Data
CLASSIFICATION(S): Confidential/Protected Nonpublic
GOVERNING STATUTE: Minn. Stat. §§ 13.383, subd. 2, 144E.305, subd. 3.

DESCRIPTION OF DATA: Reports of emergency medical technicians, emergency medical technicians-intermediate, emergency medical technicians-paramedic or first responders' misconduct are considered to be confidential or protected nonpublic while an investigation is active. Except for the Emergency Medical Services Regulatory Board's final determination, all communications or information received by or disclosed to the Board relating to disciplinary matters of any person or entity subject to the Board's regulatory jurisdiction are confidential and privileged and any disciplinary hearing shall be closed to the public.

Emergency Telephone Service
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.202, subd. 6, 403.07, subd. 3 and 4
DESCRIPTION OF DATA: Names, addresses and telephone numbers provided to a 911 system are private data subject only to public safety exceptions.

Explosives or Blasting Agents
CLASSIFICATION(S): Nonpublic
GOVERNING STATUTE: Minn. Stat. § 13.6905, subd. 28a; Minn. Stat. § 299F.28 and 299F.75, subd. 4
DESCRIPTION OF DATA: Data related to use and storage of explosives by individuals holding a permit, including locations of storage, place, and time of intended use of explosives or blasting agents, and place and means of storage of explosives or blasting agents are nonpublic. Data may be shared with a government entity or utility whose job duties require access to a facility containing explosives but may not be disclosed to anyone not directly involved in work to be completed at the site where the explosives or blasting agents are stored or used.

Firearms Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.87, subd. 2
DESCRIPTION OF DATA: Data about the purchase or transfer of firearms and applications for permits to carry firearms are classified as private data on individuals.

Hazardous Substance Emergency
CLASSIFICATION(S): Nonpublic
GOVERNING STATUTE: Minn. Stat. §§ 13.6905, subd. 27, 299F.095 and 299F.096, subd. 1
DESCRIPTION OF DATA: Data contained in hazardous materials notification reports made pursuant to Minnesota Statutes, Sections 299F.091 to 299F.099 are classified as nonpublic data.

Health Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.3805, subd. 1
DESCRIPTION OF DATA: Data on individuals created, collected, received, or maintained by the City relating to the identification, description, prevention, and control of disease or as part

of an epidemiologic investigation designated by the commissioner of health as necessary to analyze, describe or protect the public health are private data on individuals.

Integrated Search Service Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 13.873
DESCRIPTION OF DATA: Data on individuals stored on one or more databases maintained by criminal justice agencies and accessible through the integrated search service operated by the Bureau of Criminal Apprehension are private.

Investigative Detention Data
CLASSIFICATION(S): Confidential
GOVERNING STATUTE: Minn. Stat. § 13.86
DESCRIPTION OF DATA: Data created, collected, used, or maintained by a municipal correctional or detention facility that, if revealed, would identify an informant who provided information about suspected illegal activities and is likely to subject the informant to physical reprisals by others are confidential data on individuals.

Law Enforcement Data
CLASSIFICATION(S): Private/Confidential/Public/Non-Public
GOVERNING STATUTE: Minn. Stat. §§13.82, 259.10, subd. 2, 626.19
DESCRIPTION OF DATA: Certain arrest data, request for service data, and response or incident data are public data.

An audio recording of a call placed to a 911 system for the purpose of requesting service for law enforcement, fire or medical emergency is private data on individuals, except that a written transcript of the audio recording is public, unless it reveals the identity of an individual otherwise protected under Minn. Stat. § 13.82, subd. 17.

Criminal investigative data collected or created by a law enforcement agency in order to prepare a case against a person for the commission of a crime or other offense for which the agency has primary investigative responsibility is confidential or protected nonpublic while the investigation is still active. Inactive investigation data is public unless the release of the data would jeopardize another ongoing investigation or would reveal the identity of individuals protected under Minn. Stat. § 13.82, subd. 17.

A law enforcement agency may make any data classified as confidential or protected nonpublic pursuant to Minn. Stat. 13.82, subd. 7 or as private or nonpublic under Minn. Stat. 13.825 or Minn. Stat. 626.19 accessible to any person, agency, or the public if the agency determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

Images and recordings, including photographs, video, and audio records, which are part of inactive investigative files, and which are clearly offensive to common sensibilities are

classified as private or nonpublic data, provided that the existence of the images and recordings shall be disclosed to any person requesting access to the inactive investigative file.

Data on court records relating to name changes under Minn. Stat. § 259.10, subd. 2 which is held by a law enforcement agency is confidential data on an individual while an investigation is still active and is private data on an individual when the investigation becomes inactive.

Data in arrest warrant indices are classified as confidential data until the defendant has been taken into custody, served with a warrant or appears before the court, except when the law enforcement agency determines that the public purpose is served by making that information public.

Data that uniquely describe stolen, lost, confiscated, or recovered property are classified as either private data on individuals or nonpublic data depending on the content.

Financial records of a program that pays rewards to informants are protected nonpublic data in the case of data not on individuals or confidential data in the case of data on individuals.

Data on registered criminal offenders as described in Minn. Stat. § 243.166 are private data on individuals.

Data included in a missing children bulletin distributed pursuant to Minn. Stat. § 299C.54 are public data.

Data that reflect deliberative processes or investigative techniques of law enforcement agencies are confidential data on individuals or protected nonpublic data, provided that information, reports, or memoranda that have been adopted as the final opinion or justification for a decision of a law enforcement agency are public data.

Booking photographs are public data.

Data that would reveal the identity of persons who are customers of a licensed pawnbroker, secondhand goods dealer or a scrap metal dealer are private data on individuals. Data describing the property in a regulated transaction with a licensed pawnbroker, secondhand goods dealer or a scrap metal dealer are public.

Investigative data that become inactive that consist of a person's financial account number or transaction numbers are private or nonpublic data.

The existence of all technology maintained by a law enforcement agency that may be used to electronically capture an audio, video, photographic, or other record of the activities of the general public, or of an individual or group of individuals, for purposes of conducting an investigation, responding to an incident or request for service, monitoring or maintaining public order and safety, or engaging in any other law enforcement function authorized by law is public data.

Data collected by a law enforcement agency using an unmanned aerial vehicle ("UAV") are private data on individuals or nonpublic data, subject to certain conditions and exceptions. Data collected by a UAV must be deleted as soon as possible or no later than seven days after collection unless the data is part of an active criminal investigation.

Orders for Protection, Harassment Restraining Orders, and No Contact Orders
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 13 and 299C.46, subd. 6
DESCRIPTION OF DATA: Data from orders for protection, harassment restraining orders, and no contact orders and data entered by law enforcement to assist in enforcement of those orders are private data on individuals. Data about the offender can be shared with the victim for purposes of enforcement of the order.

Peace Officer Discipline Procedures
CLASSIFICATION(S): Confidential/Private/Public
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 6(o), 626.89, subd. 6, 13.43, and 626.8457, subd. 3
DESCRIPTION OF DATA: Investigative report made by a law enforcement agency in connection with a peace officer disciplinary matter; identities of confidential informants in such matters; identities of witnesses expected to testify in disciplinary hearings. Certain data must be reported to the Minnesota Board of Police Officer Standards and Training ("POST Board").

Peace Officer Records on Juveniles
CLASSIFICATIONS(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.875, subd. 2, 260B.171, subd. 5.
DESCRIPTION OF DATA: Peace officers' records of children who are or may be delinquent or who may be engaged in criminal acts are private data but shall be disseminated pursuant to Minn. Stat. § 260B.171, subd. 5.

Peace Officer Reports on Accidents
CLASSIFICATION(S): Confidential
GOVERNING STATUTE: Minn. Stat. § 169.09, subd. 13
DESCRIPTION OF DATA: Data collected by law enforcement agencies as required for a report of an accident under Minn. Stat. § 169.09, subd. 8. Data must be disclosed to, upon written request by, individuals involved in an accident or representing the individual's estate, surviving spouse, next of kin, or an appointed trustee, or other person injured in person, property, or means of support, or who incurs other pecuniary loss by virtue of the accident.

Reports of Gunshot Wounds
CLASSIFICATION(S): Confidential
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 6 (a), 626.53

DESCRIPTION OF DATA: A report made by a health professional concerning a wound or injury arising from or caused by discharge of a firearm or inflicted by the perpetrator of a crime using a dangerous weapon other than a firearm is confidential data on individuals.

Safe at Home Program Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.805 and 5B.07, subd. 1(b).
DESCRIPTION OF DATA: Identity and location data on a Safe at Home program participant not otherwise classified by law are private data. "Program participant" means an individual certified as a program participant under Minn. Stat. § 5B.03. "Identity and location data" means any data used to identify or physically locate a program participant, including but not limited to the program participant's name, residential address, work address, and school address, and that is collected received or maintained prior to the date a program participant's certification expires, or notice of withdrawal from the participant. Private or confidential identity and location data on a program participant who submits a notice in writing that the participant is certified in the Safe at Home address confidentiality program may not be shared with any other government entity or disseminated to any person unless 1) the program participant has expressly consented in writing to sharing the dissemination of the data for the purpose in which the sharing will occur; 2) the data are subject to dissemination pursuant to a court order; 3) the data are subject to sharing pursuant to Minn. Stat. § 5B.07, subd. 2; 4) the location data related to county of residence are needed to provide public assistance or other government services, or to allocate financial responsibility for the assistance or services; 5) the data are necessary to perform a government entity's health, safety, or welfare functions, including the provision of emergency 911 services, the assessment and investigation of child or vulnerable adult abuse or neglect, or the assessment or inspection of services or locations for compliance with health, safety, or professional standards; or 6) the data are necessary to aid an active law enforcement investigation of the program participant. Regardless of whether certification has been submitted, the City must accept the address designated by the Secretary of State as a program participant's address and is subject to the requirements contained in Minn. Stat. § 5B.05.

Sex Offender HIV Tests
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 5(b), 611A.19, subd. 2
DESCRIPTION OF DATA: Results of HIV tests of sex offenders are private data on individuals and must be handled in accordance with Minnesota Statutes, Section 611A.19.

Sexual Assault Crime Victims
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 3(e), 609.3471
DESCRIPTION OF DATA: Data that specifically identifies a victim who is a minor, in records or reports relating to petitions, complaints or indictments made are private data, if related to any of the following offenses: solicitation/inducement/promotion of prostitution, sex trafficking, criminal sexual predatory conduct, and criminal sexual conduct in the first, second, third or fourth degrees.

Videotapes of Child Abuse Victims
CLASSIFICATION(S): Private/Confidential
GOVERNING STATUTE: Minn. Stat. §§ 13.821, 611A.90
DESCRIPTION OF DATA: An individual subject of data may not obtain a copy of a videotape in which a child victim or alleged victim is alleging, explaining, denying, or describing an act of physical or sexual abuse without a court order under Minn. Stat. § 13.03, subd. 6 or 611A.90.

Visa Eligibility Data
CLASSIFICATION(S): Private
GOVERNING STATUTE: Minn. Stat. § 611A.95
DESCRIPTION OF DATA: Data provided to a local law enforcement agency for the purposes of certification for "U nonimmigrant status" (or "U visa"). U nonimmigrant status is for victims of certain crimes who have suffered mental or physical abuse and are helpful to law enforcement or government officials in the investigation or prosecution of criminal activity. Local law enforcement agencies must not disclose the immigration status of victims of certain criminal activity as described by the federal Immigration and Nationality Act, except to comply with a federal law or legal process or when given authority by the victim or the victim's legal representative requesting certification.

Vulnerable Adult Report Records
CLASSIFICATION(S): Private/Confidential
GOVERNING STATUTE: Minn. Stat. §§ 13.871, subd. 6 (l), 626.557, subd. 12(b).
DESCRIPTION OF DATA: Data contained in reports made pursuant to Minn. Stat. § 626.557 of possible incidents of maltreatment of vulnerable adults and identities of individuals making such reports are confidential data on individuals or protected nonpublic data.