

CITY OF CHASKA

DATA PRACTICES POLICIES

1. Introduction.

- A. **Purpose.** These policies are adopted to comply with the requirements of the Minnesota Government Data Practices Act found at Minnesota Statutes, Chapter 13, as amended (the “**Act**”) and the Rules promulgated by the Commissioner of Administration. Specifically, these policies and the guides discussed below have been adopted to comply with Minnesota Statutes, Sections 13.03, subdivision 2, 13.05, subdivision 5 and Chapter 1205 of the Minnesota Rules (the “**Rules**”).
- B. **Guides.** In addition to the policies set forth in this document, the City of Chaska (“**City**”) adopts two guides regarding government data. The first is titled “Guide for Members of the Public Requesting Government Data,” and the second is titled “Guide for Data Subjects Requesting Government Data.” The guides have been prepared to provide information to the public and data subjects, respectively, regarding the City’s data practices policies. These policies and the guides, together, constitute the City’s policies regarding government data.
- C. **Interpretation.** The City intends to remain in compliance with the Act and Rules, and if any procedure contained in these policies or the guides is inconsistent with the requirements of the Act, as amended, or Rules the specific provisions of the Act or Rules shall control.

2. **Responsible Authority, Designees, and Practices Compliance Official.** Pursuant to Minnesota Rules, Part 1205.1000 and Minnesota Statutes Section 13.02, subd. 16, the City Council is required to appoint a person that is responsible for the collection, use and distribution of government data (the “**Responsible Authority**”). The Responsible Authority, in turn, may appoint designees to carry out the Responsible Authority’s required duties (the “**Designees**”). Further, the Responsible Authority must appoint a Data Practices Compliance Official (the “**Compliance Official**”) to handle questions or issues that may arise in regard to data access. Exhibit 1 to these policies lists: i) the Responsible Authority appointed by the City Council; ii) the Designees appointed by the Responsible Authority, if any; and iii) the Compliance Official appointed by the Responsible Authority. 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 and Rules. The Responsible Authority is also authorized to amend or supplement the Exhibits attached to these policies as needed to further the intent of these policies and the City’s compliance with the Act. For purposes of carrying out these policies, the term Responsible Authority shall include Designees unless the context in which the term is used indicates a different intent.

3. **Types of Governmental Data.** The Act applies to government data. Government data is defined in the Act to include “all data collected, created, received, maintained or disseminated” by the City “regardless of its physical form, storage media or conditions of use.” The Act divides government data into three broad classifications: i) data on individuals; ii) data on decedents; and iii) data not on individuals or decedents. All government data is presumed to be public unless there is a specific statute, federal law or temporary classification that classifies it otherwise. The only time this presumption is not true is in the case of City personnel data, where the presumption is reversed. All personnel data is presumed to be private unless a specific state statute or federal law classifies it as public. As required by the Act, Exhibit 2 to these policies lists the private and confidential data on individuals that the City maintains. The remaining sections of this policy describe who has access to government data held by the City and, when access is allowed, the procedure that a person can use to obtain access.

4. Access to Public Data.

- A. **People Entitled to Access.** Any person has the right to inspect or view public data. The person does not need to state his or her name or give the reason for the request. 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 8). Copyrighted public documents may be shown to anyone but shall not be reproduced or photocopied without express written permission from the copyright holder.

- 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.
- Public documents created by the City of Chaska and/or 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.

B. Form of Request. Any request to view or receive copies of public data must be in writing. The form to request data can be found in the Guide for Members of the Public Requesting Government Data, which is available from the City upon request.

C. 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. 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. The Responsible Authority must also 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.

D. 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 electronic copy.

E. Time Limits.

- Requests. Requests will be received and processed only during normal business hours.
- Response. Except as provided in the next sentence, the City's response will be provided as soon as is reasonably possible. If data is requested by an individual that is the subject of the data, the City will provide a response within ten (10) days of the date of the request, excluding Saturdays, Sundays and legal holidays.

The Responsible Authority will respond to public data requests as soon as reasonably possible. The Responsible Authority may require the requesting person to make an appointment or return at a later time to inspect or to pick up copies of the requested data.

F. 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 Guide for Members of the Public Requesting Government Data if the request is made by a member of the public that is not the subject of the data. If the request is made by the subject of the data, fees will be charged as described in the Guide for Data Subjects Requesting Government Data. Both Guides are available from the City upon request.

5. Access to Private and Confidential Data on Individuals. Government data on individual people is classified by law as public, private, or confidential. A list of the private and confidential data maintained by the City is contained in Exhibit 2.

A. People Entitled to Access.

- **Public data** about an individual may be shown or given to anyone for any reason as described in Section 4 above.
- **Private data** about an individual may be shown or given to:
 - The individual, but only once every six (6) months, unless a dispute has arisen or additional data has been collected.
 - A person who has been given access by the express written consent of the data subject. This consent must be on the form attached as Exhibit 7, or a form reasonably similar.
 - A person authorized to have access by federal, state, or local law or court order.
 - A person about whom the individual was advised at the time the data was collected. The identity of those people must be part of the Tennessee warning described below.
 - A person who is a member of the City staff, the City Council, or outside agents (such as attorneys) whose work assignment or responsibility reasonably requires access.
- **Confidential data** may not be given to the subject of the data, but may be given or shown to:
 - A person authorized to have access by federal, state, or local law or court order.
 - A person who is a member of the City staff, the City Council, or outside agents (such as attorneys) whose work assignment or responsibility reasonably requires access.

B. Form of Request. Any request to view or receive copies of private or confidential data on an individual must be in writing. Such 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. If the subject of the data is making the request, the requestor can use the written request form attached to the Guide for Data Subjects Requesting Government Data. If the requestor is not the subject of the data, the form attached to the Guide for Members of the Public Requesting Government Data should be used, accompanied by a fully executed Consent to Release Private Data, the form of which is attached as Exhibit 7.

C. Identification of Requesting Party. The Responsible Authority or Designee 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.

D. Time Limits.

- Requests. Requests will be received and processed only during normal business hours.
- Response. Except as provided in the next sentence, the City's response will be provided as soon as is reasonably possible. If data is requested by an individual that is the subject of the data, the City will provide a response within ten (10) days of the date of the request, excluding Saturdays, Sundays and legal holidays.

E. Fees. Fees may be charged in the same manner as for public data, except when the requestor is the subject of the data. When the requestor is the subject of the data, the requestor shall be allowed to inspect data without charge and if the requestor wants copies of the data, the City shall require the requestor to pay the actual cost of making, certifying and compiling the copies in the same manner as when actual costs are charged to provide copies of public data.

F. Summary Data. Summary data is 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 or Designee will prepare summary data upon request, if the request is in writing and the requesting party pays for the cost of the preparation. The Responsible Authority or Designee 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 ten (10) days after receiving the request. If the summary data cannot be prepared within ten (10) days, the Responsible Authority must notify the requester of the anticipated time schedule and the reason for the delay. (Exhibit 4).

Summary data may be prepared by “blacking out” personal identifiers, cutting out portions of the records that contain personal identifiers, 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. In this situation, the Responsible Authority may use the form attached as Exhibit 5.

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

- Parental/Guardian Access. In addition to the people listed above who may have access to private data, a Parent of an individual may have access to private data about a minor or an incapacitated person. For the purposes of these policies, “**Parent**” means a natural parent of the minor, a guardian or an individual acting as a parent or guardian in the absence of a parent or guardian. The Parent is presumed to have this right unless the minor has requested the Responsible Authority or Designee to withhold the data and withholding the data would be in the best interest of the minor, or it has been given evidence that there is a state law, court order, or other legally binding document, which prohibits this right.
- Notice to Minor and Incapacitated Persons. Before requesting private data from a minor or incapacitated person, City staff shall notify the minor or incapacitated person that he or she may request that the data not be given to a Parent (as defined above). This notice should be in the form attached as Exhibit 6.
- Denial of Parental/Guardian Access. The Responsible Authority or Designee may deny a Parent access to private data when the individual requests this denial and the Responsible Authority or Designee 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 or Designee will consider:
 - Whether the individual is of sufficient age and maturity to explain the reasons and understand the consequences,
 - Whether denying access may protect the individual from physical or emotional harm,
 - Whether there are reasonable grounds to support the individual’s reasons, and
 - 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 would seriously jeopardize the health of the individual.

The Responsible Authority or Designee may also deny access to a Parent without a request from the minor or incapacitated person under Minnesota Statutes, Section 144.335.

- Parents’ Access to Educational Records. In accordance with Minnesota Rules Part 1205.0500, the Responsible Authority shall not deny access to parents to data that is considered an “education record,”

as that term is defined in the Code of Federal Regulations, Title 45, Part 99, Section 99.3, unless the minor to whom that data pertains is enrolled as a full-time student in a postsecondary educational institution or the student has attained the age of 18.

6. 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 private and confidential data maintained by the City is contained in Exhibit 2. 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 (10) years after the death of the data subject and thirty (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 ninety (90) years elapsed since the creation of the data or ninety (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.

A. People Entitled to Access.

- **Public data** about a decedent may be shown or given to anyone for any reason.
- **Private data** about a decedent may be shown or given to:
 - The representative of the decedent, but only once every six (6) months, unless a dispute has arisen or additional data has been collected. 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 of the personal representative, the surviving spouse, any child of the decedent, or, if there is no surviving spouse or children, the parents of the decedent.
 - 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.
 - A person authorized to have access by federal, state, or local law or court order.
 - A person 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 Tennessee warning described below.
 - A person who is a member of the City staff, the City Council, or outside agents (such as attorneys) whose work assignment or responsibility reasonably requires access.
- **Confidential data** may not be given to the legal representative of the decedent, but may be given or shown to:
 - A person authorized to have access by federal, state, or local law or court order.
 - A person who is a member of the City staff, the City Council, or outside agents (such as attorneys) whose work assignment or responsibility reasonably requires access.

B. Form of Request. Any request to view or receive copies of private or confidential data on an individual must be in writing. Such 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. If a representative of the decedent is making the request, the requestor can use the written request form attached to the Guide for Members of the Public Requesting Government Data. In this circumstance, however, the representative of the decedent shall note his or her authority on the written request form and sign as the representative of the decedent. The Responsible Authority shall document the identity and authority of the representative of the decedent, the data requested, and the City's response.

C. Identification of Requesting Party. The Responsible Authority or Designee must verify the identity of the requesting party as a person entitled to access when private or confidential data is requested for a decedent. 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.

D. Time Limits.

- Requests. Requests will be received and processed only during normal business hours.
- Response. The response will be as soon as reasonably possible.

E. Fees. Fees may be charged in the same manner as for public data.

F. Summary Data. Summary data is handled as described in Section 5.F. above.

7. 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 data, except for security data, becomes public either ten (10) years after it was created by the City or ten (10) years after the data was received or collected by the City unless the Responsible Authority reasonably determines that, if the data was made available to the public, or to the data subject, that the harm to the public or to the data subject would outweigh the benefit to the public or the data subject.

A. People Entitled to Access.

- **Public data** not about an individual may be shown or given to anyone for any reason. Copyrighted documents will not be reproduced or photocopied without express written permission from the copyright holder.
- **Nonpublic data** not about an individual may be shown or given to:
 - The legal representative of the subject entity of the data, but only once every six (6) months, unless a dispute has arisen or additional data has been collected.
 - A person who has been given access by the express written consent of the legal representative of the entity which is the subject of the data.
 - A person authorized to have access by the federal, state, or local law or court order.
 - A person 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 Tennessee warning described below.
 - A person who is member of the City staff, the City Council, or outside agents (such as attorneys) whose work assignment or responsibility reasonably requires access.
- **Protected nonpublic data** may not be given to the legal representative of the subject entity, but may be given or shown to:
 - A person authorized to have access by federal, state, or local law or court order.
 - A person who is a member of the City staff, the City Council, or outside agents (such as attorneys) whose work assignment or responsibility reasonably requires access.

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

C. Identification of Requesting Party. The Responsible Authority or Designee must verify the identity of the requesting party as a person entitled to access when nonpublic 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, nonpublic, 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.

D. Time Limits.

- Requests. Requests will be received and processed only during normal business hours.
- Response. The response will be as soon as reasonably possible.

E. Fees. Fees may be charged in the same manner as for public data.

F. Summary Data. Summary data is handled as described in Section 5.F. above.

8. Temporary Classification. If the Responsible Authority determines data not expressly classified by law should be protected, that person may apply to the Commissioner for permission to classify data 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 data shall be in accordance with Minnesota Statutes, Section 13.06, as amended.

9. Denial of Access. If the Responsible Authority or Designee determines that the requested data is not accessible to the requesting party, the Responsible Authority or Designee must inform the requesting party orally at the time of the request or in writing as soon after that as possible. The Responsible Authority or Designee must give the specific legal authority, including statutory section, for withholding the data. The Responsible Authority or Designee must place an oral denial in writing upon request, which writing must include the specific legal authority for the denial.

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

A. Tennesen 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 Tennesen warning. This warning must contain the following:

- The purpose and intended use of the requested data;
- Whether the individual may refuse or is legally required to supply the requested data;
- Any known consequences from supplying or refusing to supply the information; and
- The identity of other persons or entities authorized by state or federal law to receive the data.

A Tennesen warning is not required when:

- An individual is requested to supply investigative data to a law enforcement officer;
- The data subject is not an individual (e.g., the data subject is a corporation or partnership);
- The data subject offer information that has not been requested by the City;
- The information requested from the individual is about someone else; or
- The information requested from the subject is classified as public data.

A Tennesen warning may be on a separate form or may be incorporated into the form which requests the private or confidential data. See attached Exhibit 10.

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

- At the time that the 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.
- An individual data subject should be encouraged to review his/her file for accuracy, completeness and to ensure that all information is current.
- Whenever possible and practical, City employees shall 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.)

- 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.
- 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.
- Department Heads should periodically conduct quality/validity checks on sample case files that contain data on individuals.

11. 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. The individual must notify the Responsible Authority in writing describing the nature of the disagreement. Within thirty (30) days, the Responsible Authority 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.

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

12. Data Protection.

A. Accuracy, Currency and Security of Data.

- Department Heads should, on an annual basis, 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 State of Minnesota General Records Retention Schedule.
- At least annually, each government entity shall conduct a comprehensive security assessment of any personal information maintained by the government entity.

B. Data Safeguards.

- Private and confidential data will be stored in files or databases which are not readily accessible to individuals who do not have authorized access and which will be secured during hours when the offices are closed.
- Private and confidential data must be kept only in City offices, except when necessary for City business (e.g. data provided to the City Attorney).
- Only those employees whose job responsibilities require them to have access will be allowed access to files and records that contain private or confidential data. These employees will be instructed to:
 - Not discuss, disclose, or otherwise release private or confidential data to anyone who is not authorized to access the data including City employees whose job responsibilities do not require access to the data,
 - Not leave private or confidential data where non-authorized individuals might see it, and
 - Shred private or confidential data before discarding.
- When a contract with an outside party requires access to private or confidential data, the contracting party will be required to use and disseminate the data consistent with the Act. The City may include in a written contract the language contained in Exhibit 11.

C. Disclosure of Breach in Security.

- "Breach of the Security of the Data" is defined by Minnesota Statutes Section 13.055, Subdivision 1.
- Notice to Individuals: A government entity that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach. Written notification must be made to any individual who is the subject of the data and must inform the individual that a report will be prepared, how the individual may obtain access to

the report and that the individual may request delivery of the report by mail or e-mail. Method of notice shall be in accordance with Minnesota Statutes Section 13.055, Subdivision 4.

- Investigative Report: Upon completion of an investigation into any Breach of the Security of Data and final disposition of any disciplinary action, the Responsible Authority shall prepare a report on the facts and results of the investigation. If the breach involves unauthorized access to or acquisition of data by an employee, contractor, or agent of the government entity, the report must at a minimum include:
 - A description of the type of data that were accessed or acquired;
 - The number of individuals whose data was improperly accessed or acquired;
 - If there has been a final disposition of disciplinary action for purposes of Minnesota Statutes Section 13.43, the name of each employee determined to be responsible for the unauthorized access or acquisition; and
 - The final disposition of any disciplinary action taken against each employee in response.

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 1

Responsible Authority, Data Practices Compliance Officer and Designees

Responsible Authority

Elise Durbin, Assistant City Administrator
City of Chaska 1 City Hall Plaza
Chaska, MN 55318
Phone: (952) 227-7539
Fax: (952) 448-9300

Positions appointed as Designees in system administration are as follows:

Designee

Denise Beebe, City Clerk
City of Chaska
1 City Hall Plaza
Chaska, MN 55318
Phone: (952) 227-7511
FAX: (952) 448-9300

Data Practices Compliance Official

Elise Durbin, Assistant City Administrator
City of Chaska
1 City Hall Plaza
Chaska, MN 55318
Phone: (952) 227-7539
Fax: (952) 448-9300

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 2

PRIVATE AND CONFIDENTIAL DATA MAINTAINED BY THE CITY OF CHASKA

1. PERSONNEL DATA (PRIVATE)

Minn. Stat. § 13.43

Generally all data about people who are or were an employee, applicant for employment, volunteer, independent contractor, or member of or applicant for a board or commission is private, with the exceptions noted below.

Public Data – Applicants

The following data on current and former applicants is public:

- Veteran status
- Relevant test scores
- Rank on eligible 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 and addresses of applicants for and members of an advisory board or commission

Public Data – Employees

The following data on current and former employees, volunteers, independent contractors, and members of advisory boards and commissions are public:

- Name
- Actual gross salary
- Salary range
- Contract fees
- Actual gross pension
- Value and nature of employer paid fringe benefits
- Basis for and 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 or not the complaint or charge resulted in disciplinary action
- Final disposition of any disciplinary action, with specific reasons for the action and date documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body
- Complete 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 award received
- Payroll time sheets or 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

Harassment

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 this would threaten the personal safety of the complainant or witness, or subject them to harassment. However, this data will be provided to the employee in order for him/her to prepare for a disciplinary proceeding that has been initiated.

Peer Counseling Debriefing

Data acquired by a peer group member in a public safety peer counseling debriefing is private data on the person being debriefed.

Protection of Employee or Others

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, data 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 pre-petition screening team in the commitment process, and (3) a court, law enforcement agency or prosecuting authority.

2. APPLICANTS TO A PUBLIC BODY

Minn. Stat. § 13.601

Generally, all data about people who are or were an applicant to or an appointed member of a public body is private, with the exceptions noted below. The following data on applicants to members of a public body are public:

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

3. APPOINTED (NOT ELECTED) MEMBERS TO A PUBLIC BODY

Minn. Stat. § 13.601

Generally, all data about people who are or were appointed, not elected, to a public body is private, with the exceptions noted below. The following data on applicants to members of a public body 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
- First and last dates of service on the public body
- The existence and status of any complaints or charges against an appointee
- Upon completion of an investigation of a complaint or charge against an appointee, the final investigative report is public, unless access would jeopardize an active investigation

4. PROPERTY COMPLAINT DATA (CONFIDENTIAL)

Minn. Stat. § 13.44

The identities of individuals who register complaints concerning violations of state laws or local ordinances concerning the use of real property (nuisance complaints).

5. PLANNING QUESTIONNAIRES (PRIVATE)

Minn. Stat. § 13.59

Names, addresses, and legal descriptions of property, that are collected in questionnaires or surveys of individuals and businesses for the purposes of planning, development, or redevelopment.

6. SECURITY INFORMATION (NONPUBLIC/PRIVATE)

Minn. Stat. § 13.37

Data which 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. This includes checking account numbers, crime prevention block maps and lists of volunteers who participate in community crime prevention programs and their home addresses and telephone numbers, but these may be disseminated to other volunteers participating in crime prevention programs, telephone numbers, e-mail or other digital addresses, Internet communication services accounts information or similar accounts information.

7. SEALED BIDS (NONPUBLIC)

Minn. Stat. § 13.37

Sealed bids, including the number of bids received, prior to opening.

8. LABOR RELATIONS INFORMATION (NONPUBLIC)

Minn. Stat. § 13.37

Management positions on economic and non-economic items that have not been presented during the collective bargaining process or interest arbitration, including data collected or created to prepare the management position.

9. EXAMINATION DATA (NONPUBLIC)

Minn. Stat. § 13.34

Completed versions of personnel and licensing examinations shall be accessible to the individuals who completed the examination, unless the Responsible Authority determines that access would compromise the objectivity, fairness, or integrity of the examination process.

10. ELECTED OFFICIALS CORRESPONDENCE (PRIVATE)

Minn. Stat. § 13.601

Correspondence between individuals and elected officials is private data on individuals, but may be made public by either the sender or the recipient.

11. CIVIL INVESTIGATIVE DATA (PRIVATE)

Minn. Stat. § 13.39

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 is **protected nonpublic**, except that a complainant's statement is **private**.

12. APPRAISAL DATA (PRIVATE/CONFIDENTIAL)

Minn. Stat. § 13.44

Appraisals made for the purpose of selling or acquiring land.

13. ASSESSOR'S DATA (PRIVATE)

Minn. Stat. § 13.51

Data on sales sheets from private multiple listing service organizations

Income data on individuals used to determine eligibility of property for classification 4d under Minn. Stat. § 273.13 and 273.126.

The following data regarding income producing properties:

- Detailed income and expense figures,
- Average vacancy factors,
- Verified net rentable or useable areas,
- Anticipated income and expenses,
- Projected vacancy factor, and
- Lease data

14. SOCIAL SECURITY NUMBERS (PRIVATE)

Minn. Stat. §13.355

Social Security Numbers collected in whole or in part are Private Data on Individuals.

15. TRANSPORTATION SERVICE DATA (PRIVATE)

Minn. Stat. § 13.72

Personal, medical, financial, familial or location data, except name, of applicants or users of transportation services for the disabled or elderly.

16. SOCIAL RECREATIONAL DATA (PRIVATE)

Minn. Stat. § 13.548

For people enrolling in recreational or other social programs: name, address, telephone number, any other data that identify 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.

17. LAW ENFORCEMENT DATA

Minn. Stat. § 13.80, 13.82

Data collected under the domestic abuse act is confidential.

The audio recording of a 911 call is private regarding the individual making the call, but written transcript is public. Certain arrest data, request for service data, and response or incident data is public under Minn. Stat. §13.82. Otherwise, investigative data collected to prepare a case against a person for the commission of a crime or civil wrong is confidential while the investigation is active. Photographs which are part of inactive investigation files are private if they are clearly offensive to common sensibilities. Booking photographs are public.

The identity of a victim of child abuse or neglect is private. The identity of a reporter of child abuse or neglect is confidential. Inactive investigative data which relates to the alleged abuse or neglect of a child by a person responsible for the child's care is private.

Videotapes of child abuse victims may not be released under any circumstances without a court order.

The following are private:

- The identity of undercover law enforcement officers
- The identity of criminal sexual conduct victims
- The identity of certain informants
- The identity of victims, witnesses, people making a 911 call whose personal safety or property would be threatened by disclosure
- The identity of a person making a 911 call to receive help in a mental health emergency

Unique descriptions of stolen, lost, confiscated, or recovered property are private.

Identities of customers of licensed pawnshops and secondhand goods dealers are private.

Detention data which would disclose personal, medical, psychological or financial data or endanger an individual's life is private (Minn. Stat. § 13.85).

Criminal history data is private, except convictions of crimes within the past 15 years (Minn. Stat. § 13.87).

Deliberative processes or investigative techniques are confidential.

18. CITY ATTORNEY RECORDS (CONFIDENTIAL)

Minn. Stat. § 13.393

Statutes, rules, and professional standards concerning discovery, production of documents, introduction of evidence, and professional responsibility govern the use, collection, storage, and dissemination of data by the City attorney.

19. COUNCIL MEETINGS HAVING DATA CLASSIFIED AS NONPUBLIC

Minn. Stat. § 13D.05

Any portion of a meeting must be closed if expressly required by other law or if the following types of data are discussed:

1. data that would identify alleged victims or reporters of criminal sexual conduct, domestic abuse, or maltreatment of minors or vulnerable adults;

2. active investigative data as defined in Section 13.82, subdivision 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
3. educational data, health data, medical data, welfare data, or mental health data that are not public data under Section 13.32, 13.3805, subdivision 1, 13.384, or 13.46, subdivision 2 or 7.

20. AUDITING DATA (CONFIDENTIAL/PROTECTED NONPUBLIC) Minn. Stat. § 13.392

Data, notes, and preliminary drafts of audit reports are confidential or protected nonpublic until the final report has been published or the audit or investigation is no longer being pursued actively.

21. DRUG AND ALCOHOL TEST RESULTS (PRIVATE) Minn. Stat. § 181.954

With respect to public sector employees and job applicants, the results of drug or alcohol tests are Private Data on Individuals.

22. BENEFITS DATA (PRIVATE) Minn. Stat. § 14.362

Information on individuals regarding benefits/services under various housing, home ownership, rehabilitation and communication action agencies, Head Start and food assistance programs.

23. EMPLOYMENT AND TRAINING DATA Minn. Stat. § 13.47

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, including those provided under the Workforce Investment Act of 1998, United States Code, title 29, section 2801.

24. AWARD DATA Minn. Stat. § 13.48

Financial data on business entities submitted to a government entity for purposes of presenting businesses with awards.

25. DEFERRED ASSESSMENT DATA (PRIVATE) Minn. Stat. § 13.52

Data which indicates amount or location of cash or other valuables kept in homes of applicants for deferred assessment.

26. RETIREMENT DATA (PRIVATE) Minn. Stat. § 13.63

Information regarding PERA information on beneficiaries.

27. MUNICIPAL UTILITY CUSTOMER DATA (PRIVATE)

Minn. Stat. § 13.685

Data on customers of municipal electric utilities are private data on individuals or nonpublic data, but may be released to:

- (1) a law enforcement agency that requests access to the data in connection with an investigation;
- (2) a school for purposes of compiling pupil census data;
- (3) the Metropolitan Counsel for use in studies or analyses required by law;
- (4) a public child support authority for purposes of establishing or enforcing child support; or
- (5) a person where use of the data directly advances the general welfare, health, or safety of the public; the commissioner of administration may issue advisory opinions construing this clause pursuant to section 13.072.

28. FEDERAL CONTRACTS DATA (PRIVATE/NONPUBLIC)

Minn. Stat. § 13.35

To the extent that a federal agency requires it as a condition for contracting with a government entity, all government data collected and maintained by the government entity because that agency contracts with the federal agency are classified as either private or nonpublic depending on whether the data are data on individuals or data not on individuals.

29. TRADE SECRET INFORMATION (PRIVATE)

Minn. Stat. § 13.37

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.

30. LIBRARY AND HISTORICAL DATA (PRIVATE)

Minn. Stat. § 13.40

Data that links patrons with materials requested.

31. LICENSING DATA (PRIVATE/CONFIDENTIAL)

Minn. Stat. § 13.41

Data regarding individuals applying for licenses and investigation of said licenses.

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 3

DATA REQUEST COST CALCULATION FORM

Fees charged are in accordance with MN Statutes Section 13.03 (3).

Date of Request: _____

Description of data requested: (Please be specific)

Costs for duplication of standard materials are included on Exhibit 3. Please use this section to calculate fees for other data requests.

		Estimated Cost	Actual Cost
A.	LABOR		
	_____ x _____		
	# Hours Hourly Rate		
	_____ x _____		
	# Hours Hourly Rate		
B.	PHOTOCOPY		
	_____ x _____		
	Rate # of Pages		
C.	MAILING		

D.	PRINTING COSTS:		

E.	OTHER COSTS: (May include computer time, programming, terminal access, microfilming, and any other costs not listed above.)		
	1. _____		
	2. _____		
	3. _____		
	4. _____		
	TOTAL CHARGES		
	AMOUNT TO BE PREPAID		
	(50% of est. total if exceeds \$50)		
	AMOUNT DUE UPON COMPLETION		

Prepared by: _____

Department: _____ Date: _____

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 4

SUMMARY DATA REQUEST

Request for Private Data without Data Subject Identification

Notice: *Within ten (10) days of the receipt of this request, you will receive an estimate of charges and time required to prepare the summary data. The City of Chaska must be reimbursed for these costs. You may be required to pay these charges before the data will be prepared.*

Completed by Requester

Name (Last, First, MI)	Date of Request
Street Address	Phone Number
E-mail Address	
City, State, ZIP	

You do not have to provide contact information to view or obtain public data. However, if you want us to mail you copies of data, we will need some type of contact information. In addition, if we do not understand your request and need to get clarification from you, without contact information we will not be able to begin processing your request until you contact us.

Description of the data requested: (attach additional sheets if necessary)

Completed by the City of Chaska

Preparation Charges:	Estimated	Actual
A. Labor		
Rate per hour * X Hours =	_____	_____
Rate per hour * X Hours =	_____	_____
B. Photocopies: Rate per Page .25 x Pages =	_____	_____
C. Mailing: _____ =	_____	_____
D. Printing: _____ =	_____	_____
E. Other: <i>Include computer time, programming time, terminal access, etc.</i>		
1. _____	_____	_____
2. _____	_____	_____
3. _____	_____	_____
4. _____	_____	_____
Total Charges =	_____	_____

* See rate in Chapter 1100 of the Carver City Code

Action: Approved Approved in part (explain below) Denied (explain below)

Handled by _____

Authorized Signature _____

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 5

GOVERNMENT DATA ACCESS AND NONDISCLOSURE AGREEMENT

1. **AUTHORIZATION.** The City of Chaska (“City”) hereby authorizes _____,
“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 which applies):

- The Authorized Party 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 determined to be \$_____.
- The Authorized Party has been requested by the City to prepare summary data and will be paid in accordance with the attached Exhibit 2 and Exhibit 3.

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, 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. This Agreement is subject to Minn. Stat. §13.05, subd. 11.

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:

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 officers and employees harmless from any liability, claims, damages, costs, judgments, or expenses, including reasonable attorneys' fees, resulting directly or indirectly from an act or omission of the Authorized Party, its agents, employees or assignees under this Agreement and against all loss by reason 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 \$1,000,000 per claimant for personal injuries and/or damages and \$1,000,000 per occurrence. The policy must cover the indemnification obligation specified above.

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

8. **ACCESS RESULTS.** (Check which applies):
_____ If the Authorized Party is the Requester, a copy of all reports, summaries, compilations, articles, publications or any document or series of documents that are created from the data provided under this Agreement must be made available to the City in its entirety.

_____ If the Authorized Party is a Contractor of the City, all copies of reports, summaries, compilations, articles, publications or any document or series of documents that are created from the data provided under this Agreement must be provided to the City. The Authorized Party may retain one (1) copy 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 CHASKA:

By: _____ Date: _____

Its: _____

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 6

NOTICE TO PERSONS UNDER AGE 18

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

Your request does not automatically mean that the data 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 is 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 data:

Be withheld from: _____

For these reasons:

Date: _____ Print Name: _____

Signature: _____

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 7

CONSENT TO RELEASE PRIVATE DATA

I, _____, authorize the City of Chaska to release the following private data about me:

To the following person or people:

The person or people receiving the private data may use it only for the purpose or purposes of:

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 data being released and that in any event, this consent expires automatically ninety (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: _____

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 8

CONSENT TO RELEASE COPYRIGHTED DATA

I, _____, certify that I have the authority to authorize the City of Chaska 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 (1) 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.

Print Name Title

Complete Address Street City State ZIP

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: _____

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 9

DATA PRACTICES ADVISORY

(Tennessee Warning)

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

Our purpose and intended use of this data is:

You _____ ARE _____ ARE NOT legally required to provide this data.

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

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

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 10

SAMPLE TENNESSEN WARNING

It is the City of Chaska's responsibility to inform potential employees of their privacy rights. Please carefully read the Tennesen Warning provided below. Sign and date the form and return it with your application. Your signature indicates that you have received data 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 Chaska is required to inform you of your rights as they relate to the private data collected from you. Private data is data that is available to you, but not to the public; the personal information we collect about you is private. Minnesota Statutes 13.04 and 13.43 are two sections that govern what affects you as an applicant for employment at the City of Chaska. All data collected is considered private except for the following:

- Veteran status
- Relevant test scores
- Rank on eligibility list
- Job history
- Education and training
- Work availability

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

The data supplied by you may be used for such other purposes as may be determined to be necessary in the administration of personnel procedures, rules, and regulations of the City of Chaska. Furnishing social security numbers is voluntary for applicants to the City of Chaska, 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 Chaska in determining your suitability for the position for which you are applying.

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

Applicant Signature

Date

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 11

SAMPLE CONTRACT PROVISION

Data Practices Compliance. Contractor will have access to data collected or maintained by the City only to the extent necessary to perform Contractor's obligation under this contract. Contractor agrees to maintain all data obtained from the City or produced for the City in the same manner as the City is required to maintain data under the Minnesota Government Data Practices Act, Minn. Stat. Chap. 13 (the "Act"), specifically Minn. Stat. §13.05, subd. 11. Contractor agrees to defend and indemnify the City from any claim, liability, damage or loss asserted against the City as a result of Contractor's failure to comply with the requirements of the Act or this contract. Upon termination of this contract, Contractor agrees to return data to the City, as requested by the City.

CITY OF CHASKA DATA PRACTICES POLICIES

Exhibit 12

BUILDING PERMIT DATA PRACTICES ADVISORY

You may be required to submit building plans with your building permit application so that the City of Chaska 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, state statute, or 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 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 of Chaska are generally public data and will be presumed to be available for copying and release to the public. **If you hold a copyright to the plans and do not want them copied for the public, you will need to indicate as such below.** Also, if you believe that your building plans qualify for the classification of nonpublic data, you must provide documentation verifying your claim. The Responsible Authority for the City of Chaska will determine whether or not the plans qualify for nonpublic data classification within ten (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 State of Minnesota Commissioner of the Department of Administration who will either grant or disapprove of the application within forty-five (45) days after it has been filed with the Office of the Administration.

Building Permit Data Advisory

Building plans and related documents submitted to the City of Chaska are presumed to be public. 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 data under Minnesota law and may be viewed by the public.

- The building plans I have submitted contain **TRADE SECRET INFORMATION** as defined by Minnesota Statutes Section 13.36, 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 data under law.

- The building plans I have submitted contain **SECURITY INFORMATION** as defined by Minnesota Statutes Section 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 data under law.

Explanation:

Name of Applicant (Please Print)

Date

Signature of Applicant

Property Address

Contact Address

Contact Phone

E-mail Address