

MINNESOTA GOVERNMENT DATA PRACTICES POLICY



229 Broadway St E, Rockville, MN 56369

320-251-5836

www.rockvillecity.org

INTRODUCTION

This Data Practices Policy ("Policy") contains the procedures and forms adopted by the City of Rockville ("City") to comply with the requirements of the Minnesota Government Data Practices Act ("MGDPA"), set forth in Minn. Stat. § 13.01 et seq.

I. **RESPONSIBLE AUTHORITY AND COMPLIANCE OFFICIAL; DESIGNEES.**

The City Council has appointed the City Administrator, as the Responsible Authority and Compliance Official for purposes of the MGDPA. The Responsible Authority and Compliance Official has designated the Fire Chief and the Utility Billing Clerk, to assist in complying with the MGDPA to whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices concerns. The phrase "Responsible Authority or a designee" used in this Policy means the person responding to a MGDPA request for the City.

II. **GOVERNMENT DATA GENERALLY IS ACCESSIBLE TO THE PUBLIC.**

"Government Data" means all data collected, created, received, maintained or disseminated by the City regardless of its physical form, storage media or conditions of use. Government Data is public data and is generally accessible by the public according to the terms of the MGDPA, unless it is specifically classified differently by the MGDPA or other law, and may be subject to a fee (see § V in this Policy). The MGDPA classifies categories of Government Data that *are not generally accessible to the public* as follows:

- a. "**Confidential data on individuals**" is inaccessible to the public or to the individual subject of the data.
- b. "**Private data on individuals**" is inaccessible to the public, but is accessible to the individual subject of the data.
- c. "**Protected nonpublic data**" is data *not on individuals* that is inaccessible to the public or the subject of the data, if any.
- d. "**Nonpublic data**" is data *not on individuals* that is inaccessible to the public, but accessible to the subject of the data, if any.

If data is determined to be inaccessible to the requesting party, see § IV in this Policy.

III. **ACCESS PROCEDURES.** Procedures for responding to requests for access to Government Data vary depending on the classification of the data requested and the person making the request. The Responsible Authority or a designee:

- (1) Must determine whether the City maintains the data requested. The City is not required to provide data it does not maintain or to produce data in a new format.
- (2) Must determine the statutory category of data requested in order to respond appropriately according to MGDPA requirements. Classifications for "not public data" (data classified as private, confidential, or nonpublic data) under Minn. Stat. § 13.02, subd. 8a. maintained by the City are attached to this Policy as Exhibit A, and responses should follow the protocol below depending on the category of data.
 - a. **Public data.** All Government Data is public data unless it is specifically given a different classification by statute or law.

- i. **Who can access the data?** Any person has the right to inspect and copy public data and receive an explanation of its meaning. The person is not required to provide identification or a reason for the request.
 - ii. **How can the data be accessed?** Requests for Public Data may be oral or written. Written requests should utilize the Data Disclosure Request form (see Exhibit B). The City should consult with legal counsel on any request related to litigation. If clarification of an oral request is required in order to respond, the representative may use the Data Disclosure Form. For handling of requests for “summary data,” see iv. below.
 - iii. **When must accessible data be provided?** Requests will be received and processed during normal business hours and the information supplied as soon as reasonably possible.
 - iv. **Summary Data.** “Summary data” means statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable. Unless otherwise classified by MGDPA, another statute, or federal law, summary data is public and must be provided on written request. Summary data is subject to the following procedures: (1) the Responsible Authority or a designee must prepare summary data by redacting, by any reasonable means, data that identifies any individual; (2) the Responsible Authority or a designee must inform the requesting party of the approximate timeframe for preparing the summary data and the reason for any delay; (3) all costs for preparation must be paid by the requesting party. The Responsible Authority may authorize an outside agency or person to prepare summary data if (1) the specific purpose is given in writing; (2) the outside agency or person agrees not to disclose the private or confidential data; and (3) the Responsible Authority determines that access by the outside agency or person will not compromise the privacy or confidentiality of the data (see Exhibit E).
- b. **Confidential and Protected nonpublic data.**
- i. **Who can access the data?** Data within these two classifications is *not accessible* and should not be provided to members of the general public (even if the requestor is the subject of the data) under any circumstances. Confidential data may be provided only to the following: (1) persons authorized by federal, state, or local law or court order whose identity is disclosed in a valid *Tennessee* Warning (see Exhibit C) or (2) City staff, City Council members, or outside agents (e.g. attorneys) whose work assignments or responsibilities reasonably require access.
 - ii. **How can the data be accessed?** In limited cases where such data is accessible, a written request is required unless waived by the Responsible Authority or a designee.
 - iii. **When must accessible data be provided?** Requests will be received and processed during normal business hours and the information supplied as soon as reasonably possible.
- c. **Private data on individuals and Nonpublic data**

- i. **Who can access the data?** Private data on individuals and nonpublic data may be accessed only by (1) the subject of the data; (2) a person given access by written consent of the subject of the data (see Exhibit D); (3) persons authorized by federal, state, or local law or court order whose identity is disclosed in a valid *Tennessean* Warning or (4) City staff, City Council members, or outside agents (e.g. attorneys) whose work assignments or responsibilities reasonably require access. Private data on individuals relating to juveniles is subject to special handling (see iv. below); as is Trade Secret and Security Information as determined by the Responsible Authority (see § VII, d).
- ii. **How can the data be accessed?** All requests for private data on individuals and nonpublic data must be in writing on a Data Disclosure Request form (see Exhibit A) unless waived by the Responsible Authority or a designee. The Responsible Authority or a designee must verify the identification of the requestor through personal knowledge, presentation of written identification, or other reasonable means. The City should consult with legal counsel on any request related to litigation.
- iii. **When must accessible data be provided?** Requests will be received and processed during normal business hours. The response must be provided immediately or, in the event an immediate response is not possible, within ten working days. After an individual has been shown the private data and informed of its meaning, the data need not be disclosed to that individual again *for six months* unless a dispute or action pursuant to MGDPA requirements arises or additional data on that individual is collected.
- iv. **Data on juveniles.** Private data on individuals under the age of 18 is subject to special handling.
 1. **Notice to juvenile subject of data.** When requesting private data on individuals from juvenile subjects, the Responsible Authority or a designee must notify the subject of the data that the subject may request that the private data be withheld from the subject's parent or legal guardians, stating reasons for the request. See Exhibit F. This notice must be given in addition to a *Tennessean* Warning.
 2. **Parental Access.** In addition to the individuals listed in paragraph i., a parent or legal guardian, or an individual acting as a legal guardian in the absence of a parent or legal guardian, generally may access private data on individuals who are under the age of 18. This access is presumed unless (a) the Responsible Authority or a designee has evidence (in the form of a federal or state law, court order, or other legally binding document) that such access should be denied; or (b) the juvenile has requested that such access be denied and the Responsible Authority or a designee determines that access should be denied based on the following criteria: (i) the juvenile is of sufficient age and maturity to explain the reasons given for the denial and to understand the consequences, (ii) reasonable grounds support the reasons given, (iii) denial of access may prevent physical or emotional harm to the juvenile, (iv) the data involves medical, dental or other health services

provided under Minn. Stat. § 144.341 et seq., in which case the data may be released only if the failure to disclose the data to the parent or legal guardian would seriously jeopardize the health of the juvenile.

IV. **DENIAL OF ACCESS TO DATA.** In the event the Responsible Authority or a designee determines that requested data, of whatever classification, is not accessible to the requesting party, the Responsible Authority or a designee must inform the requesting party orally at the time of the request or in writing as soon thereafter as possible. A denial must be given in writing, including the specific legal authority for the denial, on request of the party requesting data.

V. **FEES**

- a. **Data separation must be completed free of charge.** The City cannot charge a fee for the time it takes to separate Public Data from Private, Nonpublic, or Confidential Data.
- b. **Inspection is available free of charge.** The City cannot charge a fee for the inspection of Government Data. Inspection includes individuals' ability, through their own devices, to photograph or "copy" a document without removing it from City offices or damaging or defacing it in any manner.
- c. **Fees for copies and transmission.** If, either before or after inspection, a requesting party wishes to have Government Data reproduced and/or transmitted to any location outside of City offices, the City charges fees for that service as permitted by the MGDPA. The City Council will determine annually, through ordinance, charges for copies.

The *actual cost* of copies includes the cost of searching for and retrieving the data, including the cost of employee time, and for making, certifying, and electronically transmitting copies of the data and/or mailing copies of the data and other production expenses (e.g. microfilm, recording systems, or use of computers) as requested.

- i. **Data with Commercial Value.** If a request involves copies of Government Data that have commercial value and is a substantial or discreet portion of an entire pattern, program, device, method, technique, process, data base, or was otherwise developed by the City with significant expenditure of public funds, the Responsible Authority shall determine a reasonable fee to be charged in addition to other fees for copies and transmission. Upon written request, the City Council will determine annually, through ordinance, charges for copies.
- ii. **All other copies.** For other than single-sided, black and white, letter or legal size documents, the charge will be the actual cost of copying as defined herein. The City Council will determine annually, through ordinance, charges for copies.
- iii. **City may require Prepayment.** The City, in the discretion of the Responsible Authority or a designee, may require the requesting party to prepay any fees associated with a request for copies or transmission.

VI. **DATA COLLECTION.** Collection and storage of data on individuals is limited to that which is necessary for the administration and management of programs specifically authorized by the City Council, state legislature, or federal government. When an individual is asked to provide that individual's private or confidential data, the Responsible Authority or a designee must give that individual a *Tennessean* warning as provided for by the city. Information that must be incorporated on forms used as a *Tennessean* warning is attached to this Policy as Exhibit C. A *Tennessean* warning is not required when a law enforcement officer requests data during an investigation.

VII. **DATA ACCURACY AND SECURITY SAFEGUARDS.**

- a. **Data Accuracy.** In order that Government Data be kept in the most accurate and current state practicable, the following guidelines should be followed:
 - i. All City employees must provide updated personal data to the City Administrator or Finance/Payroll Clerk for tax purposes, insurance coverage, emergency notifications, and other personnel-related reasons.
 - ii. Individuals providing private or confidential data should be encouraged to provide updated data as appropriate.
- b. **Challenges to Data Accuracy.** An individual who is the subject of Government Data may contest the accuracy or completeness of that data by notifying the Responsible Authority in writing describing the nature of the disagreement. Within thirty days, the Responsible Authority must review the data in question and respond by either (i) correcting data found to be inaccurate or incomplete and attempting to notify past recipients of the inaccurate or incomplete data, including recipients named by the individual; or (ii) notifying the individual that the Responsible Authority believes the data to be accurate. An individual who is dissatisfied with the Responsible Authority's response may appeal the matter to the Commissioner of the Department of Administration, utilizing the contested case procedures in Minn. Stat. Chap. 14.
- c. **Data Security**
 - i. City staff should pay careful attention to and abide by the City's Records Retention Schedule, disposing of records as appropriate.
 - ii. Private, nonpublic, and confidential data should be stored in secure files or databases which are not accessible to unauthorized personnel. The Responsible Authority or a designee should instruct authorized personnel to (1) not discuss, disclose or otherwise release private, nonpublic, or confidential data to personnel who are not authorized to access such data; (2) protect access to private, nonpublic, or confidential data in their possession; (3) shred private, nonpublic, or confidential data prior to discarding it or dispose of it in confidential locked recycling.
 - iii. Private, nonpublic, and confidential data should be kept within City offices at all times unless necessary for off-premises City business.
 - iv. Contracts with outside entities that involve the use or access to private, nonpublic, and confidential data must include language intended to insure compliance with MGDPA requirements (see Exhibit G).
- d. **Trade Secret and Security Information.** Trade Secret and Security Information (e.g. plans for alarm systems, vaults, sprinkler systems, security protocols) is Nonpublic Data. The Responsible Authority, in consultation with legal counsel as necessary, will

determine whether particular information qualifies as Trade Secret or Security Information according to the following definitions:

- i. "Trade Secret information" is government data that includes a formula, pattern, compilation, program, device, method, technique, or process that is (1) supplied by an individual or organization; (2) subject to efforts by the individual or organization to maintain secrecy of the information; and (3) derives independent actual or potential economic value by not being known to or accessible to the public through lawful means.
- ii. "Security information" is government data the disclosure of which would be likely to substantially jeopardize the security of the information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury. Security information includes crime prevention block maps and lists of volunteers who participate in community crime prevention programs and their home addresses and telephone numbers.

VIII. FORMS AND RESOURCES

Exhibit A	GOVERNMENT DATA CLASSIFIED AS NOT PUBLIC (PRIVATE, NONPUBLIC, OR CONFIDENTIAL)
Exhibit B	DATA DISCLOSURE REQUEST
Exhibit C	DATA PRACTICES ADVISORY (<i>TENNESSEN</i> WARNING)
Exhibit D	CONSENT TO RELEASE PRIVATE DATA
Exhibit E	GOVERNMENT DATA ACCESS AND NONDISCLOSURE AGREEMENT
Exhibit F	NOTICE TO PERSONS UNDER THE AGE OF 18
Exhibit G	SAMPLE PROVISION FOR CONTRACTS WITH OUTSIDE ENTITIES ACCESSING PRIVATE, NONPUBLIC, OR CONFIDENTIAL DATA

This policy has been adopted by the City Council of the City of Rockville this 15th day of Aug, 2012.

Mayor Jeff Hagen

Verena M. Weber
City Administrator

EXHIBIT A

GOVERNMENT DATA CLASSIFIED AS NOT PUBLIC (PRIVATE, NONPUBLIC, OR CONFIDENTIAL)

The following categories and summaries should serve as a guideline for responding to MGDPA requests. Specific questions should be directed to the City Attorneys office.

1. **Personnel Data (Private)** Minn. Stat. § 13.43

All data on all individuals who are or were an employee, volunteer, or independent contractor is Private Data on Individuals—except the following, which is Public Data:

Name
Actual gross salary
Salary range
Contract fees
Bargaining unit
Actual gross pension
Value and nature of employer paid fringe benefits
Basis for and amount of added remuneration, including expense reimbursement
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, whether or not resulting in discipline
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
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 medical leave or other not public data
Employee number

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

2. **Undercover Law Enforcement Officer Data (Private)** Minn. Stat. § 13.43, subd. 5

All data about an individual who is employed as, or is an applicant to be, an undercover law officer is Private Data on Individuals. When the individual is no longer assigned to an undercover position, the data is Personnel Data unless the law enforcement agency determines that revealing the data would threaten the personal safety of the officer or jeopardize an active investigation.

3. **Applicant Data (Private)** Minn. Stat. § 13.43, subd. 3

Data about current and former applicants for City employment is Private Data on Individuals—except the following, which is Public Data:

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)

4. **Applicants for Appointment to a Public Body (Private)** Minn. Stat. § 13.601

Data about applicants for appointment to a public body that are collected as a result of the applicant's application, including contact information, is Private Data on Individuals—except the following, which is Public Data:

Name

City of residence (unless the appointment has a residency requirement that requires the entire residence address to be public)

Education

Training

Employment history

Volunteer work

Awards and honors

Prior government service

Once an individual is appointed to a public body, the following additional data are public:

Residential Address

A telephone number or electronic mail address where the appointee can be reached, or both at the request of the appointee.

5. **Property Complaint Data (Confidential)** Minn. Stat. § 13.44

The identity of any individual who register complaints concerning violations of state laws or local ordinances concerning the use of real property is Confidential Data on Individuals.

6. **Security Information (Nonpublic)** Minn. Stat. § 13.37, subd. 1(a)

Government Data that, 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 Nonpublic. This includes 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. This also includes interior sketches, photos, or plans of buildings where detailed information about alarm systems or similar issues could jeopardize security.

The Responsible Authority must make a determination regarding all data to be classified as Nonpublic “Security Information.”

The location of a National Night Out event is Public Data.

7. **Trade Secret Information (Nonpublic)** Minn. Stat. § 13.37, subd. 1(b)

Government Data that includes a formula, pattern, compilation, program, device, method, technique, or process that is (1) supplied by an individual or organization; (2) subject to efforts by the individual or organization to maintain secrecy of the information; and (3) derives independent actual or potential economic value by not being known to or accessible to the public through lawful means is Nonpublic.

The Responsible Authority must make a determination regarding all data to be classified as Nonpublic “Trade Secret Information.”

8. **Registered Voter Lists and Absentee Ballots (Protected Nonpublic)**

Minn. Stat. §§ 13.37, 203B.12, and 201.091

Sealed absentee ballots before opening by an election judge are Protected Nonpublic. Names of voters submitting absentee ballots are Private until the close of voting.

Registered voter lists can only be used for elections, political activities, or law enforcement. The date of birth, portion of a Social Security number, driver’s license number or other identification card number on voter lists cannot be provided on any material available for public inspection.

9. **Labor Relations Information (Nonpublic/Protected Nonpublic)**

Minn. Stat. § 13.37, subd. 1(c)

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

10. **Examination Data (Private or Confidential)** Minn. Stat. § 13.34

Completed versions of personnel and licensing examinations are Private Data, unless the Responsible Authority determines that they should be Confidential because access would compromise the objectivity, fairness, or integrity of the examination process.

11. **Election Officials Correspondence (Private)** Minn. Stat. § 13.601

Correspondence between individuals and elected officials is Private Data, but may be made Public Data by either the author or any recipient.

12. **Housing Agency (HRA) Data (Nonpublic/ Private)** Minn. Stat. § 13.585

Data pertaining to negotiations with property owners regarding the purchase of the property are Nonpublic Data. Except the HRA's evaluation of properties that it does not purchase, all other negotiation data becomes Public Data at the time of the closing of the property sale.

Data pertaining to individuals' income collected for purposes of determining eligibility of property for classification 4d under Minn. Stat. §§ 273.128 and 273.13 is Private Data on Individuals. Such data may be disclosed to county and local assessors responsible for determining eligibility of property for classification 4d.

Law enforcement access to data may be subject to different regulation. Contact the City Attorneys' office for assistance in responding to any such requests.

13. **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 City, all government data collected and maintained by the City are classified as private or nonpublic.

14. **Civil Investigation Data (Confidential/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 confidential or nonpublic, except that a complainant's statement is private.

Contact the City Attorneys' office for assistance in responding to any such requests.

15. **Appraisal Data (Confidential/Protected Nonpublic/Public)**
Minn. Stat. § 13.44, subd. 3

Data on estimated or appraised values of real property made by or on behalf of the City for the purpose of selling or acquiring real property are Confidential or Protected Nonpublic Data.

Appraised values of real property obtained by owners who have received from the City an offer to purchase property are Private or Nonpublic Data.

All such data become Public Data when (1) submitted to a court-appointed condemnation commissioner; (2) submitted in court during condemnation proceedings; or (3) the parties enter into an agreement for the purchase and sale of the real property.

16. **Assessor's Data (Private/Nonpublic)** Minn. Stat. § 13.51

Data on sale sheets from private MLS organizations where the contract with the organization requires that the data not be made available to the public is Private Data.

The following income property data is Private Data or Nonpublic Data: (a) detailed income and expense figures; (b) average vacancy factors; (c) verified net rentable areas or net usable areas, whichever is appropriate; (d) anticipated income and expenses; (e) projected vacancy forms; and (f) lease information.

Income information on individuals collected for purposes of determining eligibility of property under class 4d (Minn. Stat. §§ 273.128 and 273.13) are Private Data.

Social Security Nos. and Federal Employer Identification Nos. on Certificates of Value, homestead applications, and other documents is Private Data.

17. **Transportation Service Data (Private)** Minn. Stat. § 13.72

Personal, medical, financial, familial or locational information, except the name, of applicants or users of transportation services for the disabled or elderly is Private Data.

18. **Social Recreational Data (Private)** Minn. Stat. § 13.548

The 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 individuals enrolling in recreational or social programs are Private Data.

19. **Law Enforcement and Investigative Data (Confidential/Protected Nonpublic/Private)** Minn. Stat. §§ 13.80, 13.82 and various other statutes

Data collected under Minn. Stat. § 518B.01 (Domestic Abuse Act) is Confidential until a temporary court order is executed or served on the respondent in the action.

Audio recordings of 911 calls are Private Data on Individuals with respect to the individual making the call, but a written transcript of the call is Public provided it does not reveal the identity of an individual subject to protection under Minn. Stat. § 13.82, subd. 17 (e.g. undercover law enforcement officer, victim of criminal sexual conduct, other crime victim or witness requesting anonymity).

Criminal investigative data during an active investigation is confidential or protected nonpublic. Data on inactive investigations, unless the release of the data would jeopardize an ongoing investigation or reveal the identity of an individual subject to protection under Minn. Stat. § 13.82, subd. 17, is public—with the exception of photographs that are clearly offensive to common sensibilities, which are private or nonpublic data, provided the existence of the photographs is disclosed to individuals requesting the inactive investigation file. An investigation is “inactive” when an agency or prosecuting authority decides not to pursue a case, when the statute of limitations (or thirty years after the offense, whichever comes first) expires, or upon the exhaustion of appeal rights of a person convicted on the basis of the investigative data.

A law enforcement agency can make investigative data public to aid law enforcement, promote public safety, or dispel unrest. Written requests to access data by victims of crimes or alleged crimes must be granted unless the authority reasonably believes that release of data will interfere with an investigation or the request is prompted by a desire by the requester to engage in unlawful behavior.

Investigations involving reports of child abuse or neglect or maltreatment of a vulnerable adult, either active or inactive, are Private Data on Individuals in cases where the alleged victim is identified. The identity of the reporter of child abuse or neglect is Confidential, unless compelled by law. The identity of the reporter of maltreatment of a vulnerable adult is Private Data on Individuals.

Data on court records relating to name changes is Confidential during an active investigation and Private Data on Individuals when an investigation is inactive.

Data that uniquely describes stolen, lost, confiscated, or recovered property are Private Data or Nonpublic Data.

Data that identifies customers of pawn shops, scrap metal dealers, or secondhand stores are Private Data on Individuals.

Deliberative process data or data revealing investigative techniques are Confidential.

Data presented as evidence in court is public. Arrest data (including booking photographs), requests for service data, and response or incident data is public.

20. **Human Rights Data (Confidential/Private)** Minn. Stat. §§ 13.552, 363A

Human rights investigative data are Confidential. The name and address of a charging party and respondent, factual basis of the allegations, and the statute under which the action is brought are Private Data on Individuals.

21. **Planning Survey Data (Private/Nonpublic)** Minn. Stat. § 13.59

The following data collected in surveys of individuals conducted by the City for the purpose of planning, development and redevelopment are classified as Private or Nonpublic: names

and addresses of individuals and the legal descriptions of property owned by the individuals, and the commercial use of the property to the extent disclosure of the use would identify a particular business.

22. **Data on Rentals (Private/Nonpublic)**

Intentionally omitted.

23. **City Attorney Data (Confidential) Minn. Stat. § 13.393**

The use, collection, storage, and dissemination of data by the city attorney is 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 or subject to protection as attorney work product is confidential.

24. **Business Data (Private/Nonpublic) Minn. Stat. § 13.591**

The following data submitted by a business requesting financial assistance, a license, or other benefit are Private or Nonpublic: financial information about the business, including credit reports, financial statements, net worth calculations, business plans, income and expense projections, balance sheets, customer lists, income tax returns, and design, market, and feasibility studies not paid for with public funds. This data becomes public when assistance, a license, or other benefits are granted, except the following, which remain Private or Nonpublic: 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.

25. **Proposals and Bids (Private/Nonpublic) Minn. Stat. § 13.591**

Proposals submitted in response to a Request for Proposals are Private or Nonpublic Data until the responses are opened. Once opened, the name becomes Public, but all other data remain Private or Nonpublic until completion of the selection process. After the process is completed, all remaining data are Public with the exception of trade secret data.

Data submitted by a business in response to a Request for Bids are Private or Nonpublic Data until the bids are opened. Once opened, the name of the bidder and the dollar amount specified in the response become Public Data. All other data in a bidder's response to a bid are Private or Nonpublic data until the completion of the selection process. After the process is completed, all remaining data are Public with the exception of trade secret data.

In the event that all responses to a Request for Proposals or a Request for Bids are rejected, information that was Private or Nonpublic remains that way until a resolicitation of bids results in completion of the selection process or the process is abandoned. If resolicitation does not occur within one year, the remaining data become Public.

26. **Municipal Obligation Registers (Private/Nonpublic) Minn. Stat. § 475.55**

Information with respect to the ownership of municipal obligations is Private or Nonpublic.

27. **Hazardous Materials Data (Private/Nonpublic)** Minn. Stat. § 145.94

Data relating to exposure to hazardous substances is Private or Nonpublic.

28. **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 is published.

29. **Salary/Benefit Survey Data (Nonpublic)** Minn. State. § 13.435

Salary and personnel benefit data purchased from consulting firms is nonpublic.

30. **Social Security Numbers (Private)** Minn. Stat. § 13.355

SSNs, collected in whole or in part, are Private Data on Individuals.

31. **Public Employees Retirement Association Data (Private)** Minn. Stat. § 13.63

The home address, date of birth, direct deposit account number, and tax withholding data of individual beneficiaries and survivors of members are Private Data on Individuals.

32. **Electronic Payments, Credit Card and Bank Account Numbers (Private/Nonpublic)**
Minn. Stat. § 13.37

Information that would substantially jeopardize the security of information, possessions, or individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury is Private or Nonpublic.

33. **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.

34. **Group Auto Self-Insurance Claims Data (Private/Nonpublic)** Minn. Stat. § 471.617

Claims data, either as to single claims or total claims of an individual, is Private or Nonpublic Data, except that it may be disclosed to authorized personnel of the City in order to administer a health benefit program.

35. **Welfare (Private)** Minn. Stat. § 13.46

Generally, welfare data (except summary data) is Private Data. The welfare data section of the MGDPA, however, has numerous exceptions and special treatment for particular data types and applications. Contact the City attorney for requests involving welfare data.

36. **Benefit Data (Private)** Minn. Stat. §§ 13.462

Data on individuals seeking information about becoming an applicant for or a recipient of benefits or services provided, or that is or was an applicant or recipient of such benefits or services, under various housing, home ownership, rehabilitation and community action agency, Head Start, and food assistance programs administered by government entities, with the exception of names and addresses, is Private Data.

EXHIBIT B

DATA DISCLOSURE REQUEST

TO BE COMPLETED BY REQUESTER:

Date: _____

Description of Data Requested: _____

Note: You will be required to identify yourself and verify your identity if the data you request is classified as Private.

TO BE COMPLETED BY DEPARTMENT:

Department Name: _____ Handled By: _____

Information classified as: _____ PUBLIC
_____ PRIVATE
_____ NONPUBLIC
_____ CONFIDENTIAL
_____ PROTECTED NONPUBLIC

Verification: For Private Data, identification must be verified using a driver's license or state ID (), comparison of requester's signature on file (), or personal knowledge of identity ().
Attach a copy if applicable.

Action: _____ APPROVED
_____ APPROVED IN PART (Explain Below)
_____ DENIED (Explain Below)
Basis for denial or partial approval, including statutory section where applicable:

Fees: See Data Practices Policy Section V.c for appropriate charges.

Total Charges: _____ Prepayment Required? Yes () No ()

Authorized Signature: _____ Date: _____



EXHIBIT C

Office of Administration

229 Broadway St E
Rockville, MN 56369
320-251-5836
320-240-9620 fax
www.rockvillecity.org

Minnesota Government Data Practices Act – Chapter 13
TENNESSEN WARNING

Data is requested from the applicant on various forms. The purpose and intended use of the requested data is to verify the applicant meets all state statute and city code provisions and, if the license or permit is approved, to verify that all required data remains current.

The following data collected, created, or maintained is classified under the Minnesota Government Data Practices Act as Private data **until license approval** when the data becomes **Public**: (13.41, Subd. 5).

1. Data submitted by applicants (other than names and designated addresses).
2. Orders for hearing and findings of fact.
3. Conclusions of law and specification of the final disciplinary action contained in the record of the disciplinary action.
4. Entire record concerning the disciplinary proceeding.
5. License numbers.
6. License status.

The following data collected, created, or maintained is classified as **Private**: (13.41, Subd. 2).

1. The identity of complainants who have made reports concerning licenses or applicants which appear in inactive complaint data unless the complainant consents to the disclosure.
2. The nature or content of unsubstantiated complaints when the information is not maintained in anticipation of legal action.
3. Inactive investigative data relating to violations of statutes or rules.
4. The record of any disciplinary proceeding except as limited by Subd. 4.

The following data collected, created, or maintained is classified as **Confidential**: (13.41, Subd. 4).

1. Active investigative data relating to the investigation of complaints against any license.

Under law, private data may be shared with licensing and inspection employees, approval authorities, insurance providers, law enforcement employees, contracted inspection officials, as required by court order and City officials who have a bona fide need for it. The City of Rockville may make any data classified as private or confidential accessible to an appropriate person or agency if the licensing agency determines that failure to make the data accessible is likely to create a clear and present danger to public health or safety.

We ask that you complete or provide all data requested on the application form(s) unless we have noted that it is not required. Refusal to supply required information may mean that your application cannot be processed.

I READ AND UNDERSTAND THE ABOVE INFORMATION REGARDING MY RIGHTS AS A SUBJECT OF GOVERNMENT DATA.

Date

Signature of Applicant



EXHIBIT D

Office of Administration

229 Broadway St E
Rockville, MN 56369
320-251-5836
320-240-9620 fax
www.rockvillecity.org

CONSENT TO RELEASE PRIVATE DATA

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

Name _____

Home Address _____

Home Telephone Number _____

This information can be released to the media, public, and the City of Rockville publications, including the City web site and newsletter. The public requests receiving this information, will have to complete a *Request for Government Data* form. This request form will be kept on file.

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

Signature (First Name, Middle, Last)

Date

Witness Signature and Date
City Employee

Notary Public _____

EXHIBIT E

GOVERNMENT DATA ACCESS AND NONDISCLOSURE AGREEMENT

1. **AUTHORIZATION.** The Rockville ("City") hereby authorizes the following party, _____ ("Authorized Party"), to access the following Government Data:

2. **PURPOSE.** Access to the above Government Data is limited to the creation of summary data for the following purpose(s):

3. **COSTS.**

() The Authorized Party requested the summary data and agrees to bear the City's costs associated with the preparation of the data.

That cost is \$ _____ and is payable to the City.

() The City has asked the Authorized Party to prepare summary data and will bear the costs accordingly.

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. No data which is not public will ever be disclosed or communicated to anyone by any means.

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. If the data can in any way identify an individual, the Authorized Party agrees not to make reproductions of any data or remove any data from the site where it is provided.

The Authorized Party warrants that the following named individual(s) will be the only person(s) to participate in the collection of the data and the creation of the summary 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 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 of its 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 the Agreement to maintain insurance covering the Authorized Party's activities under this Agreement. The insurance will cover \$1,000,000.00 per claimant for personal injuries and/or damages and \$1,000,000.00 per occurrence. The policy must cover the indemnification obligation specified above.

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

8. **SUMMARY DATA RESULTS**

() If the Authorized Party is the requester, a copy of all reports, summaries, compilations, articles, publications or any document or series of documents which are created from the data provided under this Agreement must be made available, in its entirety, to the City.

() If the Authorized Party is a contractor of the City, the Authorized Party may retain one copy of all reports, summaries, compilations, articles, publications or any document or series of documents which are created from the data provided under this Agreement for its own records, but may not disclose it or any portion of it without permission, except in defense of claims brought against it. All other copies of reports, summaries, compilations, articles, publications or any document or series of documents which are created from the data provided under this Agreement must be provided to the City.

AUTHORIZED PARTY: _____ Date: _____

By: _____
Its: _____

CITY OF ROCKVILLE Date: _____

By: _____
Its: _____

EXHIBIT F

NOTICE TO PERSONS UNDER THE AGE OF 18

Some of the information you are asked to provide is classified as private data 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. If you wish to request that data be withheld, complete the following:

Data to be withheld:

From: _____

For the following reason:

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 (a) you are of sufficient age and maturity to explain the reasons for your request and understand the consequences of asking that the data be withheld, (b) denying access may protect you from physical or emotional harm, (c) there are reasonable grounds to support your reasons, and (d) the data concerns medical, dental, or other health services provided under Minn. Stat. §§ 144.341 to 144.347. If so, the data may be released only if failure to inform the parent or legal guardian would seriously jeopardize your health.

I have received and reviewed this notice.

PRINT NAME: _____

DATE OF BIRTH: _____

Signature: _____

DATE: _____

EXHIBIT G

SAMPLE PROVISION FOR CONTRACTS WITH OUTSIDE ENTITIES ACCESSING PRIVATE, NONPUBLIC, OR CONFIDENTIAL DATA

Data Practices Compliance. Contractor will have access to data collected or maintained by the City to the extent necessary to perform Contractor's obligations under this contract. Contractor agrees to maintain all data obtained from the City in the same manner as the City is required under the Minnesota Government Data Practices Act, Minnesota Statutes Chap. 13 ("MGDPA"). Contractor will not release or disclose the contents of data classified by the MGDPA as not public to any person except at the written direction of the City. 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 MGDPA or this contract. Upon termination of this contract, Contractor agrees to return data to the City, as requested by the City.