CITY OF KIMBALL
MUNICIPAL POLICY NUMBER 04-2010
DATA PRACTICES POLICY

DATE COUNCIL APPROVED: September 7, 2010
UPDATED: June 12, 2012
UPDATED: November 7, 2017

The Data Practices Policy (Policy) contains the procedures and forms adopted by the City of Kimball (City) to comply with the requirements of the Minnesota Government Data Practices Act, (MGDPA) MN Statutes Chapter 13.01 et seq.

Section I: Responsible Authority and Compliance Official.

The data practices compliance official is the designated employee of the government entity to whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices issues. The City Council has appointed Nicole Pilarski, City Clerk/Treasurer, as the City's Responsible Authority and the Compliance Official for the Act. The phrase "Responsible Authority or a designee" used in this Policy means the person responding to a MGDPA request for the City.

Section 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. The MGDPA classifies categories of Government Data that are not generally accessible to the public as follows:

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

Section 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 must determine:

(1) 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) 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 *MN Stat. § 13.02, subd. 8a* maintained by the City are attached to this Policy as Exhibit D, and responses should follow the protocol below depending on the category of data.

A. **Access to Public Data.** All data maintained by the City is public unless there is a specific statutory designation which gives it a different classification.

B. **People Entitled to Access**. Any person has the right to inspect and copy public data. The person also has the right to have an explanation of the meaning of the data. The person does not need to state his or her name, provide identification or give the reason for the request (*MN Stat. § 13.05, subd. 12*). To fulfill the request, the representative of the City may ask questions to clarify the request and may use the form contained in this policy as Exhibit B. The City must determine whether it maintains the requested data. The City is not required by the MGDPA to provide data that it does not maintain, nor is the City required to produce data in a new format.

C. Form of Request. The request for public data must be in writing. The City will consult with its attorney in preparing a response for data relating to litigation.

D. **When Must Accessible Data Be Provided.** Requests will be received and processed during normal business hours. If requests cannot be processed or copies cannot be made immediately at the time of the request, the information must be renewed by the party making the request.

E. **Fees.** Fees may be charged only if the requesting person asks for a copy or electronic transmittal of the data. The fee may not include time necessary to separate public from non-public data. Fees may not be charged for inspection of government data.

- **Single-Sided, Black and White, Letter or Legal-Size Documents**

  100 or fewer pages 25¢ per page (MN Statute 13.03, subd. 3 c.)

  More than 100 pages Actual Cost (as defined below)

  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 any other production expenses. Actual costs shall be determined by the department fulfilling the data request.

  The City may require the requesting party to prepay any fees associated with a request for copies or transmission.

  The Responsible Authority may also charge an additional fee if the copies have commercial value and are a substantial and discrete portion of a formula, compilation, program, process, or system developed with significant expenditure of public funds. This additional fee must relate to the actual development costs of the information.

Section IV. Access to Data on Individuals. Data about individual people is classified by law as public, private, or confidential. A list of the private and confidential information maintained by the City is attached as Exhibit C (Non-public Data Maintained by City). Information to be incorporated on forms used to collect private and confidential information is also attached as Exhibit D (Tennessen Warning).

A. People Entitled to Access.

1. Public data about an individual may be shown or given to anyone.

2. Private data about an individual may be shown or given to:

- The individual
- 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 E or a form reasonably similar.

- People who are authorized access by federal, state, local law or court order.
- People about whom the individual was advised at the time the data was collected. The identity of those people must be part of the Tennessen Warning.
- People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

3. Confidential and Protected nonpublic information may not be given to the subject of the data, but may be shown or given to:

- People who are authorized access by federal, state, local law or court order and whose identity is disclosed in the Tennessen Warning.
- People within the City staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

B. Form of Request. Any individual may request verbally or in writing whether the City has stored data about that individual and whether the data is classified as public, private, nonpublic, confidential or protected nonpublic.

All requests to see or copy private nonpublic, confidential or protected nonpublic information must be in writing. An information disclosure request, attached as Exhibit F, must be completed to document who requests and who receives this information. The Responsible Authority or Designee must complete the relevant portions of the form. The Responsible Authority or Designee may waive the use of this form if there is other documentation of the requesting party's identity, the data requested, and the City's response. A response to a request for data relating to litigation will be made after consultation with the City Attorney.

C. Identification of Requesting Party. The Responsible Authority or Designee must verify the identity of the requesting party as a person entitled to access. This can be done through personal knowledge, presentation of written 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 will be received and processed during normal business hours. The response must be immediate, if possible, or within 10 working days if an immediate response is not possible (*MN Stat. § 13.04 subd. 3*).

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

F. Summary Data. Summary data means statistical records and reports derived from data on individuals but which does not identify an individual by name or any other private, nonpublic, confidential or protected nonpublic data. Summary 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 a deposit for the cost of preparation in advance. The Responsible Authority or Designee must notify the requester of the anticipated time schedule and the reasons for the delay.

Summary data may be prepared by redacting (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 authorize 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, nonpublic, confidential or protected nonpublic data, and (3) the Responsible Authority determines that access by this outside agency or person will not compromise the privacy of the private, nonpublic,

confidential or protected nonpublic data. The Responsible Authority may use the form attached as Exhibit F.

G. Juvenile Records. The following applies to private (not confidential) data about people under the age of 18.

1. **Notice to Juvenile Subject of Data.** Before requesting private data from juveniles, City personnel must notify the juveniles subjects that they may request that their private data be withheld from their parent(s) or legal guardians, stating reasons for the request. This notice should be in the form attached as Exhibit H and must be given in addition to a Tennessen Warning.

2. **Parental Access.** In addition to the people listed above who may have access to private data, a parent may have access to private information about a juvenile subject. "Parent" means the parent or legal guardian of a juvenile data subject, or individual acting as a parent or legal guardian in the absence of a parent or legal guardian. The parent is presumed to have this right unless the Responsible Authority or designee has been given evidence that there is a state law, court order, or other legally binding document which prohibits this right.

3. **Denial of Parental Access.** The Responsible Authority or Designee may deny parental access to private data when the juvenile requests this denial and the Responsible Authority or Designee determines that withholding the data would be in the best interest of the juvenile. The request from the juvenile must be in writing stating the reasons for the request. In determining the best interest of the juvenile, the Responsible Authority or Designee will consider:

   - Whether the juvenile is of sufficient age and maturity to explain the reasons and understand the consequences;
   - Whether denying access may protect the juvenile from physical or emotional harm;
   - Whether there is reasonable grounds to support the juvenile's reasons; and
   - Whether the data concerns medical, dental, or other health services provided under *MN Stat. § 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 minor.
   - The Responsible Authority or Designee may also deny parental access without a request from the juvenile under *MN Stat. § 144.335*.

Section V. Denial of Access. If the Responsible Authority or Designee determines that the requested data of whatever classification 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. A denial must be given in writing, including the specific legal authority for the denial upon request of the party requesting data.

Section VI. Collection of Data on Individuals. The collection and storage of information about individuals will be limited to that necessary for the administration and management of programs specifically authorized by the State Legislature, City Council or Federal Government.

When an individual is asked to supply private, nonpublic, confidential or protected nonpublic information about himself or herself, the City employee requesting the information must give the individual a Tennessen warning. This warning must contain the following:

1. the purpose and intended use of the requested data;
2. whether the individual may refuse or is legally required to supply the requested data;

3. any known consequences from supplying or refusing to supply the information; and
4. the identity of other persons or entities authorized by state or federal law to receive the data.

A Tennessen warning is not required when an individual is requested to supply investigative data to a law enforcement officer.

A Tennessen warning may be on a separate form or may be incorporated into the form which requests the private, nonpublic, confidential or protected nonpublic data. In certain situations, a victim and/or witness to a crime may request that their identity be withheld from the public.

Section VII. Challenge to Data Accuracy. An individual who is the subject of public or private data may contest the accuracy or completeness of that data maintained by the City. The individual must notify the City's Responsible Authority in writing describing the nature of the disagreement. Within 30 days, the Responsible Authority or Designee must respond and either (1) correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual, or (2) notify the individual that the Authority believes the data to be correct.

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

Section VIII. Data Accuracy and Security Safeguards.

A. Accuracy of Data. In order that Government Data be kept in the most accurate and current state practicable, the following guidelines should be followed:

1. All employees will be requested to provide updated personal information to the appropriate supervisor and Human Resources. The information is necessary for tax purposes, insurance coverage, emergency notifications and other personnel purposes.
2. Other people who provide private, nonpublic, confidential or protected nonpublic information will also be encouraged to provide updated information when appropriate.
3. Department directors and division managers should periodically review forms used to collect data on individuals to delete items that are not necessary and to clarify items that may be ambiguous.

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 or designee 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 *MN Stat. Ch. 14*.

C. Data Security.

1. City Staff must pay careful attention to and abide by the City's Records Retention Schedule, disposing of records as appropriate.

2. Private, nonpublic and confidential data must be stored in secure files or databases which are not accessible to unauthorized personnel. Pursuant to *Minn. Stat. § 13.05, subd. 5*, 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. The City conducts ongoing security checks and must complete, at least annually, a comprehensive assessment of security of the Private, Nonpublic and Confidential Data maintained.
3. Private, nonpublic and confidential data should be kept within City offices at all times unless necessary for off-premises City business.
4. Only those employees whose job responsibilities require them to have access will be allowed access to files and records that contain private and confidential information. These employees will be instructed to:
   - not discuss, disclose or otherwise release private, nonpublic, confidential or protected nonpublic data to City employees whose job responsibilities do not require access to the data;
   - not leave private, nonpublic, confidential or protected nonpublic data where non-authorized individuals might see it; and
   - shred private, nonpublic, confidential or protected nonpublic data before discarding, or dispose through confidential locked recycling.
   - When a contract with an outside party requires access to private, nonpublic, confidential or protected nonpublic information, the contracting party will be required to use and disseminate the information consistent with the Act. The City may include in a written contract the language contained in Exhibit I.

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:

1. "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.
2. "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.

E. Contracts with Private Entities. If the City enters into a contract with a private person to perform any of the City's functions, all of the data created, collected, received, stored, used, maintained or disseminated by such private person in performing those functions is subject to the requirements of *Minn. Stat. § 13.01 et seq.* and such person must comply with the requirements as if he or she were a

government entity. All such contracts must include a notice that the requirements of *Minn. Stat. § 13.01 et seq.* apply to the contract. See Exhibit I.

F. Procedures in the Event of Unauthorized Access. This Policy establishes that only those personnel who need to access Nonpublic Data do so. In the event of a breach of that requirement, the City is required to notify any individual or entity whose Nonpublic Data was wrongfully accessed, to conduct an investigation into the matter, and to prepare a report. Notification must occur in the most expedient time frame possible and must inform the individual or individuals how they can obtain a copy of the report. If the breach involves unauthorized access by an employee, contractor or agent of the government entity, the report must include at least (i) the description of the type of data accessed (ii) the number of individuals affected; (iii) final disposition of disciplinary action against any employee determined to be responsible for the breach. See *Minn. Stat. § 13.055*.

Section IX. Forms and Resources.

Exhibit A	**List of Designees**
Exhibit B	**Request for Public Data Request Form**
Exhibit C	**Classified Data Access Request**
Exhibit D	**Government Data Classified as Not Public (Private, Nonpublic, Confidential or Protected Nonpublic) Maintained**
Exhibit E	**Data Practices Advisory (Tennessen Warning)**
Exhibit F	**Consent to Release Private Data**
Exhibit G	**Government Data Access and Nondisclosure Agreement**
Exhibit H	**Notice to Persons Under the Age of 18**
Exhibit I	**Sample Contract Provision for Contracts with Outside Entities Accessing Private, Nonpublic, Confidential or Protected Nonpublic Data**

EXHIBIT A

LIST OF DESIGNEES

The following persons are officially designated by the Responsible Authority as "Designees" to be in charge of individual files or systems containing government data and to receive and comply with the requests for government data.

EXHIBIT B
CITY OF KIMBALL
REQUEST FOR PUBLIC DATA
MINNESOTA GOVERNMENT DATA PRACTICES ACT

REQUESTER: Complete this form and return it to Kimball City Hall. You may submit it via e-mail at nicole.pilarski@ci.kimball.mn.us, in person or via U.S. Mail.

You do not have to provide contact information. 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.

The City of Kimball will respond to you as soon as reasonably possible.

NOTICE: You may cancel this request at any time prior to the release of information.
You may be required to pay the actual costs of making copies.

Last Name	*First Name*		*Phone*	*Date*
Street Address	*City*	*State*	*Zip*	*Email*

Information Requested (be as specific as possible):

DEPARTMENT USE ONLY - ***Requester, please do not write below this line.***

Department _____ **Handled by:** _____

Request Type: ☐ **In-person,** ☐ **Mail** ☐ **Phone** ☐ **E-mail**

Fees Charged: _____

EXHIBIT C
CLASSIFIED DATA
ACCESS REQUEST
GOVERNMENT DATA PRACTICES ACT

REQUESTER: Complete this form and return it to Kimball City Hall.

NOTICE: You may cancel this request at any time prior to the release of information. In any event, this consent form will expire 90 days after signing.
After being shown private data on individuals and informed of its meaning, this data need not be disclosed again for six months unless additional information has been collected or an action is pending.
You may be required to pay the actual costs of making and/or compiling data.
NOTE: The subject of the data request must authorize the release of private information to the subject's agent or another agency. An "Informed Consent to Release" must be completed by the subject of the data.

Name: _____

Last First M.I. Date

Address: _____

Street City State Zip Phone No.

Information Requested _____

_____

_____

_____

Requester's Signature: *If not the subject of the data requested, see note above.*

DEPARTMENT USE ONLY - *Please do not write below this line.*

NOTE: Reasonable identification must be obtained from the person seeking the information.
NOTE: If Data Subject is a minor, consult Attorney prior to release of information.

_____

Department Handled by:

_____

Identification Viewed (Driver's License, State ID, Notarized Request)

Requester is: _____ Data Subject _____ Not Data Subject (See NOTE above)

Request Type: _____ In-person _____ Mail

Data Classification: _____ Public _____ Non-Public _____ Protected Non-Public _____ Private

_____ Confidential

Request: _____ Approved _____ Denied Authorized Signature_____

_____

_____

Comments: Enter any appropriate remarks or comments. If data access is denied, cite authority or reason.

Fees Charged: _____

EXHIBIT D
CITY OF KIMBALL
RESOURCE LIST
NON-PUBLIC DATA MAINTAINED
BY THE CITY OF KIMBALL

Personnel Data (Private) *MN Stat. §13.43*
All data about an individual who is employed as, or an applicant to be, an undercover law enforcement officer is private*. All data on all other individuals who are or were an employee, an applicant for employment, volunteer, independent contractor, **except the following which is public:**

1. **PUBLIC DATA**
   - 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
   - Bargaining unit
   - 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 Identification Number (not a social security number)
   - If it is 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.

   * Undercover Law Enforcement Officer Data (Private – *MN 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.

2. **Applicant Data (Private)** ***MN 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:**

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)

3. Applicants for Appointment (*MN Stat. § 13.601, subd. 3.*)

Data about applicants for appointment to a public body collected by a government entity as a result of the applicant's application for appointment to the public body are Private Data on Individuals except that the following are public: name; city of residence, except when the appointment has a residency requirement that requires the entire address to be public; education and training; employment history; volunteer work; awards and honors and prior government service.

- Once an individual is appointed to a public body, the following additional data are public: residential address and either a telephone number or e-mail address where the appointee can be reached, or both at the request of the appointee.
- An e-mail address or telephone number provided by a public body for use by an appointee shall be public. An appointee may use an e-mail address or telephone number provided by the public body as the designated e-mail address or telephone number at which the appointee can be reached.

4. Real Property Complaint Data (Confidential) *MN Stat. § 13.44*

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

5. Security Information (Private/Nonpublic) *MN Stat. § 13.37, subd. 1 (a)*

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 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 location of a National Night Out event is Public Data.

6. Trade Secret Information (Nonpublic) *MN Stat. § 13.37, subd. 1 (b)*

The Responsible Authority, in consultation with legal counsel as necessary, will determine whether particular information qualifies as Trade Secret according to the following definition:

- "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.

7. Bids, Proposals, Sealed Bids (Private/Nonpublic) *MN Stat. § 13.37, subd. 2 and 13.591*

- Sealed bids, including the number of bids received, prior to opening are Nonpublic Data.
- 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 re-solicitation of bids results in completion of the selection process or the process is abandoned. If re-solicitation does not occur within one year, the remaining data become Public.

8. **Labor Relations Information (Nonpublic)** ***MN Stat. § 13.37, subd. 1 (c)*** **Protected Nonpublic**
   - 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.

9. **Firearms Data (Private)** ***MN Stat. § 13.87, subd. 2***
   - Data about the purchase or transfer of firearms and applications for permits to carry firearms.

10. **Examination Data (Private or Confidential)** ***MN 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. **Elected Officials Correspondence (Private)** ***MN 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. **Federal Contracts Data (Private/Nonpublic)** ***MN 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 is classified as private or nonpublic.

13. **Law Enforcement and Investigative Data (Confidential/Protected Nonpublic/ Private)** ***MN Stat. § 13.80, 13.82, 13.85, 13.87, 169.09, 168.10, 169A.70, 171.043, 171.07, 171.071, 171.12, 171.32, 299A.61, 299C.065, 299C.091, 299C.093, 299C.095, 299C.46, 299C.48, 299C.53, 299C.56, 611.272, 626.53, 609.324, 609.3452, 609.3471, 626.556, 626.5563, 626.557, 626.558, 626.5593, 626.89, 629.341, 260B.171, 260B.198, 260B.235, 299C.68, 299F.035, 299F.04, 299F.05, 299F.054, 299F.055, 299F.056, 299F.095 and 299F.096***
    - Data collected under *Minn. Stat. §* 518B.01 (Domestic Abuse Act) are 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. Details of arrest previous to charges being filed by prosecutor are private.

14. Planning Survey Data (Private/Nonpublic) ***MN 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.

15. City Attorney Records (Confidential) ***MN 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 is Confidential. Data which is the subject of the "work product" privilege is Confidential.

16. Business Data (Private/Nonpublic) ***MN 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.

17. Municipal Obligation Register Data (Private/Nonpublic) ***MN Stat. § 475.55***
Information with respect to the ownership of municipal obligations is Private or Nonpublic.

18. Hazardous Materials (Private/Nonpublic) ***MN Stat. § 145.94***
Data relating to exposure to hazardous substances is Private or Nonpublic.

19. Auditing Data (Nonpublic/Protected Nonpublic) ***MN Stat. § 13.392***
Data, notes and preliminary drafts of audit reports are confidential or protected nonpublic until the final report is published.

20. Social Security Numbers (Private) ***MN Stat. § 13.355***
SSNs collected in whole or in part are Private Data on Individuals.

21. Public Employees Retirement Association Data (Private) ***MN 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.

22. Electronic Payments, Credit Card Numbers, Bank Account Numbers (Private/Nonpublic) ***MN Stat. § 16A.626***
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.

23. Drug and Alcohol Test Results (Private) ***MN Stat. § 181.954 and 49 CFR 382.405***
With respect to public sector employees and job applicants, the results of drug or alcohol tests are Private Data on Individuals.

24. Welfare (Private) ***MN Stat. § 13.46***
Generally, welfare data (expect 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.

25. Domestic Abuse Data (Confidential) ***MN Stat. § 13.80***
Data on individuals collected, created, received or maintained by the police department pursuant to the Domestic Abuse Act, section 518B.01, are classified as confidential data, pursuant to section 13.02, subdivision 3, until a temporary court order made pursuant to subdivision 5 or 7 of section 518B.01 is executed or served upon the data subject who is the respondent to the action.

26. Personal Contact and Online Account Information (Private) ***MN Stat. § 13.356***
Data on an individual collected, maintained, or received for notification purposes or as part of a subscription list for electronic periodic publications as requested by the individual are private data on individuals: (1) telephone number; (2) e-mail address; and (3) Internet user name, password, Internet protocol address, and any other similar data related to the individual's online account or access procedures.

EXHIBIT E
CITY OF KIMBALL DATA PRACTICES ADVISORY
(TENNESSEN WARNING)

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

Our purpose and intended use of this information is: _____

_____

_____

You ☐ are ☐ are not legally required to provide this information.

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

_____

_____

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

_____

_____

_____

_____

Your signature on this form indicates that you understand this advisory.

X_____

Signature

EXHIBIT F
CITY OF KIMBALL
CONSENT TO RELEASE PRIVATE DATA

I,_____, authorize the City of Kimball ("City")
(print name)
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 following purpose or purposes:

_____

_____

_____

This authorization is dated _____ and expires on _____.

The expiration cannot exceed one year from the date of the authorization, except in the case of authorizations given in connection with applications for life insurance or non-cancelable or guaranteed renewable health insurance and identified as such, two years after the date of the policy.

I 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

X_____
Signature

Identification must be verified by a driver's license, state ID, passport or other valid identification.
On this _____day of _____, _____ personally appeared before me; whose identity I proved on the basis of satisfactory evidence to be the signer of the above instrument, and he/she acknowledged that he/she executed it.

_____
Notary Public

EXHIBIT G
CIT OF KIMBALL
GOVERNMENT DATA ACCESS
AND NONDISCLOSURE AGREEMENT

1. **AUTHORIZATION.** City of Kimball ("City") hereby authorized _____ _____ , ("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 purposes: _____

   _____

   _____

3. **COST.** (Check which applies)

   ☐ The Authorized Party is the person who requested the summary data and agrees to bear the City's cost 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 a reasonable fee.

4. **SECURITY.** The Authorized Party agrees that it and any employees or agents under its control must protect the privacy interest 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 non-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 to remove any data from the site where it is provided, if the data can in any way identify an individual.

   No data which are not public and which are irrelevant to the purpose stated above will ever be disclosed or communicated to anyone by any means.

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

5. **LIABILITY FOR DISCLOSURE.** The Authorized Party is liable for any unlawful use or disclosure of government data collection, 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 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 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 information described above from _____ to _____.

8. **SUMMARY DATA 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 which are created from the information 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, publication or any document or series of documents which are created from the information provided under this Agreement must be provided to the City. The Authorized Party may retain one 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): _____

CITY OF KIMBALL

By: _____ Date: _____
City Clerk/Treasurer

EXHIBIT H
CITY OF KIMBALL
NOTICE TO PERSONS UNDER AGE OF 18

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

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

- Whether you are of sufficient age and maturity to explain the reasons and understand the consequences,
- Whether denying access may protect you from physical or emotional harm,
- Whether there are reasonable grounds to support your reasons, and
- Whether the data concerns medical, dental or other health services provided under *MN Stat. § 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: _____ _____
(Title)

Request to Withhold Information

I request that the following information: _____

_____

_____

Be withheld from: _____

_____

For these reasons: _____

_____

_____

I have received and reviewed this notice: _____

Date of Birth: _____ _____ _____
Print Name Signature

EXHIBIT I
SAMPLE CONTRACT PROVISION
DATA PRACTICES ACT

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, *MN Stat. § Chapter 13*. Contractor will not release or disclose the contents of data classified as not public to any person except at the written direction of the City. Contractor agrees to defend and indemnify the City, its elected officials and employees, from any claim, liability, damage or loss asserted against the City, its elected officials and employees, 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.