

KEARNS CITY COUNCIL

ORDINANCE NO. 2025-O-20

DATE: December 8, 2025

AN ORDINANCE TO INITIATE THE ESTABLISHMENT OF THE CITY OF KEARNS DATA PRIVACY PROGRAM; DESIGNATE CHIEF ADMINISTRATIVE AND AUTHORIZED RECORDS OFFICERS; REQUIRE RECORDS FOR PROOF OF OFFICER AND EMPLOYEE PRIVACY TRAINING; PREPARE WEBSITE DATA PRIVACY NOTICE; ENDORSE THE STATE OF UTAH'S DATA PRIVACY POLICY; AND COMPLETE KEARNS' INTERNAL DATA PRIVACY PROGRAM REPORT

WHEREAS, the Kearns City Council ("**Council**") adopts programs to guide decision-making and policy; and

WHEREAS, the State of Utah requires each governmental entity, including the City of Kearns ("**Kearns**"), to initiate a data privacy program ("**DPP**") that recognizes the state policy that "an individual has a fundamental interest in and inherent expectation of privacy regarding the individual's personal data that an individual provides to a governmental entity" and each governmental entity shall process personal data consistent with this state policy pursuant to Utah Code § 63A-19-401; and

WHEREAS, the Utah State Legislature enacted HB 444, Data Privacy Amendments, in 2025, which requires Kearns to prepare an internal DPP report ("**Report**") no later than December 31, 2025, pursuant to Utah Code Ann. § 63A-19-401.3; and

WHEREAS, the Council resolves to fully comply with the requirements of Utah Code, Title 63A, Chapter 19, Government Data Privacy Act ("**GDPA**"); Utah Code, Title 63G, Chapter 2, Government Records Access and Management Act ("**GRAMA**"); and Utah Government Operations Code, Title 63A; including the completion of the Report; and

WHEREAS, Kearns is a member of the Greater Salt Lake Municipal Services District ("**MSD**") that collects the majority of data from the residents of the MSD member cities and towns for Planning & Development services. Kearns supports MSD's own Data Privacy Program as approved by the MSD Board of Trustees; and

WHEREAS, the Council desires to initiate and establish an official Kearns DPP to be developed and implemented over time to comply with the requirements of Utah Code, Title 63A, Chapter 19, Part 4, Duties of Governmental Entities, and other applicable laws; and

WHEREAS, the Council desires to appoint a Chief Administrative Officer ("**CAO**") and an administrative records officer ("**ARO**") for the City's DPP.

NOW, THEREFORE BE IT ORDAINED by the Kearns City Council that:

1. Approval of Forms: The Council approves the following forms:

a. The internal privacy report form template included as **Exhibit A** of this Ordinance; and

b. The website data privacy statement attached as **Exhibit B** of this Ordinance.

2. Appointment of CAO: The Council designates Marla Howard, General Manager for the Greater Salt Lake Municipal Services District as the CAO of the Kearns DPP and directs the CAO to:

a. Obtain all required training(s); and

b. Oversee the compliance of all Kearns staff and applicable agents with the data privacy training pursuant to Utah Code § 63A-19-401.2; and

c. Report the names of the designated CAO and ARO to the Division of Archives and Records Services pursuant to Utah Code Subsections 63A-12-103(8)(c)(ii) and 63G-2-108; and

d. Prepare the Report to the best of the CAO's ability using the template attached as Exhibit A in accordance with applicable law and to file the completed report in Kearns' records, provided that such report will be a protected record; and

e. Prepare the website data privacy statement in a manner that is substantially similar to the notice template attached as Exhibit B and publish the completed statement to the City of Kearns' official website and the Utah Public Notice Website.

3. Appointment of ARO: The Council designates Diana Baun, City Recorder as the ARO of the Kearns DPP to fulfill all duties under applicable law and Kearns ordinances and directs the ARO to take all required training(s).

4. Endorsement: The Council endorses the State of Utah's data privacy policy.

5. Enactment of DPP: The Council approves:

a. The initiation and establishment of the Kearns DPP, with direction to the Mayor and staff to and present to the Council for approval at a later date such other ordinances, rules, or policies needed to implement the DPP and to comply with applicable law; and

b. The designation of the CAO and appointment of the ARO, the intended recordkeeping for proof of completion of ARO training and certification and employee privacy training; and

- c. The preparation and publication of the website data privacy notice; and
- d. The completion of the Report.

6. Additional Direction to Mayor and Staff: The Mayor and staff are authorized and directed to take such other steps as may be needed:

- a. For this Ordinance to become effective under Utah law; and
- b. To make any non-substantive edits to correct any scrivener's, formatting, and numbering errors that may be needed, if any, to this Ordinance.

7. Severability: If a court of competent jurisdiction determines that any part of this Ordinance is unconstitutional or invalid, then such portion of this Ordinance, or specific application of this Ordinance, shall be severed from the remainder, which shall continue in full force and effect.

8. Effective Date: This Ordinance will go into effect immediately.

[execution on following page]

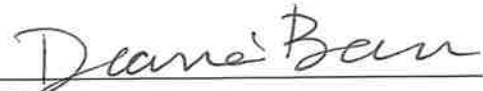
ADOPTED AND APPROVED at a duly called meeting of the Kearns City Council
on this 8th day of December 2025.

CITY OF KEARNS



By: Kelly Bush, Mayor

ATTEST:



Diana Baun, City Recorder

Voting:

Mayor Bush	voting	<u>aye</u>
Council Member Butterfield	voting	<u>aye</u>
Council Member Peterson	voting	<u>ABSENT</u>
Council Member Schaeffer	voting	<u>aye</u>
Council Member Snow	voting	<u>aye</u>

(Complete as Applicable)

Date ordinance summary was published on the Utah Public Notice Website per Utah Code §10-3-

711: December 9, 2025

Effective date of ordinance: December 9, 2025

**SUMMARY OF
CITY OF KEARNS
ORDINANCE NO. 2025-O-20**

On December 8, 2025, the Kearns Council enacted Ordinance No. 2025-O-20 to: (1) establish a data privacy program per H.B. 444; (2) designate chief administrative and authorized records officers; (3) require records for proof of officer and employee privacy training; (4) prepare a website data privacy notice; (5) endorse the State of Utah's data privacy policy; and (6) complete an initial data privacy program report.

CITY OF KEARNS


By: Kelly Bush, Mayor

ATTEST:


Diana Baun, City Recorder

Voting:

Mayor Bush	voting	<u>aye</u>
Council Member Butterfield	voting	<u>aye</u>
Council Member Peterson	voting	<u>ABSENT</u>
Council Member Schaeffer	voting	<u>aye</u>
Council Member Snow	voting	<u>aye</u>

A complete copy of Ordinance No. 2025-O-20 is available in the office of the Kearns City Recorder, 860 Levoy Drive, Suite 300, Taylorsville, Utah 84123.

EXHIBIT A

CITY OF KEARNS TEMPLATE DATA PRIVACY PROGRAM REPORT

Section 1: Governmental Entity Information

Governmental Entity Name: _____

Governmental Entity Type (Select One):

☐ State Agency

☐ Interlocal

☐ County

☐ Associations of Government

☐ Municipality

☐ Charter School

☐ Special Service District

☐ Public School

☐ Board or Commission

☐ Independent or Quasi-Government

☐ College or University

☐ Other _____

Mailing Address:

Chief Administrative Officer (CAO):

- **Name:** _____
- **Title:** _____
- **Email:** _____
- **Phone:** _____
- **Date of Report Completion:** _____

Section 2: Privacy Program Status

Utah Code Ann. Subsection 63A-19-401.3(1)(a):

- Has your governmental entity initiated a **privacy program**?
☐ Yes ☐ No
- What mechanism(s) has your governmental entity used to initiate its **privacy program**?

☐ Administrative Rule

☐ Ordinance

☐ Resolution

☐ Policy

☐ Privacy Program Report

Other: _____

Section 3: Privacy Practices, Maturity and Strategies

Utah Code Ann. Subsections 63A-19-401.3(1)(b)(i) and (ii):

Privacy Practice Maturity Model:

Level	Description
Level 0 Non-Existent	The practice is not implemented or acknowledged.
Level 1 Ad Hoc	The practice may occur but is undocumented (no policies or procedures), application is reactive and not standardized.
Level 2 Defined	The practice is implemented and documented, but documentation may not cover all relevant aspects, and application may be informal and inconsistent.
Level 3 Consistently Implemented	The practice is documented to cover all relevant aspects, application is formal and consistent.
Level 4 Managed	The practice is actively managed with metrics that are regularly reviewed to assess efficacy and facilitate improvement.
Level 5 Optimized	The practice is fully embedded in the entity with recognition and understanding across the workforce through active training and awareness campaigns, and inclusion in operations and strategy.

Privacy Practices Implemented:

List all privacy practices implemented, and the strategies your entity will implement, in the coming calendar year to improve its privacy practices and program. The Office recommends entities indicate the current maturity level (0–5) of each practice and select the target maturity they plan to achieve for a given practice by the end of the following calendar year. This will be beneficial to the entity in moving their privacy programs forward.

Governance				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Gov-1. Chief Administrative Officer (CAO) Designation	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance formally adopting this practice and defines who will make CAO designation and how that designation will be made.	Level 0
Gov-2. Records Officers Appointment	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance formally adopting this practice and defines how the CAO will appoint records officers and review appointments.	Level 0
Gov-3. Records Officer Training and Certification	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance formally adopting this practice and require records	Level 0

			officers complete certification.	
Gov-4. Statewide Privacy Awareness Training	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Gov-5. Privacy Program Report	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Identify				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Ide-1. Record Series Creation and Maintenance	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-2. Record Series Designation and Classification	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-3. Retention Schedule Proposal and Approval	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-4. Record Series Privacy Annotation	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Ide-5. Inventorying	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example strategy:</i> Adopt policy or ordinance that formally adopts this practice.	Level 0
Ide-6. Privacy Impact Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-7. Record and Data Sharing, Selling, or Purchasing	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance requiring any sharing, selling or purchasing of data be reported and inventoried.	Level 0

Control				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Con-1. Data Subject Requests for Access	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Con-2. Data Subject Requests for Amendment or Correction	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Con-3. Data Subject Requests for an Explanation	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Con-4. Data Subject Request At-Risk Employee Restrictions	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
---	---	---------	--	---------

Communicate				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Com-1. Website Privacy Notice (Policy)	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Com-2. Privacy Notice (Notice to Provider of Information)	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Protect				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Pro-1. Minimum Data Necessary	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Pro-2. Record Retention and Disposition	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Pro-3. Incident Response	<input type="checkbox"/> Yes	Level 0		Level 0

	<input type="checkbox"/> No			
Pro-4. Breach Notification	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Other Privacy Practices Implemented by the Governmental Entity				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Section 4: High-Risk Processing Activities

Fulfills requirement of Subsection 63A-19-401.3(1)(b)(iii): The chief administrative officer of each governmental entity shall prepare a report that includes a description of: the governmental entity's high-risk processing activities.

Definition – Utah Code § 63A-19-101(17)(a) and (b):

- (a) “**High-risk processing activities**” means a governmental entity’s processing of personal data that may have a significant impact on an individual's privacy interests, based on factors that include:
- (i) the sensitivity of the personal data processed;
 - (ii) the amount of personal data being processed;

- (iii) the individual's ability to consent to the processing of personal data; and
- (iv) risks of unauthorized access or use.

(b) High-risk processing activities may include the use of:

- (i) facial recognition technology
- (ii) automated decision making
- (iii) profiling
- (iv) genetic data
- (v) biometric data
- (vi) geolocation data.

4.1 High-Risk Activities:

Select all applicable high-risk processing activities your entity engages in and provide a brief description of the purposes and uses of each activity.

☐ **Facial recognition technology**

Explanation of Purpose:

☐ **Automated decision making**

Explanation of Purpose:

☐ **Profiling (e.g., behavioral or predictive analysis)**

Explanation of Purpose:

☐ **Genetic data processing**

Explanation of Purpose:

☐ **Biometric data processing (e.g., fingerprints, voice, iris scans)**

Explanation of Purpose:

☐ **Geolocation data processing**

Explanation of Purpose:

4.2 Additional high-risk activities (not listed above):

List any other processing activities your entity has identified as high-risk under the statutory definition and a brief description of the purposes and uses of each.

[Insert narrative or list here]

Section 5: Personal Data Sharing, Selling, and Purchasing

5.1 Personal Data Sharing, Selling, and Purchasing

Fulfills requirements of Subsections 63A-19-401.3(1)(c) and (d):

The chief administrative officer of each governmental entity shall prepare a report that includes: **a list of the types of personal data the governmental entity currently shares, sells, or purchases and the legal basis for sharing, selling, or purchasing personal data.**

Using the checkboxes below identify whether, and the types of, personal data that your governmental entity shares, sells, or purchases and provide a summary of the legal basis for the sharing, selling, or purchasing.

Types of Personal Data	Share, Sell and Purchase Status	Legal Basis for Sharing, Selling or Purchasing
Basic Identification & Contact Information <ul style="list-style-type: none">● Full Name● Date of Birth● Place of Birth● Gender● Age	<input type="checkbox"/> Share <input type="checkbox"/> Sell	

<ul style="list-style-type: none"> ● Government-Issued Identifiers: <ul style="list-style-type: none"> ○ Social Security Number ○ Driver's License or State ID Number ○ Passport Number ○ Other national or government-assigned IDs ● Contact Information: <ul style="list-style-type: none"> ○ Home Address ○ Email Address(es) ○ Phone Number(s) ○ Mailing Address (if different from home address) 	<input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Demographic & Personal Characteristics ● Race or Ethnicity ● Marital Status ● Nationality or Citizenship ● Language Preferences ● Household Information <ul style="list-style-type: none"> ○ Household Size ○ Household Composition 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	

<ul style="list-style-type: none"> ● Employment & Professional Information ● Job Title and Position ● Employment History ● Employer Name ● Professional Credentials <ul style="list-style-type: none"> ○ Professional Licenses ○ Certifications ● Work Contact Information 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Financial Data ● Banking Details <ul style="list-style-type: none"> ○ Bank Account Numbers ○ Credit Card Numbers ● Tax Identification Numbers ● Income and Wage Data ● Credit Information <ul style="list-style-type: none"> ○ Credit Reports ○ Credit Scores ● Payment History 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Health and Medical Information 	<input type="checkbox"/> Share	

<ul style="list-style-type: none"> • Medical History • Diagnoses or Treatments • Mental Health Data • Health Insurance Information • Prescription Information • Disability Status 	<input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> • Education Information • School or Institution Attended • Student ID Numbers • Academic Records <ul style="list-style-type: none"> ○ Grades ○ Transcripts • Special Education Status • Disciplinary Records 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> • Government Program & Benefits Data • Program Participation (e.g., SNAP, Medicaid, TANF) • Eligibility Determinations • Benefit Amounts or Disbursements • Case Management Notes 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase	

<ul style="list-style-type: none"> ● Appeals/Decisions 	<input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Biometric Data ● Physical Biometrics <ul style="list-style-type: none"> ○ Fingerprints ○ Facial Recognition Data ○ Retina or Iris Scans ● Voiceprints ● Genetic Information: DNA or other genetic data 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Online & Digital Identifiers ● Network Identifiers <ul style="list-style-type: none"> ○ IP Addresses ○ Device IDs ● Tracking Technologies <ul style="list-style-type: none"> ○ Cookies ○ Browser Fingerprints ● Location Data (e.g., GPS, precise geolocation) ● Login Credentials (e.g., usernames, hashed passwords) ● Online Activity Logs 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	

<ul style="list-style-type: none"> ● Social Media Handles 		
<ul style="list-style-type: none"> ● Criminal or Legal Information ● Arrest Records ● Conviction History ● Court Records ● Probation or Parole Status ● Incarceration Records 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Vehicle & Property Data ● Vehicle Information <ul style="list-style-type: none"> ○ Vehicle Registration ○ VIN Numbers ● Property Ownership <ul style="list-style-type: none"> ○ Property Ownership or Deed Information ○ Property Tax Records ● Utility Usage Data 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Photographic or Video Data ● Surveillance Footage 	<input type="checkbox"/> Share <input type="checkbox"/> Sell	

<ul style="list-style-type: none"> ● Correspondence <ul style="list-style-type: none"> ○ Emails or Written Correspondence ○ Call Transcripts or Recordings ● Case Notes related to complaints or service requests ● 	<input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Other <p>Explain:</p> <hr/>	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	

5.2 Personal Data Recipients and Sources

Fulfills requirements of Subsections 63A-19-401.3(1)(e)(i), (ii), and (iii):

The chief administrative officer of each governmental entity shall prepare a report that includes: **the category of individuals or entities with whom, to whom, and from whom the governmental entity shares, sells, or purchases personal data.**

Mark all that apply:

Processing Activity	Categories of Recipients or Sources
Personal Data Shared With:	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities:</p> <p><input type="checkbox"/> State, Local, Federal, or Tribal Governmental Entities</p> <p><input type="checkbox"/> Law Enforcement Agencies</p> <p><input type="checkbox"/> Judicial or Court Systems</p> <p><input type="checkbox"/> Legislative Bodies or Policy Research Organizations</p> <p><input type="checkbox"/> Regulatory Agencies</p> <p><input type="checkbox"/> Professional Licensing Boards</p> <p>II. International Governmental Entities:</p> <p><input type="checkbox"/> Foreign Governments or International Organizations</p> <p><input type="checkbox"/> Public Services & Emergency:</p> <p><input type="checkbox"/> Emergency Services / Disaster Response Agencies</p> <p><input type="checkbox"/> Public Utilities or Infrastructure Partners</p> <p>III. Public Disclosure:</p> <p><input type="checkbox"/> Public Disclosure / Open Records Releases</p> <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors:</p> <p><input type="checkbox"/> Third-Party Service Providers / Contractors / Vendors</p> <p><input type="checkbox"/> Cloud Service Providers / Hosting Platforms</p> <p><input type="checkbox"/> Technology Integrators or Software Developers</p>

	<p>II. Data & Marketing:</p> <p><input type="checkbox"/> Private Sector / Commercial Companies</p> <p><input type="checkbox"/> Data Brokers / Aggregators</p> <p><input type="checkbox"/> Social Media Platforms</p> <p>III. Financial & Insurance:</p> <p><input type="checkbox"/> Credit Bureaus or Financial Institutions</p> <p><input type="checkbox"/> Insurance Providers</p> <p>IV. Healthcare:</p> <p><input type="checkbox"/> Healthcare Providers or Health Information Exchanges</p> <p>V. Media:</p> <p><input type="checkbox"/> Media or News Organizations</p> <p>Research, Education, and Nonprofit Entities</p> <p><input type="checkbox"/> Research Institutions / Universities</p> <p><input type="checkbox"/> Educational Institutions</p> <p><input type="checkbox"/> Nonprofit Organizations</p> <p><input type="checkbox"/> Non-Governmental Watchdogs / Advocacy Groups</p> <p>Individuals and Oversight</p> <p><input type="checkbox"/> Individuals (e.g., data subjects or their authorized representatives)</p> <p><input type="checkbox"/> Auditors / Oversight Bodies</p> <p>Other/Not Applicable (N/A)</p> <p><input type="checkbox"/> Other (Specify as needed)</p>
--	---

	<input type="checkbox"/> N/A (Indicate if no data is shared with or received from any of these categories)
Personal Data Sold To:	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities:</p> <p><input type="checkbox"/> State, Local, Federal, or Tribal Governmental Entities</p> <p><input type="checkbox"/> Law Enforcement Agencies</p> <p><input type="checkbox"/> Judicial or Court Systems</p> <p><input type="checkbox"/> Legislative Bodies or Policy Research Organizations</p> <p><input type="checkbox"/> Regulatory Agencies</p> <p><input type="checkbox"/> Professional Licensing Boards</p> <p>II. International Governmental Entities:</p> <p><input type="checkbox"/> Foreign Governments or International Organizations</p> <p><input type="checkbox"/> Public Services & Emergency:</p> <p><input type="checkbox"/> Emergency Services / Disaster Response Agencies</p> <p><input type="checkbox"/> Public Utilities or Infrastructure Partners</p> <p>III. Public Disclosure:</p> <p><input type="checkbox"/> Public Disclosure / Open Records Releases</p> <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors:</p> <p><input type="checkbox"/> Third-Party Service Providers / Contractors / Vendors</p> <p><input type="checkbox"/> Cloud Service Providers / Hosting Platforms</p> <p><input type="checkbox"/> Technology Integrators or Software Developers</p>

	<p>II. Data & Marketing:</p> <p><input type="checkbox"/> Private Sector / Commercial Companies</p> <p><input type="checkbox"/> Data Brokers / Aggregators</p> <p><input type="checkbox"/> Social Media Platforms</p> <p>III. Financial & Insurance:</p> <p><input type="checkbox"/> Credit Bureaus or Financial Institutions</p> <p><input type="checkbox"/> Insurance Providers</p> <p>IV. Healthcare:</p> <p><input type="checkbox"/> Healthcare Providers or Health Information Exchanges</p> <p>V. Media:</p> <p><input type="checkbox"/> Media or News Organizations</p> <p>Research, Education, and Nonprofit Entities</p> <p><input type="checkbox"/> Research Institutions / Universities</p> <p><input type="checkbox"/> Educational Institutions</p> <p><input type="checkbox"/> Nonprofit Organizations</p> <p><input type="checkbox"/> Non-Governmental Watchdogs / Advocacy Groups</p> <p>Individuals and Oversight</p> <p><input type="checkbox"/> Individuals (e.g., data subjects or their authorized representatives)</p> <p><input type="checkbox"/> Auditors / Oversight Bodies</p> <p>Other/Not Applicable (N/A)</p> <p><input type="checkbox"/> Other (Specify as needed)</p>
--	---

	<input type="checkbox"/> N/A (Indicate if no data is shared with or received from any of these categories)
Personal Data Purchased From:	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities:</p> <p><input type="checkbox"/> State, Local, Federal, or Tribal Governmental Entities</p> <p><input type="checkbox"/> Law Enforcement Agencies</p> <p><input type="checkbox"/> Judicial or Court Systems</p> <p><input type="checkbox"/> Legislative Bodies or Policy Research Organizations</p> <p><input type="checkbox"/> Regulatory Agencies</p> <p><input type="checkbox"/> Professional Licensing Boards</p> <p>II. International Governmental Entities:</p> <p><input type="checkbox"/> Foreign Governments or International Organizations</p> <p><input type="checkbox"/> Public Services & Emergency:</p> <p><input type="checkbox"/> Emergency Services / Disaster Response Agencies</p> <p><input type="checkbox"/> Public Utilities or Infrastructure Partners</p> <p>III. Public Disclosure:</p> <p><input type="checkbox"/> Public Disclosure / Open Records Releases</p> <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors:</p> <p><input type="checkbox"/> Third-Party Service Providers / Contractors / Vendors</p> <p><input type="checkbox"/> Cloud Service Providers / Hosting Platforms</p> <p><input type="checkbox"/> Technology Integrators or Software Developers</p>

	<p>II. Data & Marketing:</p> <p><input type="checkbox"/> Private Sector / Commercial Companies</p> <p><input type="checkbox"/> Data Brokers / Aggregators</p> <p><input type="checkbox"/> Social Media Platforms</p> <p>III. Financial & Insurance:</p> <p><input type="checkbox"/> Credit Bureaus or Financial Institutions</p> <p><input type="checkbox"/> Insurance Providers</p> <p>IV. Healthcare:</p> <p><input type="checkbox"/> Healthcare Providers or Health Information Exchanges</p> <p>V. Media:</p> <p><input type="checkbox"/> Media or News Organizations</p> <p>Research, Education, and Nonprofit Entities</p> <p><input type="checkbox"/> Research Institutions / Universities</p> <p><input type="checkbox"/> Educational Institutions</p> <p><input type="checkbox"/> Nonprofit Organizations</p> <p><input type="checkbox"/> Non-Governmental Watchdogs / Advocacy Groups</p> <p>Individuals and Oversight</p> <p><input type="checkbox"/> Individuals (e.g., data subjects or their authorized representatives)</p> <p><input type="checkbox"/> Auditors / Oversight Bodies</p> <p>Other/Not Applicable (N/A)</p> <p><input type="checkbox"/> Other (Specify as needed)</p>
--	---

	<input type="checkbox"/> N/A (Indicate if no data is shared with or received from any of these categories)
--	--

Section 6: Privacy Training Completion

Fulfills requirement of Subsection 63A-19-401.3(1)(f):

The chief administrative officer of each governmental entity shall prepare a report that includes: **the percentage of the governmental entity's employees that have fulfilled the data privacy training requirements described in Section 63A-19-401.2.**

What percentage of your entity's employees have completed the required privacy training requirements described in Section 63A-19-401.2?

<i>Enter %</i>

Section 7: Non-Compliant Processing Activities (Must be completed by Dec 31, 2027)

Fulfills requirement of Subsections 63A-19-401(2)(a)(iv)(D) and 63A-19-401.3(1)(g):

The chief administrative officer of each governmental entity shall prepare a report that includes: **a description of any non-compliant processing activities identified under Subsection 63A-19-401(2)(a)(iv) and the governmental entity's strategy for bringing those activities into compliance with Part 4 of the Government Data Privacy Act.**

Have any non-compliant processing activities been identified pursuant to Utah Code § 63A-19-401(2)(a)(iv)?

☐ *Yes*

☐ *No*

If yes, provide details:

<i>Processing Activity Name</i>	<i>Processing Activity Type</i>	<i>Issues Identified</i>	<i>Strategies for Compliance</i>	<i>Estimated Completion Date</i>

Certification

Certification must be completed by the governmental entity's chief administrative officer.

I, the undersigned, certify that the information provided in this report is accurate to the best of my knowledge.

Name: _____

Signature: _____

Date: _____

EXHIBIT B
CITY OF KEARNS WEBSITE PRIVACY NOTICE

Draft Template – Website Privacy Notice

Disclaimer—

The following document is intended to be a draft website privacy notice template that a governmental entity may use as a baseline in creating its own website privacy notice. An entity that uses the template must revise and refine the template to be specific to the particular entity; this includes reformatting and accounting for any relevant laws, regulations, rules, policies, etc. The template is not legal guidance and should be reviewed and discussed with an entity's legal counsel to determine applicability and compliance. See Utah Code § 63A-19-402.5.

Template Option 1 – List Form

*(The website privacy notice or a link to a separate webpage containing the notice should be prominently posted on the homepage of the government website.)

Website Privacy Notice

[*Name of governmental entity*] is committed to protecting the privacy of individuals who access its websites. The notice informs those accessing [*name of governmental entity*] websites about what user data¹ is collected, why it is collected, and how they can update and manage personal data² or user data.

I. Website Operational Information

The [*name of governmental entity*] is responsible for this website.

The [*name of governmental entity*] may be contacted by:

Telephone: [*contact info of the governmental entity as applicable*]

Email: ...

II. Individual's Personal Data and User Data

By contacting the [*name of governmental entity*] an individual may:

¹ "User data" means any information about a user that is automatically collected by a government website when a user accesses the government website.

(b) "User data" includes information that identifies:

(i) a user as having requested or obtained specific materials or services from a government website;

(ii) Internet sites visited by a user;

(iii) the contents of a user's data-storage device;

(iv) any identifying code linked to a user of a government website; and

(v) a user's:

(A) IP or Mac address; or

(B) session ID. (Utah Code § 63A-19-101(38)(a) and (b)).

² "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual. (Utah Code § 63A-19-101(24)).

- seek access to the individual's personal data or user data;
- request to correct or amend the individual's personal data or user data; or
- if the individual qualifies as an at-risk employee³, request that the individual's personal data be classified as a private record.

III. Data Privacy Ombudsperson

An individual may contact the Data Privacy Ombudsperson to file a complaint about a privacy practice of a governmental entity by using the following contact information:

Email: privacyombudsperson@utah.gov

*(If the website collects user data, the website privacy notice should also include the following information.)

IV. Website User Data

This website may use website tracking technology⁴ to collect user data. Website tracking technology used on this website includes:

- *[List/describe any website tracking technology used]*
- ...

User data collected on this website includes:

- *[List/describe types of user data collected]*
- ...

V. Purposes and Uses for User Data

The *[name of governmental entity]* collects user data for the following purposes:

- *[List/describe intended purposes of the user data]*
- ...

Uses of user data include:

- *[List/describe intended uses of the user data]*

³ (a) "At-risk government employee" means a current or former:

- (i) peace officer as specified in Section 53-13-102;
- (ii) state or federal judge of an appellate, district, justice, or juvenile court, or court commissioner;
- (iii) judge authorized by Title 39A, Chapter 5, Utah Code of Military Justice;
- (iv) judge authorized by Armed Forces, Title 10, United States Code;
- (v) federal prosecutor;
- (vi) prosecutor appointed pursuant to Armed Forces, Title 10, United States Code;
- (vii) law enforcement official as defined in Section 53-5-711;
- (viii) prosecutor authorized by Title 39A, Chapter 5, Utah Code of Military Justice; or
- (ix) state or local government employee who, because of the unique nature of the employee's regular work assignments or because of one or more recent credible threats directed to or against the employee, would be at immediate and substantial risk of physical harm if the employee's personal information is disclosed. (Utah Code § 63G-2-303(1)(a)).

⁴ (39) "Website tracking technology" means any tool used by a government website to:

- (a) monitor a user's behavior; or
- (b) collect user data. (Utah Code § 63A-19-101(39)).

- ...

VI. Sharing and Selling of User Data

The classes of persons and entities with whom the *[name of governmental entity]* shares user data includes:

- *[List/describe the classes of persons and entities with whom user data is shared]*
- ...

The classes of persons and entities to whom the *[name of governmental entity]* sells user data includes:

- *[List/describe the classes of persons and entities to whom user data is sold]*
- ...

VII. Record Series

The user data collected on this website is included in Record Series #_____ *(Include hyperlink)*

Template Option 2 – Paragraph Form

*(The website privacy notice or a link to a separate webpage containing the notice should be prominently displayed on the homepage of the government website. Depending on how an entity decides to provide the website privacy notice—either on the homepage or a link to a separate webpage—the following language should be revised accordingly.) See Utah Code § 63A-19-402.5.

The *(name of governmental entity)* is committed to protecting your privacy. To find out more about your privacy interests and what user data may be collected when you visit this website, click here: *(include a link to a separate webpage with the website privacy notice)*.

Website privacy notice listed on separate webpage, as applicable:

Website Privacy Notice

This website is operated by the *(name of governmental entity)*. You may contact the *(name of governmental entity)* at *(contact info for the governmental entity)*. By contacting the *(name of governmental entity)* you may:

- access your personal dataⁱ or your user dataⁱⁱ;
- request to correct or amend your personal data or user data; or
- if you qualify as an at-risk employeeⁱⁱⁱ, request that your personal data be classified as a private record.

If you are concerned with the data privacy practices of a governmental entity, you may file a complaint with the Data Privacy Ombudsperson by sending an email to privacyombudsperson@utah.gov.

*(If the website collects user data, the website privacy notice should also include the following information.)

This website uses *(describe the website tracking technology^{iv} used)* to collect *(describe type of user data)*. This user data is used to *(describe the intended purposes and uses of the user data)*. Your user data may be shared with *(describe the classes of persons and governmental entities with whom the user data is shared with)*. Your user data *is/is not* sold to *(describe the classes of persons and governmental entities to whom the user data is sold, if user data is not sold indicate that user data is not sold)*. The user data collected is included in Record Series # _____ *(include hyperlink)*.

ⁱ "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual. (Utah Code § 63A-19-101(24)).

ⁱⁱ "User data" means any information about a user that is automatically collected by a government website when a user accesses the government website. (Utah Code § 63A-19-101(38)).

ⁱⁱⁱ "At-risk government employee" means a current or former:

- peace officer as specified in Section 53-13-102;
- state or federal judge of an appellate, district, justice, or juvenile court, or court commissioner;
- judge authorized by Title 39A, Chapter 5, Utah Code of Military Justice;
- judge authorized by Armed Forces, Title 10, United States Code;
- federal prosecutor;
- prosecutor appointed pursuant to Armed Forces, Title 10, United States Code;
- law enforcement official as defined in Section 53-5-711;
- prosecutor authorized by Title 39A, Chapter 5, Utah Code of Military Justice; or
- state or local government employee who, because of the unique nature of the employee's regular work assignments or because of one or more recent credible threats directed to or against the employee, would be at immediate and substantial risk of physical harm if the employee's personal information is disclosed. (Utah Code § 63G-2-303(1)(a)).

^{iv} (39) "Website tracking technology" means any tool used by a government website to:

- (a) monitor a user's behavior; or
- (b) collect user data. (Utah Code § 63A-19-101(39)).