Greater Salt Lake Municipal Services District (MSD)

Privacy Policy

Approved by MSD Board of Trustees: November 12, 2025

Effective Date: November 12, 2025

Legal Authorities
- Division of Archives and Records Services (DARS) – Utah Code § 63A-12-100 et seq.
- Government Data Privacy Act (GDPA) – Utah Code § 63A-19-101 et seq.
- Government Records Access and Management Act (GRAMA) – Utah Code § 63G-2-101 et seq.
- Management of Records and Access to Records – Utah Administrative Code R13-2.
- Division of Technology Services (DTS) Information Security Policy 5000-0002.

Greater Salt Lake Municipal Services District (MSD) Privacy Policy

1. Purpose

This policy serves to document the Greater Salt Lake Municipal Services District (MSD) privacy program, which includes policies, practices, and procedures for the processing of personal data in accordance with Utah Code § 63A-19-401(2)(a), and which aligns with the records management and data governance requirements provided in both GRAMA and DARS. Where applicable, this policy will refer to a more specific or detailed policy, procedure, or guidance that addresses a particular practice that MSD has developed.

2. Guiding Principles

This policy consolidates privacy practices, outlines governance roles and responsibilities, and ensures compliance with generally applicable records management, data protection, and data privacy obligations. It is designed to safeguard individual privacy rights, promote transparency, maintain the integrity and security of personal data, and ensure accountability across MSD. This policy is meant to guide further alignment of MSD with the State Data Privacy Policy as detailed in Utah Code § 63A-19-102.

3. Scope

This policy applies to all MSD employees involved in the management, creation, and maintenance of records or who have access to personal data as part of their job duties. This policy also applies to all contractors of MSD that process or have access to personal data as part of the contractor's duties under an agreement with MSD pursuant to Utah Code § 63A-19-401(4).

> **Formatted:** Font color: Accent 2

4. Definitions

"Classification," "classify," and their derivative forms mean determining whether a record series, record, or information within a record is public, private, controlled, protected, or exempt from disclosure under Subsection § 63G-2-201(3)(b).[2]

"Cookie" means "Technology that records a user's information and activity when the user accesses websites. Cookies are used by website owners, third parties, and sometimes threat actors to gather user data."[3]

"Data breach" means— the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by a governmental entity, unless the governmental entity concludes, according to standards established by the Cyber Center, that there is a low probability that personal data has been compromised."[4]

"Designation," "designate," and their derivative forms mean indicating, based on a governmental entity's familiarity with a record series or based on a governmental entity's review of a reasonable sample of a record series, the primary classification that a majority of records in a record series would be given if classified and the classification that other records typically present in the record series would be given if classified.[5]

"Device fingerprinting" means collecting attributes of a user's device configurations to create a trackable profile for the device.

"Individual" means a human being.[6]

"Key logger" means "a program designed to record which keys are pressed on a computer keyboard..."[7]

"Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.[8]

"Processing activity" means any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.[9]

"Record" means the same as that term is defined at Utah Code § 63G-2-103(25).[10]

"Record series" means a group of records that may be treated as a unit for purposes of designation, description, management, or disposition.[11]

"Records officer" means the individual appointed by the chief administrative officer of each governmental entity, or the political subdivision to work with State Archives in the care, maintenance, scheduling, designation, classification, disposal, and preservation of records.[12]

"Schedule," "scheduling," and their derivative forms mean the process of specifying the length of time each record series should be retained by a governmental entity for administrative, legal, fiscal, or historical purposes and when each record series should be transferred to the State Archives or destroyed.[13]

---

[5] Utah Code § 63G-2-103(7)

[7] National Institute of Standards and Technology, Computer Security Resource Center, Glossary.
https://csrc.nist.gov/glossary/term/key_logger#:~:text=Definitions%3A,NIST%20SP%20800%2D82r3
[8] Utah Code § 63A-19-101(13)
[9] Utah Code § 63A-19-101(14)
[10] Only the citation to the definition of "record" is provided here due to the length of the definition.
[11] Utah Code § 63G-2-103(26)
[12] Utah Code § 63G-2-103(27)
[13] Utah Code § 63G-2-103(28)

5. Governance

5.1. Chief Administrative Officers (CAOs)

A. The Chief Executive Officer of MSD is Marla Howard, General Manager. Marla is tasked with fulfilling the duties outlined in Utah Code § 63A-12-103.

B. The Executive Director may assign responsibility for the duties outlined in Utah Code § 63A-12-103 to one, or among several, CAOs as the Executive Director sees fit.

C. The designation of the CAO(s) shall be reported to the Utah Division of Archives and Records Services (Archives) within 30 days of the designation.

D. If responsibility for the duties outlined in Utah Code § 63A-12-103 are divided between more than one CAO, such specification should be reported to Archives along with the designation.

E. The designation of, and responsibilities assigned to, a CAO shall be reviewed and confirmed by MSD on an annual basis.

5.2. Appointed Records Officers (AROs)

A. Designated CAO(s) shall appoint one or more individuals to serve as records officers in fulfilling the duties of working with Archives and the Office of Data Privacy in the care, maintenance, scheduling, disposal, classification, designation, access, privacy, and preservation of records.[14]

B. A designated CAO may assign responsibility for the duties of appointed records officers to one, or among several, officers as the CAO deems appropriate.

C. The appointment of records officers shall be reported to Archives within 30 days of the appointment.

D. If responsibility for the duties of appointed records officers are divided between more than one officer, such specification should be reported to Archives along with the appointment.

E. The appointment of, and responsibilities assigned to, a records officer shall be reviewed and confirmed by MSD on an annual basis.

6. Records Series

6.1. Records and Records Series

A. MSD shall create and maintain records and records series in accordance with the requirements provided in DARS and GRAMA in addition to correlated guidance issued by Archives.

B. MSD shall appropriately designate and classify records and records series in accordance with the requirements provided in DARS and GRAMA.

C. CAO(s) shall be responsible for submitting a proposed retention schedule for each type of material defined as a record under GRAMA to the state archivist for review and final approval by the Records Management Committee (RMC).

D. Upon approval by the RMC, MSD shall maintain and dispose of records in strict accordance with the approved retention schedule. In instances where MSD has not received an approved retention schedule for a specific type of record, the general retention schedule maintained by the state archivist shall govern the retention and disposition of those records.

6.2. Record Series Privacy Annotation

A. Each MSD department shall perform a privacy annotation for each record series that contains personal data pursuant to Utah Code § 63A-12-115.

B. Privacy annotations shall include:
   a. the legal authority under which personal data is processed;
   b. the purposes and uses for the personal data; and
   c. the types of personal data that may be processed within the record series.

C. Privacy annotations shall be conducted and reported in accordance with additional requirements provided by Archives via administrative rule.

---

[14] Utah Code § 63A-12-103(2)

7. Awareness & Training

7.1. Departmental Data Privacy Training

A. The CAO of MSD shall ensure that all employees that have access to personal data as part of the employees' work duties complete a data privacy training program within 30 days after beginning employment and at least once in each calendar year.

B. The CAO of MSD is responsible for monitoring completion of data privacy training by MSD employees.

7.2. Agency-Specific Training

A. In addition to the general privacy awareness training, agencies may create and require employees to complete agency-specific privacy training tailored to the unique privacy needs, practices, and requirements of the agency.

7.3. Appointed Records Officer Training and Certification

A. The CAO of MSD shall ensure that, on an annual basis, all appointed records officers successfully complete online training on the provisions of GRAMA and obtain certification from Archives in accordance with Utah Code § 63A-12- 110.

B. The CAO of MSD shall, on an annual basis, review and confirm the certification of all appointed records officers.

C. GRAMA Access AROs: AROs who handle GRAMA transparency responsibilities are required to complete the GRAMA transparency training and obtain certification from Archives in accordance with Utah Code § 63A-12-110.

D. Records Management and Privacy AROs: AROs specializing in records management or privacy are required to complete both records management and GRAMA transparency training, as well as obtaining the corresponding certifications.

8. Identify

8.1. Inventorying

A. The CAO of MSD shall maintain a comprehensive inventory of:

   a. All IT systems that may process state or federal data which the state owns or is responsible for, using the standard process that DTS provides.[15]

   b. All records and record series that contain personal data and the types of personal data included in the records and record series.[16]

   c. All processing activities, the inventory of which shall include:

      i. Non-compliant processing activities—pursuant to the GDPA—that were implemented prior to May 1, 2024, and a prepared strategy for bringing the non-compliant processing activity into compliance by no later than January 1, 2027;[17] and

      ii. All processing activities implemented after May 1, 2024, with documentation confirming compliance status.

8.2. Information Technology Privacy Impact Assessment

A. The CAO of MSD shall ensure that the division completes a Privacy Impact Assessment (PIA) for all IT systems that may process personal data prior to the initiation of data processing in the IT system as required under DTS Information Security Policy 5000-0002.

B. The responsible CAO shall use the PIA template that is created and maintained by the Chief Privacy Officer and which is approved by the Chief Information Officer pursuant to DTS Information Security Policy 5000-0002.

C. CAOs must maintain a copy of each completed assessment for a period of four years to provide audit documentation and ensure accountability in privacy practices.

---

[15] DTS Information Security Policy 5000-0002, section 2.4.2.1
[16] Utah Code §§ 63A-12-104 and 63A-12-115
[17] Utah Code § 63A-19-401

9. Transparency

9.1. Website Privacy Policy

A. The CAO of MSD shall create and maintain privacy policies on their websites as outlined in Utah Code § 63D-2-103 ~~and Utah Admin. Code R895-8~~.

B. The CAO of MSD shall ensure that personal data related to a user of MSD website is not collected unless MSD website complies with Utah Code § 63D-2-103(2).

C. The CAO MSD shall ensure that all websites of MSD contain a privacy policy statement that discloses:

    a. The identity of the governmental website operator;
    b. How the governmental website operator may be contacted;
    c. The personal data collected by the governmental entity;
    d. The practices related to disclosure of personal data collected by the governmental entity and/or the governmental website operator; and
    e. The procedures, if any, by which a user of a governmental entity may request:
        i. Access to the user's personal data; and
        ii. Access to correct the user's personal data.
    f. A general description of the security measures in place to protect a user's personal data from unintended disclosure.

9.2. Privacy Notice

A. Employees shall only collect personal data from individuals if, on the day the personal data is collected, MSD has provided a privacy notice to an individual asked to furnish personal data that complies with Utah Code §§ 63G-2-601(2), 63A-19-402, 63D- 2-103(2)-(3), or other governing law, as applicable.

B. Such a personal data request privacy notice shall generally include[18]:

    a. the record series that the personal data will be included in;
    b. the reasons the person is asked to furnish the information;
    c. the intended purposes and uses of the information;
    d. the consequences for refusing to provide the information; and
    e. the classes of persons and entities that:
        i. share the information with MSD; or
        ii. receive the information from MSD on a regular or contractual basis.

10. Individual Requests

A. The CAO of MSD shall ensure that MSD has established appropriate processes and procedures that facilitate compliance with applicable governing law for handling the following privacy requests of individuals:

    a. Individual requests to access their personal data;

    b. Individual requests to amend or correct their personal data;

    c. Individual requests for an explanation of the purposes and uses of their personal data; and

    d. At-risk governmental employee requests to restrict access to their personal data.

B. The CAO MSD shall ensure that MSD has established processes for public access requests to inspect or copy MSD's records, which are not requests from an individual to access their personal data.[19]

C. The CAO [of each division of the Department] shall ensure that employees of MSD follow established business practices with respect to GRAMA.[20]

---

[18] Utah Code §§ 63G-2-601(2) and 63A-19-402.
[19] This is likely detailed in a specific Department policy.
[20] Dept. of Government Operations Internal Policy 01. Code of Conduct. Section 3.2 Managing Records and Information

11. Processing

11.1. Minimum Data Necessary

A. The CAO of MSD shall ensure that all programs within MSD obtain and process only the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose.[21]

B. The CAO of MSD shall ensure that all programs within MSD regularly review their data collection practices to ensure compliance with the data minimization requirement.

11.2. Record and Data Sharing or Selling Policy

A. MSD will only share or disclose personal data when there is appropriate legal authority. The sale of personal data is prohibited unless required by law.

B. Data sharing must comply with GRAMA or other governing laws and may include sharing with governmental entities, contractors, private providers, or researchers. Compliance with GRAMA or other governing law is contingent upon the purpose of the sharing, the parties involved, and the nature of the records.

C. The CAO is required to report annually to the Chief Privacy Officer on personal data sharing and selling activities, including types of data shared, the legal basis for sharing, and the entities receiving this data.

D. All contracts involving personal data must incorporate appropriate privacy protection terms. Written agreements for data sharing are recommended to ensure compliance with applicable laws and regulations.

11.3. Retention and Disposition of Records Containing Personal Data

A. Employees shall maintain, archive, and dispose of records, which includes all personal data, in accordance with an approved retention schedule.[22]

B. Employees shall comply with all other applicable laws or regulations related to retention or disposition of specific personal data held by the MSD or by a particular operating unit or program of the MSD.

---

[21] Utah Code § 63A-19-401(2)(c).
[22] Utah Code §§ 63G-2-604(1)(b) and 63A-19-404.

12. Information Security

12.1.   Incident Response

A. MSD adopts and follows the **DTS Cybersecurity Incident Response Plan** to manage and address all security incidents, including data breaches, and privacy violations.

B. Employees shall report all suspected security incidents, including non-IT incidents such as unauthorized access to physical records, to the **Enterprise Information Security Office (EISO)**. Any additional agency-specific response measures for non-IT incidents are the responsibility of the CAO of MSD to develop and implement as appropriate.

C. The CAO of MSD shall ensure compliance with all other applicable laws or regulations related to incident response and breach notification of specific personal data held by MSD.

12.2.   Breach Notification

A. MSD is required to provide notice to an individual or the legal guardian of an individual, if the individual's personal data is affected by a data breach in accordance with Utah Code § 63A-19-406.[23]

B. MSD is required to notify the Cyber Center and the state attorney general's office of a data breach affecting 500 or more individuals in accordance with Utah Code § 63A-19-405. MSD that experience a data breach affecting fewer than 500 individuals must create and report an internal incident report in accordance with Utah Code § 63A-19-405(5). These requirements are in addition to any other reporting requirement that MSD may be subject to.

C. The CAO of MSD that is subject to other breach notification requirements, such as those required for compliance with federal regulations, laws or other governing requirements (e.g., HIPAA or 42 CFR Part 2) are required to create and maintain their own [division] specific breach notification policies and procedures that meet the requirements of the applicable governing laws and regulations.

13. Surveillance

13.1.   Covert Surveillance

A. Employees may not establish, maintain, or use undisclosed or covert surveillance of individuals unless permitted by law.[24] Consistent with MSD policy, MSD does monitor and surveil organizational assets including, but not limited to, vehicles and computers. Surveillance may also occur in the form of facility security. Employees are notified and informed of these types of surveillance.

B. Employees are responsible for engaging with appropriate leadership for review—to include legal counsel where pertinent—of any activity that may be considered a type of surveillance.

C. The CAO of MSD shall ensure that surveillance activities are documented and that a PIA for the activity has been completed. Utah State GRAMA and Records Retention Rules

13.2.   Cookies, Fingerprinting, Key Loggers, and Tracking Technologies

MSD is committed to transparency and privacy protection for individuals that visit a website of MSD with regard to the use of any tracking technologies, including but not limited to cookies, device fingerprinting, key loggers, and other similar methods for monitoring or collecting information from website users.

A. **Cookies**
The use of cookies on MSD websites and digital services must comply with applicable privacy and security policies. Cookies should be limited to essential operational purposes, and any use of tracking or third-party cookies for analytics or similar functions must be disclosed clearly to users, with an option to consent where required by law.

B. **Device Fingerprinting**
Device fingerprinting is prohibited unless explicitly authorized by the CAO and where the legal basis or appropriate justification for such processing is documented in a privacy impact assessment. The purpose and extent of fingerprinting must be clearly defined, documented, and disclosed to users in a privacy notice or statement that complies with applicable legal requirements.

---

[23] Utah Code § 63A-19-401(2)(b).

C. **Key Loggers**

Key loggers are prohibited without specific authorization from the CAO and documented justification in the activity's PIA. Key loggers may only be used when there is a clearly defined operational need that complies with security standards and legal requirements, including appropriate user notice where required.

D. **Other Tracking Technologies**

The use of other tracking technologies, such as web beacons, pixel tags, or similar tools, is prohibited unless explicitly authorized by the CAO, and the legal basis for such tracking is documented in a PIA. Disclosure of these technologies must be included in user-facing privacy statements, with user consent obtained when required by law.

E. **User Notification and Consent**

MSD must ensure users are informed about the use of tracking technologies. A clear website privacy statement must explain the types of data collected, the purpose of the tracking, and how users can manage their preferences or consent. Any updates to tracking practices must be promptly reflected in the privacy statement.

F. **Data Security and Retention**

Data collected through authorized tracking technologies must be securely stored, with access limited to authorized personnel. Retention of this data must align with approved retention schedules, and the data should only be retained as long as necessary for the defined operational purpose.

14. Related Documents

- [Department of Government Operations Internal Policy 01. Code of Conduct. Section 3.2 Managing Records and Information.]
- [DTS Cybersecurity Incident Response Plan]
- [Dept. of Government Operations Internal Policy 01.]
- [Department policy on handling public records requests under GRAMA]

---

[24] Utah Code § 63A-19-401(2)(f).