STATE OF UTAH
OFFICE OF THE UTAH STATE AUDITOR

TINA M. CANNON
UTAH STATE AUDITOR

Ogden City

Privacy Audit Report

For the year ended December 31, 2025

Report No. PA-25-05

Office of the Utah State Auditor

Audit Leadership:
Tina M. Cannon, State Auditor
Warisara Watanawongworakula, CPA, CISA, Information Systems Audit Supervisor
Mark Meyer, CIPM, CompTIA Security+, Assistant State Privacy Auditor
Tristan Olcott, PNPT, CompTIA Security+, Cybersecurity Specialist

UTAH STATE CAPITOL, SUITE 260, SALT LAKE CITY, UT 84114, (801) 538-1025

Table of Contents

Management Letter No. PA-25-05 1

Findings & Recommendations 3

Finding 1. Incident and Breach Methodology 3

Finding 2. Retention and Disposition.....4

Finding 3. No Finalized Privacy Policy.....5

Finding 4. Privacy Training Program 6

Finding 5. Amendment and Correction Requests.....7

Finding 6. Incomplete Privacy Report.....8

Appendix A – Summary of Findings.....11

STATE OF UTAH
OFFICE OF THE UTAH STATE AUDITOR

TINA M. CANNON
UTAH STATE AUDITOR

Management Letter No. PA-25-05

October 6, 2026

To the Ogden City Council
and
Ben Nadolski, Mayor
Ogden City
2549 Washington Boulevard, #320
Ogden, UT 84401

Dear Mayor Nadolski,

As authorized under Utah Code §67-3-13(2)(f), the Office of the Utah State Auditor (OSA) conducted a privacy audit of Ogden City (City). The objective of the audit was to assess Ogden's overall compliance with the Utah Government Data Privacy Act (GDPA), Utah Code Title 63A, Chapter 19, and other applicable privacy requirements. The audit evaluated the City's privacy program and related controls over the collection, use, retention, disposition, and sharing of personal data, as well as privacy governance, training, notices, contractor oversight, and incident and breach response.

The procedures of this audit do not constitute an audit conducted in accordance with generally accepted auditing standards, the objectives of which would be the expression of an opinion on the City's compliance with applicable privacy requirements. Accordingly, we do not express such an opinion.

Methodology

To accomplish the audit objective, we performed the following procedures:

1. Reviewed applicable laws, regulations, and guidance relevant to governmental data privacy;
2. Reviewed selected City policies, procedures, training materials, privacy notices, data collection forms, vendor and application records, retention and disposition practices, data-sharing practices, and incident-response documentation;
3. Evaluated selected privacy-program controls and practices, including privacy governance and reporting, employee training, contract oversight, privacy notices, data minimization, data sharing, incident response, and required notifications; and
4. Interviewed selected City personnel to understand privacy responsibilities, data-handling practices, privacy-program implementation, and incident response.

Findings Overview

Our audit identified instances of noncompliance and control weaknesses in Ogden City's implementation of the Utah Government Data Privacy Act (GDPA). While a privacy program has been initiated, several elements related to incident response, data retention, policies, training, and reporting remain incomplete. The findings outline issues with incident and breach methodology, retention and disposition, the City's privacy program framework, privacy training, amendment and correction procedures, and annual privacy program reporting.

Our review was designed to assess the City's overall compliance with the GDPA and other applicable privacy requirements. The audit did not examine every form, system, process, transaction, or record. We used certain documents, practices, and samples to evaluate the City's privacy program and related controls. Accordingly, our findings reflect the conditions identified through the procedures performed and may not include every instance of noncompliance or control weakness.

Why These Findings Matter

City government systems handle sensitive personal information about individuals. Mishandling or improper access to this data can result in reputational harm, privacy violations, identity theft, or other misuse of personal information. Without effective monitoring and safeguards, privacy incidents may go undetected or unaddressed, increasing the risk that sensitive data will be accessed, used, or disclosed without authorization.

We appreciate the courtesy and assistance City personnel extended to us during the course of this engagement, and we look forward to a continuing professional relationship.

Sincerely,



Tina M. Cannon
Utah State Auditor

Findings & Recommendations

Finding 1. Incident and Breach Methodology

The City had documented incident and breach methodology content, but the materials reviewed were outdated (dated 2016), not fully governed, and did not clearly address both cyber and non-cyber privacy incidents.

Utah Code §63A-19-405 and 63A-19-406 establish breach-notification requirements when a reportable data breach occurs. These sections do not expressly require a formally approved written incident-response plan. However, current, governed, and operational incident and breach methodology helps support timely and consistent compliance. Such methodology should identify responsible roles, escalation paths, breach-evaluation steps, notification responsibilities, evidence-retention expectations, and records to be retained.

The incident-response documents reviewed included older or template-based content, unresolved placeholders, outdated terminology, and incomplete contact or governance information. The documented methodology included incident identification, escalation, investigation, evidence handling, breach evaluation, notification, and response procedures. However, interview responses indicated that the incident-response materials were older, needed updating, and were not clearly known to all relevant personnel. The City also did not demonstrate that the methodology was communicated to appropriate personnel or periodically reviewed or tested during the audit period.

This condition occurred because the City retained older incident-response documents without fully updating, approving, and governing them as current operational guidance. Interview responses also suggest reliance on institutional knowledge and informal escalation rather than a clearly maintained and communicated methodology. In addition, the documented methodology appeared primarily IT-oriented and did not clearly demonstrate how non-cyber privacy incidents would be identified, escalated, evaluated, documented, and retained.

Because the incident and breach methodology documents were outdated and not fully governed, the City runs the risk of inconsistencies and untimely or unsupported decisions. When the City has a reportable breach or other privacy incident, it is possible that personnel will not follow a consistent, current, authoritative process to comply with statute.

Recommendation

We recommend that the City formally update, approve, and maintain its incident and breach methodology documents so they reflect the City's current governance structure, terminology, responsible roles, escalation paths, breach-evaluation procedures, notification requirements, contact information, evidence-retention expectations, and response steps for both cyber and non-cyber

privacy incidents. We also recommend the City communicate the methodology to appropriate personnel and periodically review or test it.

Ogden City's Corrective Action Plan

The City is updating its incident and breach response procedures to reflect current governance, responsible roles and contacts, escalation, breach evaluation, legally required notifications, documentation and evidence retention, and both cyber and non-cyber privacy incidents. The City will approve updated incident response procedures by December 15, 2026, and communicate the procedures by December 31, 2026. The City will conduct and document a training by February 28, 2027.

Finding 2. Retention and Disposition

The City had records-management policies and provided examples of retention and disposition practices for selected records, media, and workflows. However, for several sampled personal-data holdings, documentation did not clearly identify both the applicable documented retention schedule and the disposition method to be used when the retention period ended. Interview responses also identified uncertainty regarding retention parameters for certain systems and the handling of personal data maintained outside official systems.

Pursuant to Utah Code §63A-19-404, a governmental entity that collects personal data shall retain and dispose of the personal data in accordance with a documented record retention schedule.

This condition occurred because the City had records-management policies and certain department-level practices in place but did not demonstrate a consistently documented linkage between sampled personal-data holdings, applicable retention schedules, and disposition methods across the systems and workflows reviewed.

Without consistent linkage between personal-data holdings and documented retention schedules, the City has increased risk that personal data will be retained or disposed of inconsistently and that the City will be unable to demonstrate compliance with statutory retention and disposition requirements across relevant records and copies.

Recommendation

We recommend that the City document the applicable retention schedule and disposition method for personal-data holdings, including official system records and exported, duplicate, temporary, user-created, or locally stored copies where those copies are retained by the City.

The City should implement a process to periodically review selected systems, forms, and workflows to confirm that personal-data holdings are linked to approved retention schedules and disposition methods.

Ogden City's Corrective Action Plan

The City began an inventory of department forms and information-collection processes on October 8, 2026, and held the first Privacy Committee meeting on October 15, 2026. The inventory will identify where personal data is collected, stored, copied, shared, and retained, including in paper, electronic, online, third-party, and informal processes. For each personal-data holding, the City will document the responsible department, applicable retention scheduled, and method for disposing of the data when the retention period ends. This will include copies retained by the City outside official systems, such as exports, duplicates, temporary files, and user-created or locally stored copies.

Departments will complete their inventories by January 31, 2027. The City will document the applicable retention schedule and disposition method for high-risk and high-volume holdings by March 31, 2027, and complete the remaining holdings and an initial compliance review by June 30, 2027. The City will periodically review selected systems, forms, and workflows to confirm that schedules and disposition methods remain current and are followed.

Finding 3. No Finalized Privacy Policy

The City had privacy-supporting policies and draft privacy-policy content but did not demonstrate that it had finalized and formally adopted a citywide privacy policy framework applicable across City operations during the audit period. Although the City provided multiple policies and procedures relevant to privacy, the draft citywide privacy policy remained unapproved and unpublished during the audit period and therefore was not considered evidence of an adopted City policy in effect during the audit period.

Pursuant to Utah Code §63A-19-401(2)(a), a governmental entity was required to initiate a data privacy program before December 31, 2025. Utah Code §63A-19-102 further states that individuals have a fundamental interest in and expectation of privacy regarding personal data provided to a governmental entity. A formally adopted citywide privacy policy framework helps implement those requirements consistently across City operations by establishing privacy responsibilities, processing expectations, access limitations, retention expectations, and accountability.

Privacy efforts were largely led through the IT function, and the departure of the former IT Director affected continuity of privacy leadership while the City's broader privacy governance structure was still being formalized. As a result, responsibility for finalizing and formally adopting the citywide privacy policy framework was not clearly established.

Without a formal privacy policy, the City risks inconsistent privacy standards and unclear accountability across departments. Departments may rely on different policies or informal practices rather than a single authoritative framework, increasing the risk that privacy responsibilities are not consistently assigned, communicated, or monitored.

Recommendation

We recommend Ogden City finalize, approve, and implement a citywide privacy policy framework applicable across City operations. This framework should:

- Identify privacy roles and responsibilities;
- Establish expectations for minimum-necessary processing, purpose limitation, collection notices, retention and disposition, access control, vendor handling of personal data, incident escalation, and prohibited uses; and
- Identify how the City will maintain and periodically review the policy framework for continued accuracy and alignment with applicable privacy laws and requirements.

Ogden City's Corrective Action Plan

The City will finalize, approve, and implement its citywide privacy policy by November 30, 2026, and communicate it citywide by that date. The policy will establish privacy roles and responsibilities and set expectations for minimum-necessary processing, purpose limitation, collection notices, retention and disposition, access controls, vendor handling of personal data, incident escalation, and prohibited uses. It will also describe how the City will maintain and periodically review the policy for accuracy and alignment with applicable privacy laws and requirements. The City will designate a Privacy Officer with executive oversight by the CAO.

Finding 4. Privacy Training Program

Pursuant to Utah Code §63A-19-401.2, a governmental entity is required to provide data privacy training to employees who have access to personal data as part of their work duties and to supervisors who supervise employees with access to personal data. These employees and supervisors are required to complete training within 30 days after beginning employment and at least once in each calendar year. The training must address data privacy best practices, obligations, and responsibilities; the relationship between privacy, records management, and security; the privacy interests and requirements of the Government Data Privacy Act (GDPA); and, as applicable, the privacy interests and requirements of the Government Records Access and Management Act (GRAMA). The governmental entity is also responsible for ensuring completion and reporting training completion as part of its annual privacy program report.

To fulfill this requirement, the City identified Utah Office of Data Privacy's Statewide Privacy Awareness Training as its privacy training, which appeared to address the required privacy topics.

The 2025 Town Data Privacy Assessment Report stated that approximately 80 percent of Ogden City employees with access to personal data received privacy training. Accordingly, the City did not demonstrate that all employees and supervisors completed training as required. Interview responses

indicated that the City did not provide the required annual training during calendar year 2025, due to privacy training being assigned on a fiscal year basis.

Covered employees may not receive privacy training on the schedule required by law, increasing the risk of inconsistent understanding of privacy, records, and security responsibilities.

Recommendation

We recommend that the City align its privacy training process with Utah Code §63A-19-401.2 by ensuring that covered employees complete privacy training within 30 days after beginning employment and at least once each calendar year.

Ogden City's Corrective Action Plan

The City will provide privacy training to employees who access personal data and supervisors who oversee those employees. Covered employees will complete training within 30 days after beginning employment or being assigned covered duties, and at least once each calendar year. The City will assign the 2026 training by November 15, 2026, with completion due by December 31, 2026, and will monitor completion, follow up on overdue assignments, retain training records, and report the completion percentage in its annual privacy report.

Finding 5. Amendment and Correction Requests

The City did not demonstrate a clearly documented amendment and correction request procedure during the audit period.

The materials reviewed showed GRAMA-related procedures for access to records, review, denial, extension, and appeal, but did not establish a separate procedure for amendment or correction of personal data. The City's website privacy notice referenced access and correction rights, but did not explain how an individual may submit such a request. A draft policy included amendment and correction language, but it was not approved and was not relied upon as an operative process. Interview responses described a manual process for handling correction-related requests, but the City did not provide documentation showing that the process was formalized, consistently communicated, or tracked.

Pursuant to Utah Code §63A-19-403 of the GDPA, a governmental entity that collects personal data must provide a procedure by which an individual, or the individual's legal guardian, may request amendment or correction of personal data furnished to the governmental entity. The procedure must comply with applicable law, and the statute does not require the governmental entity to make the requested amendment or correction.

This condition occurred because the City appears to have relied on existing records-access and GRAMA-related processes rather than developing and formalizing the distinct amendment and correction

procedure required by Utah Code §63A-19-403. In addition, the City's broader privacy governance framework was still developing, and draft policies had not yet been implemented or approved during the audit period.

Without a clearly documented and communicated amendment and correction procedure, individuals may not know how to request amendment or correction of personal data furnished to the City, and City personnel may handle such requests inconsistently.

Recommendation

We recommend that the City formally document and implement an amendment and correction request procedure. The procedure should identify how individuals may submit requests, who is responsible for review and response, what standards or laws apply, how decisions are documented, how requests are tracked, and how request outcomes are communicated.

The City should also communicate the procedure through appropriate privacy notices or other public-facing materials and clarify that submitting a request does not require the City to make the requested amendment or correction.

Ogden City's Corrective Action Plan

The City will formally approve and implement an amendment and correction request procedure by November 30, 2026. The procedure will explain how individuals or their legal guardians may submit requests by mail, email, or online; identify the City roles responsible for reviewing requests and responding in consultation with the department maintaining the information; and describe the applicable legal standards, including the relationship to GRAMA. The City will document and track each request, keep a record of the decision, and notify the requester in writing of the outcome and reasons.

By December 31, 2026, the City will publish the procedure through a public webpage, request form, and applicable privacy notices. Those materials will clarify that submitting a request does not require the City to make the requested amendment or correction.

Finding 6. Incomplete Privacy Report

The City provided the Town Data Privacy Assessment Report 2025 as its annual privacy program report. However, the report did not fully address all elements required by Utah Code §63A-19-401.3, and the City did not demonstrate that the report was prepared by the statutory deadline by or under the authority of the appropriate official.

Pursuant to Utah Code §63A-19-401.3, the chief administrative officer of each governmental entity is required to prepare an annual privacy program report by December 31 of each year. The report must address whether the entity has initiated a privacy program; implemented privacy practices; strategies for improving the privacy program; high-risk processing activities; the types of personal data shared,

sold, or purchased; the legal basis for that activity; the categories of recipients or sources; the percentage of employees who fulfilled training requirements; and a description of identified non-compliant processing activities and the strategy for bringing those activities into compliance.

The report identified that the City had initiated a privacy program and described certain implemented privacy practices, including website notices for collected data, notices for new public services, use of privacy impact assessments on initiatives, designation of the IT Director as Chief Administrative Officer for Data Privacy, and privacy training for employees with access to personal data. However, the report did not clearly identify the types of personal data shared with contracted vendors or the legal basis for that sharing.

The report's discussion of high-risk processing activities was also incomplete because the City was awaiting a website scan and other systems remained under review. In addition, the report did not identify specific preexisting non-compliant processing activities, potential privacy-notice gaps involving preexisting processing activities, or corresponding activity-specific strategies for bringing those activities into compliance. Instead, it stated generally that the City intended to continue evaluating existing or older systems and make changes as necessary.

This condition occurred because the City's privacy program and system review were still developing during the audit period, and the reporting process was not yet supported by complete underlying information regarding systems, data-sharing activities, legal basis, high-risk processing activities, and non-compliant processing activities.

An incomplete privacy program report limits management's and oversight bodies' ability to understand the City's privacy environment, identify non-compliant processing activities, evaluate data-sharing and high-risk processing activities, and track progress toward compliance. Without documentation of the report's completion and authorization, the City is also unable to demonstrate that the report was prepared by the statutory deadline and appropriate official.

Recommendation

We recommend that the City revise its annual privacy program report process so the report fully addresses each required element of Utah Code §63A-19-401.3. The report should identify the types of personal data shared, sold, or purchased; the legal basis for those activities; the applicable categories of recipients or sources; high-risk processing activities; and specific identified non-compliant processing activities with corresponding strategies for bringing those activities into compliance. This process should include identifying applicable compliance gaps involving preexisting processing activities and the corresponding strategies for bringing those activities into compliance.

We also recommend that the City document the report's completion date and that it was prepared by or under the authority of the chief administrative officer.

Ogden City's Corrective Action Plan

The City will revise its annual privacy reporting process so the report addresses each required element of the Utah Code §63A-19-401.3. By November 30, 2026, the City will establish a reporting checklist and a process for collecting information from departments. Departments will provide their information by December 15, and the City will complete and submit the 2026 report by December 31, 2026.

The report will identify personal data shared, sold, or purchased; the legal bases and applicable categories of recipients or sources; high-risk processing activities; and identified non-compliant processing activities, including compliance gaps involving preexisting activities and strategies to bring them into compliance. It will also address the other required reporting elements, including privacy program status and practices, improvement strategies, and employee training completion. The report will state its completion date and that it was prepared by or under the authority of the CAO. The City will retain the report and supporting workpapers for at least five years.

Appendix A – Summary of Findings

Finding #	Issues Identified	Statute	OSA's Recommendation	Ogden City's Corrective Action Plan	OSA Assessment
1	Incident and Breach Methodology	Utah Code §63A-19-405, 406	Update, approve, and maintain incident and breach methodology that reflects current roles, escalation paths, breach-evaluation procedures, notification requirements, contact information, evidence-retention expectations, and response steps for both cyber and non-cyber privacy incidents. Communicate the methodology to appropriate personnel and periodically review or test it.	The City is updating its incident and breach response procedures to address current roles, escalation, breach evaluation, required notifications, documentation, evidence retention, and cyber and non-cyber privacy incidents. Updated procedures will be approved by December 15, 2026, communicated by December 31, 2026, and related training will be completed and documented by February 28, 2027.	Ogden City concurred with our findings and outlined corrective action plans that are underway. Because the final components of the City's corrective action plan are scheduled for completion by June 30, 2027, the Office of the State Auditor will conduct a follow-up review after implementation to evaluate whether the corrective actions adequately address the recommendations.
2	Retention and Disposition	Utah Code §63A-19-404	Document the applicable retention schedule and disposition method for personal-data holdings, including retained copies outside official systems, and periodically review selected systems, forms, and workflows to confirm that personal data remains linked to approved retention schedules and disposition methods.	The City has begun an inventory of personal-data holdings and will document the responsible department, applicable retention schedule, and disposition method, including copies maintained outside official systems. Department inventories are expected by January 31, 2027; high-risk and high-volume holdings by March 31, 2027; and remaining holdings and an initial compliance review by June 30, 2027.	Refer to Finding #1.

				The city will also periodically review selected systems, forms, and workflows.	
3	No Finalized Privacy Policy	Utah Code §63A-19-401(2)(a), 102	Finalize, approve, and implement a citywide privacy policy framework that establishes privacy roles and responsibilities and expectations for processing, collection, retention, access, vendor handling, incident escalation, and other privacy requirements.	The City will finalize, approve, implement, and communicate a citywide privacy policy by November 30, 2026. The policy will establish privacy roles and responsibilities and expectations for data processing, collection notices, retention, access controls, vendor handling, incident escalation, and prohibited uses. The City will also designate a Privacy Officer with executive oversight by the CAO.	Refer to Finding #1.
4	Privacy Training Program	Utah Code §63A-19-401.2	Align the City's privacy training process with Utah Code §63A-19-401.2 by ensuring that covered employees complete privacy training within 30 days after beginning employment and at least once each calendar year.	The City will require covered employees and supervisors to complete privacy training within 30 days after beginning employment or covered duties and at least once each calendar year. The City will assign 2026 training by November 15, 2026, with completion due by December 31, 2026, and will monitor completion, retain training records, and report completion percentages in the annual privacy report.	Refer to Finding #1.
5	Amendment and	Utah Code §63A-19-403	Formally document and implement an amendment and correction procedure identifying how requests are submitted, reviewed, tracked, documented, and	The City will approve and implement an amendment and correction request procedure by November 30,	Refer to Finding #1.

	Correction Requests		communicated. Make the procedure available through appropriate privacy notices or other public-facing materials.	2026. The procedure will establish submission methods, responsible roles, applicable legal standards, tracking, documentation, and written notification of outcomes. By December 31, 2026, the City will publish the procedure through a public webpage, request form, and applicable privacy notices.	
6	Incomplete Privacy Report	Utah Code §63A-19-401.3	Revise the annual privacy program report process to address all statutory elements, including data-sharing activities and legal bases, high-risk processing, identified non-compliant activities, and corresponding compliance strategies. Document the report's completion date and that it was prepared by or under the authority of the chief administrative officer.	The City will establish a reporting checklist and departmental information-collection process by November 30, 2026, with departmental submissions due by December 15, 2026, and completion of the 2026 privacy report by December 31, 2026. The report will address all required statutory elements, document its completion date and CAO authority, and be retained with supporting workpapers for at least five years.	Refer to Finding #1.