# Preliminary FOLLOW-UP REPORT

# An Audit of Salt Lake County Criminal Justice Services: Data Access and Protections

JUNE 2026


**Chris Harding, CPA, CFE, CIA**
**County Auditor**

Office of the Auditor
Salt Lake County

## Audit Team

Brenda Nelson, CISA, Audit Manager
Tammy Brakey, CFE, Senior Internal Auditor
Anthony Kournianos, CFE, Internal Auditor
Kent Dunn, Internal Auditor
Paige Hernandez, MBA, Internal Auditor

## Audit Management

Chris Harding, CPA, CFE, CIA, County Auditor
Richard Jaussi, MBA, Chief Deputy Auditor
Roswell Rogers, Senior Advisor
Shawna Ahlborn, Audit Division Director

## Audit Committee

Marty Van Wagoner, CPA, MBA

SALT LAKE COUNTY

Office of the Auditor
Salt Lake County
2001 S State Street, Ste N3-300
Salt Lake City, UT 84190-1100
Phone: (385) 468-7200

www.saltlakecounty.gov/auditor/

# Salt Lake County Auditor

Chris Harding, CPA, CFE, CIA
County Auditor

2001 S State Street, Ste N3-300, Salt Lake City, UT 84190
Phone: (385) 468-7200 www.saltlakecounty.gov/auditor/

## AUDITOR'S LETTER

June 8, 2026

In accordance with Generally Accepted Government Auditing Standards and the established policies of the Auditor's Office, as authorized by Utah Code Title 17, Chapter 19a, "County Auditor," Part 2, "Powers and Duties," we maintain our responsibility to monitor and ensure that audit recommendations are addressed by county agencies through appropriate corrective action. This process is also instrumental in shaping future audits.

This is the preliminary follow-up report for *An Audit of Salt Lake County Criminal Justice Services: Data Access and Protections* originally issued in April 2025. The initial audit identified seven findings with 12 recommendations. The purpose of this follow-up review was to assess the status of corrective actions intended to strengthen compliance and safeguards over confidential data and systems.

Our follow-up work found that agency management implemented 11 of the 12 recommendations. Through updates to agency procedures, monitoring drug test result entries, strengthening system access based on business requirements, and improving documentation related to e-waste disposal, management has taken corrective actions to address risks identified in the original audit. These efforts have strengthened controls over confidential data and systems.

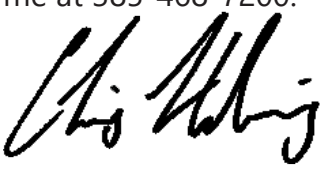
Additionally, one recommendation was closed because Criminal Justice Services employees relocated from office space shared with another agency, making the recommendation no longer applicable.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe the evidence obtained meets these requirements.

The follow-up period for this audit covered October 15, 2025, through April 15, 2026. For testing related to the revocation of terminated employee access, the scope was extended through May 31, 2026. Our review focused on verifying the implementation status of recommendations from the April 2025 audit report through document review, analysis, and discussions with Criminal Justice Services management.

We extend our appreciation to the leaders and staff of Criminal Justice Services for their cooperation. The enclosed report summarizes the status of the recommendations reviewed in this preliminary follow-up.

Should you have any questions or wish to discuss the report further, please do not hesitate to contact me at 385-468-7200.



Chris Harding, CPA, CFE, CIA
Salt Lake County Auditor

June 2026

# Actions Taken Since Audit Report

An Audit of of Criminal Justice Services: Data Access and Protections

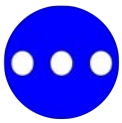
**Original Audit: Report Issued April 2025**

The original audit identified seven findings with 12 recommendations for improvement.

**Preliminary Follow-up:**

Our preliminary follow-up found that Criminal Justice Services fully implemented 11 of the 12 recommendations, two recommendations were in progress, and one recommendation was closed.

**FULLY IMPLEMENTED** **11**



**IMPLEMENTATION IN PROGRESS** **0**

**CLOSED** **1**

# Scope:

The scope of this preliminary follow-up audit covered the period from October 15, 2025, through April 15, 2026. For testing related to the revocation of terminated employee access, the scope was extended through May 31, 2026.

# Remaining Risks

Because all applicable recommendations were implemented and the remaining recommendation was closed due to changes in operations, no significant residual risk related to the original findings was identified. Accordingly, no additional follow-up work is planned by the Auditor's Office.

# FINDING 1: OPPORTUNITY TO STRENGTHEN NETWORK ACCESS TERMINATION PROCESSES

Risk Rating: Significant Risk Finding

**Recommendation 1.1** - We recommend that Criminal Justice Services Management enhance internal policies and procedures regarding employee terminations that include revoking employee network access. Management should consider including the following:

- Designating who is responsible (including a backup individual) for requesting that network access be revoked.
- Setting clear guidelines for the timing of access removal requests.
- Defining documentation to be retained and establishing a retention period for records.

Agency Action – Implemented our recommendation

**Recommendation 1.2** - We recommend that Criminal Justice Services Management consider developing and implementing a termination checklist that includes revoking user access to County systems, networks, and all applications.

Agency Action – Implemented our recommendation

# FINDING 2: OPPORTUNITIES TO STRENGTHEN TIMELINESS AND CONSISTENCY OF APPLICATION ACCESS REMOVAL

Risk Rating: Significant Risk Finding

**Recommendation 2.1** -We recommend that Criminal Justice Services Management enhance internal policies and procedures for revoking access to applications whenever an employee terminates. Management should consider including the following:

- Designating who is responsible (and back up individual) for terminating access or for contacting application administrator(s) whenever an employee terminates.
- Setting clear guidelines for the timing of access removal requests.
- Defining documentation to be retained and establishing a retention period for records.

Agency Action – Implemented our recommendation

**Recommendation 2.2** - We recommend that Criminal Justice Services Management consider developing and implementing a termination checklist that includes revoking user access to County systems, networks, and all applications.

Agency Action –Implemented our recommendation

# FINDING 3: OPPORTUNITIES TO IMPROVE DATA ENTRY CONSISTENCY IN ESUPERVISION

Risk Rating: Significant Risk Finding

**Recommendation 3.1** -We recommend that Criminal Justice Services Management update Criminal Justice Services 03-100: Case Note Policy to clarify requirements for entering in drug test scheduling and results within eSupervision, including any unique requirements for each Criminal Justice Services Program.

Agency Action –Implemented our recommendation

**Recommendation 3.2** -We recommend that Criminal Justice Services management implement periodic, documented monitoring and follow up of eSupervision entries to ensure compliance with Criminal Justice Services 03-100: Case Note Policy.

Agency Action –Implemented our recommendation

# FINDING 4: OPPORTUNITIES TO IMPROVE CONTROLS FOR THE DISPOSAL OF SURPLUS ASSETS CONTAINING HARD DRIVES

Risk Rating: Moderate Risk Finding

**Recommendation 4.1** -We recommend that Criminal Justice Services Management establish and implement internal policies and procedures to ensure proper disposal of surplus assets and secure destruction of hard drives. These policies and procedures should include:

- Completion of the Form PM-2, with the "E-Waste Disposal" box marked where applicable.
- Retention documentation indicating the vendor's name, such as a receipt from vendor, or indication on the Form PM-2, to indicate items were received by the disposal vendor.
- Requirements that the employee transferring assets to the vendor, and the vendor receiving the assets, each verify that all assets transferred are accurately listed on the form, and that no assets are listed that were not transferred.

Agency Action –Implemented our recommendation

# FINDING 5: OPPORTUNITIES TO ENHANCE NETWORK ACCESS CONTROLS TO SAFEGUARD DATA INTEGRITY IN A DYNAMIC WORK ENVIRONMENT

Risk Rating: Moderate Risk Finding

**Recommendation 5.1** - We recommend that Criminal Justice Services Management implement a process to regularly review and update security group members whenever employee roles change to ensure access is limited to that required for users to perform their job duties.

Agency Action –Implemented our recommendation

**Recommendation 5.2** - We recommend that Criminal Justice Services Management perform ongoing monitoring and management of active directory content and permissions to ensure user accounts and security groups remain up-to-date and access is limited to that required for users to perform their job duties. We also recommend that periodic, documented reviews be conducted.

Agency Action –Implemented our recommendation

# FINDING 6: OPPORTUNITY TO ENHANCE UWITS USER PERMISSIONS TO ALIGN WITH BUSINESS NEEDS

Risk Rating: Moderate Risk Finding

**Recommendation 6.1** -We recommend that Criminal Justice Services Management limit all user permissions within the system UWITS to "Read-Only" access for all non-admin level Criminal Justice Services employees and ensure that no Criminal Justice Services UWITS user is granted permissions beyond their designation level or need for access.

Agency Action –Implemented our recommendation

**Recommendation 6.2** -We recommend that Criminal Justice Services Management monitor and modify user application access whenever needs change.

Agency Action –Implemented our recommendation

# FINDING 7: OPPORTUNITY TO ENHANCE WORKSTATION PRIVACY TO SAFEGUARD SENSITIVE INFORMATION

Risk Rating: Moderate Risk Finding

**Recommendation 7.1** -We recommend that Criminal Justice Services Management ensure that all computer screens, both in office and remote locations, are in areas not viewable to unauthorized people, including other County Employees as per their internal policy.

Additionally, the policy could be updated to allow for exceptions in specific, justified circumstances, provided formal approval is obtained from the appropriate authority, such as BCI. This approach maintains security standards while allowing for necessary flexibility in their internal policy

Agency Action –This recommendation is considered CLOSED.

The Mayor's Finance Administration (MFA) space previously occupied by Criminal Justice Services has been vacated. We confirmed that access to the remaining Criminal Justice Services office locations was restricted to Criminal Justice Services employees. Therefore, the risk the recommendation was intended to address was no longer relevant. As a result, additional follow-up work is not planned and the recommendation was closed.

APPENDIX A: AUDIT RECOMMENDATION IMPLEMENTATION STATUS

| Audit Recommendation Implementation Status | | | |
|---|---|---|---|
|  Fully Implemented |  Implementation In Progress |  Not Implemented |  Closed |
| The audit recommendation has been implemented, and the corrective actions effectively address the original issue or finding, as verified by the follow-up audit. No further action is required at this time. | The agency has begun taking corrective actions to address the audit recommendation. However, full implementation has not yet been achieved. | The agency has not taken corrective action to address the audit recommendation. | Circumstances have changed surrounding the original finding or recommendation that make it no longer applicable, or the agency will only implement a portion of the recommendation as verified by the follow-up audit. No further follow-up is required. |