AUDIT REPORT

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

APRIL 2025

Chris Harding, CPA, CFE, CIA
County Auditor

Office of the Auditor
Salt Lake County

Audit Team

Brenda Nelson, CISA, Audit Manager
Tammy Brakey, Senior Internal Auditor
Anthony Kournianos, Internal Auditor
Matthew Cullinen, 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

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

April 23, 2025

I am pleased to present the results of our audit of Criminal Justice Services data access and controls for the period of January 1, 2023, to December 31, 2023. The objective of this audit was to provide reasonable assurance that the internal controls were adequate and effective, and that data access and protections complied with applicable ordinances, policies, and procedures.

Our audit identified areas where improvements could strengthen Criminal Justice Services operations, specifically, regarding the process for terminating network and application access when employees leave the agency. In several cases, access revocation requests were either not submitted or were delayed for extended periods, increasing the risk of unauthorized access.

We also noted opportunities to improve data availability and consistency. In particular, urinalysis testing results for clients were often missing from the case management system or were entered without sufficient detail, frequently only date ranges or general descriptions were entered, rather than specific results.

We urge Criminal Justice Services to promptly review and implement the detailed recommendations outlined in the attached audit report. Acting on these items will help further safeguard client data and strengthen the overall integrity and effectiveness of their systems.

Criminal Justice Services management agreed with 10 of the 12 audit recommendations. For the remaining two, while management expressed disagreement with the assigned risk ratings, they acknowledged the underlying issues and outlined plans to address them through policy and process changes. The assignment of risk ratings is a professional judgment made by the Auditor in accordance with applicable audit standards. Our responses to these specific disagreements are provided in the attached addendum.

This audit was authorized under Utah Code Title 17, Chapter 19a, "County Auditor", Part 2, "Powers and Duties." We conducted this performance audit in accordance with generally accepted government auditing standards. 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 our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

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/

We appreciate the cooperation and assistance provided by Criminal Justice Services during this audit. For further information or clarification regarding this report, please feel free to contact me at 385-468-7200.

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

Contents

REPORT HIGHLIGHTS

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

April 2025

Objectives

The audit objectives were to provide reasonable assurance that the internal controls in place are adequate and effective and data access and protections comply with applicable ordinances, policies, and procedures. Areas of audit focus included the processes and procedures for the following:

- Network and database accessibility
- Login, account, and user activity
- Data protection, privacy, and management
- Safeguarding county assets against the risk of loss, theft, waste, or abuse

The scope of the audit was from January 1, 2023, to December 31, 2023, and included dates in 2024 as necessary based on testing requirements.

Opportunity to Strengthen Network Access Termination Processes

When an individual leaves Salt Lake County employment, the agency is responsible for submitting an Information Technology Division (IT) service request to have the employee's network access revoked. We found that Criminal Justice Services did not submit a termination request to have access to County systems and networks revoked for three out of 21 (14%) employees who ended their employment in 2023.

Opportunities to Strengthen Timeliness and Consistency of Application Access Removal

Criminal Justice Services used several applications containing confidential information on clients. For the 21 employees that terminated in 2023, we tested whether Criminal Justice Services requested that the employees' access to these applications be revoked in a timely manner. We found that for the Offender Management System (OMS), Criminal Justice Services did not request that the Sheriff's Office revoke access for any of the agency's employees. For the application Uptrust, requests were not timely for 16 out of the 21 (76%) employees. Requests were made between 15 and 368 days after the employees' last day. Finally, for the Utah Web Infrastructure for Treatment Services (UWITs) application, only one of the 21 employees required access to UWITs. We found that Criminal Justice Services did not request that BHS revoke access for that employee when they terminated.

Opportunities to Improve Data Entry Consistency in eSupervision

Criminal Justice Services uses a urinalysis testing company to conduct client drug testing. The testing company hosts web-based software that allows Criminal Justice Services to track and manage client drug test scheduling and results. Data from the online system is manually entered by Criminal Justice Services staff into the Agency's client case management system. A review of client testing dates revealed that 21 of 45 (47%) scheduled tests dates were not recorded in the case management system. Additionally, 18 of the 45 (40%) scheduled tests that were entered lacked specific details, instead containing date ranges and general descriptions.

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

Finding Risk Classifications

Classification	Description
1 – Low Risk Finding	Low risk findings may have an effect on providing reasonable assurance that internal controls in place are adequate and effective, and data access and protections comply with applicable ordinances, policies, and procedures. Recommendations may or may not be given to address the issues identified in the final audit report. If recommendations are given, management should try to implement the recommendations within one year of the final audit report date if possible. Follow-up audits may or may not focus on the status of implentation.
2 – Moderate Risk Finding	Moderate risk findings may have an effect on whether there is reasonable assurance that internal controls in place are adequate and effective, and data access and protections comply with applicable ordinances, policies, and procedures. Recommendations will be given to address the issues identified in the final audit report. Management should implement the recommendations within one year of the final audit report date if possible. Follow-up audits will focus on the status of implementation.
3 – Significant Risk Finding	Significant risks are the result of one or more findings that may have an effect on whether there is reasonable assurance that internal controls in place are adequate and effective, and data access and protections comply with applicable ordinances, policies, and procedures. Recommendations will include necessary corrective actions that address the significant risks identified in the final audit report. Management should implement the recommendations within six months of the final audit report date if possible. Follow-up audits will focus on the status of implementation.
4 – Critical Risk Finding	Critical risks are the result of one or more findings that would have an effect on whether there is reasonable assurance that internal controls in place are adequate and effective, and data access and protections comply with applicable ordinances, policies, and procedures. Recommendations will include necessary corrective actions that address the critical risks identified in the final audit report. Management should implement the recommendations as soon as possible. Follow-up audits will focus on the status of implementation.

BACKGROUND

The Salt Lake County Auditor's Audit Services Division completed a limited-scope audit of Salt Lake County Criminal Justice Services data access and protections for the period of January 1, 2023, to December 31, 2023.

Criminal Justice Services is a division of the Salt Lake County Department of Human Services that provides client focused services to promote accountability, address risks to the community, and achieve behavior change. Criminal Justice Services consists of four programs: Pretrial Services, Reports and Assessment Services, Probation, and Specialty Courts.

OBJECTIVES AND SCOPE

The audit objectives were to provide reasonable assurance that the internal controls in place are adequate and effective and data access and protections comply with applicable ordinances, policies, and procedures. Areas of audit focus included the processes and procedures for the following:

- Network and database accessibility
- Login, account, and user activity
- Data protection, privacy, and management
- Safeguarding county assets against the risk of loss, theft, waste, or abuse

The scope of the audit was from January 1, 2023, to December 31, 2023, and included dates in 2024 as necessary based on testing requirements.

AUDIT CRITERIA

Salt Lake County Countywide Policy 1400-1: Information Technology Security: Acceptable Use Policy provides policy and guidelines to ensure that information technology (IT) resources and systems owned by Salt Lake County are used efficiently and appropriately; that Salt Lake County employees and other are aware of the acceptable use of IT resources and systems; that Salt Lake County will monitor the use of IT resources and systems; and, that Salt Lake County will monitor and enforce compliance with this policy.

Salt Lake County Countywide Policy 1125: Safeguarding Property/ Assets establishes responsibility for managing property, defines the types of assets subject to various controls, and provides procedures for disposal of property.

Salt Lake County Criminal Justice Services Policy 06-100: Computer and Information Systems provides a guide for Criminal Justice Services employees to effectively use division/county computers and information systems.

Salt Lake County Criminal Justice Services Policy 06-200: Utah Criminal Justice Information Systems establishes policy to ensure compliance with National Crime Information Center (NCIC) and Utah Bureau of Criminal Identification (BCI) regulations and provides the necessary procedures for using those database systems. The policy also provides guidelines for screening new hire candidates and conducting annual employee background checks.

Salt Lake County Criminal Justice Services Policy 03-100: Case Notes establishes a division-wide standard for Case Notes including rules for defining, recording, and maintaining electronic case files.

Salt Lake County Criminal Justice Services Policy on 01-07 on Controlled Asset Management establishes the process which Criminal Justice Services assets will be tagged, tracked, and disposed of.

METHODOLOGY

We used several methodologies to gather and analyze information related to our audit objectives. The methodologies included but were not limited to:

1. **Collaborative Interviews:** Auditors met with agency personnel to gain an understanding of systems and applications as well as controls in place to protect confidentiality, integrity, and availability of data.
2. **Direct Observation:** Controls were observed in operation, such as physical access controls over Criminal Justice Services offices and computers.
3. **Sampling:** Where appropriate statistical or judgmental sampling was used to identify items for review.
4. **Documentation Review:** Documentation was reviewed regarding asset disposal and user permissions.

CONCLUSIONS

During the audit we identified opportunities to improve compliance with Countywide and Criminal Justice Services policies and reduce the risk of unauthorized access, data corruption, and data loss. Specifically, we observed delays in revoking access for former employees and cases where access permissions exceeded the requirements for certain job responsibilities. We recommend strengthening controls to address the

following findings:

- Opportunity to Strengthen Network Access Termination Processes
- Opportunities to Strengthen Timeliness and Consistency of Application Access Removal
- Opportunities to Improve Controls for the Disposal of Surplus Assets Containing Hard Drives
- Opportunities to Improve Data Entry Consistency in eSupervision
- Opportunities to Enhance Network Access Controls to Safeguard Data Integrity in a Dynamic Work Environment
- Opportunity to Enhance UWITS User Permissions to Align with Business Needs
- Opportunity to Enhance Workstation Privacy to Safeguard Sensitive Information

These findings underscore the importance of enhancing governance and maintaining strict adherence to access control protocols. Ensuring that access for terminated employees is promptly revoked is important to protect County applications and sensitive information from potential unauthorized access. Additionally, maintaining thorough records for asset and hard drive disposal helps minimizing risks to data confidentiality and helps safeguards assets.

To address these concerns and foster operational improvements, we recommend that Criminal Justice Services Management establish and implement clear procedures to ensure timely revocation of access for terminated employees. We further encourage adherence to both Countywide and Criminal Justice Services policies to strengthen overall security and accountability.

FINDING 1 AND RECOMMENDATIONS

Opportunity to Strengthen Network Access Termination Processes

Risk Rating: Significant Risk Finding

Salt Lake County agencies are required to submit an Information Technology Division (IT) service request to revoke employee network access upon termination. In 2023, 21 employees from Criminal Justice Services terminated, transferred, or retired. For all 21 employees, we reviewed whether Criminal Justice Services requested the employee's network access be revoked on a timely basis. We found that:

- **Timely Requests:** For 16 of the 21 employees (76%), Criminal Justice Services submitted timely access removal requests within five business days of the employee's termination date.
- **Missed Requests:** For three of the 21 employees (14%), Criminal Justice Services did not submit an access removal request. During our testing we noted that the accounts had since been deactivated by IT.
- **Transferred Employees:** Two of the 21 employees (10%) transferred to another County division. Per County policy, the employee's new agency submitted an IT service request to have the employees' access to Criminal Justice Services' network revoked and new access established.

Criminal Justice Services did not submit an access removal request for 14% of employee terminations in 2023.

Salt Lake County Countywide Policy 1400-1: Information Technology Security: Acceptable Use Policy, Part 3 Policy Statement, Section 3.1.2, states, "Salt Lake County reserves and exercises all rights relating to all information assets. County agency management is responsible for granting users' access to County IT resources and systems, which is limited to that which is required to do their work, and for revoking user access in a timely manner. County agency management may withdraw permission for any or all use of its IT resources and systems at any time."

Criminal Justice Services management explained that they did not have a standard process for revoking user access upon termination. As a result, they did not submit the termination request for three employees.

County IT explained that they run a weekly report to identify employees offboarded according to the County's payroll software. This report provided them with information to capture terminations for which the agencies have not submitted an access termination request. Through this IT process, IT revoked network access for the three individuals noted above.

However, the employees may have retained access for at least one week following their termination. In addition, our recent payroll audits revealed that some agencies do not always terminate employees through the payroll software on a timely basis. When the agency does not complete the termination process in payroll or submit an IT request, there is a risk that the network account could remain active for an extended period.

Promptly revoking user access to the County network at termination helps protect sensitive Criminal Justice Information Services (CJIS) data, County networks, and systems. Timely action reduces the risk of unauthorized access, safeguarding against potential issues such as data misuse, operational disruptions, malware or malicious activities. Ensuring immediate deactivation also minimizes the chance of accounts being used improperly by individuals other than the former employee.

1.1	RECOMMENDATION	Establish Internal Policies and Procedures

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 RESPONSE: AGREE

IMPLEMENTATION DATE: COMPLETED ON 2/12/2025

SEE PAGE 25 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

1.2	RECOMMENDATION	Implement a Termination Checklist

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 RESPONSE: AGREE

IMPLEMENTATION DATE: COMPLETED ON 2/12/2025

SEE PAGE 26 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

FINDING 2 AND RECOMMENDATIONS

Opportunities to Strengthen Timeliness and Consistency of Application Access Removal

Risk Rating: Significant Risk Finding

Criminal Justice Services staff used a combination of applications containing sensitive and confidential client information to obtain and track information necessary to administer pretrial, probation, Specialty Court, and report and assessment services. Applications used can be seen in Table 1 on page 8. [1]

Table 1: Criminal Justice Services relied on five applications to obtain and track information necessary to serve clients.[1] *Applications included case management software, client drug testing information, client information related to jail bookings and releases, and treatment records.*

Application	Description Use by Criminal Justice Services	User Access Administration
eSupervision	Web-based case management system used by Criminal Justice Services for entering and retrieving client information as well as services provided by Criminal Justice Services.	Criminal Justice Services Staff
Averhealth	Web-based software used to manage client drug test scheduling and obtain client testing results.	Criminal Justice Services Staff
Uptrust	An application used by case managers to securely communicate and send reminders to clients about court hearings and appointments.	Vendor Support Team
Offender Management System (OMS)	Software used to obtain client information related to jail inmate bookings and releases, as well as other client information. OMS was administered by the Salt Lake County Sheriff's Office.	Salt Lake County Sheriff's Office
Utah Web Infrastructure for Treatment Services (UWITS)	Software used by Criminal Justice Services to obtain client treatment information. UWITS was administered by the State of Utah. Salt Lake County Behavioral Health Services (BHS) managed access by Salt Lake County employees, including Criminal Justice Services.	Salt Lake County Behavioral Health Services

1 Does not include the Utah Criminal Justice Information System (UCJIS), which is a centralized platform managed by the Utah Bureau of Criminal Identification. BCI compliance audits are conducted by the State of Utah, Department of Public Safety, Field Services Section and were out of scope for this audit.

During the audit period, 21 Criminal Justice Services employees terminated, transferred to a different Salt Lake County agency, or retired. We verified that Criminal Justice Services revoked user access to eSupervision and Averhealth for all 21 former employees.

For applications administered by third parties, we tested whether Criminal Justice Services requested that the terminated employees' access be revoked in a timely manner. We found that:

Access removal requests for other applications were not always submitted promptly, and in some cases, were not made at all. Observed delays ranged from 15 to 368 days.

- **Uptrust Access:**
  - **Timely Access Revocation:** Criminal Justice Services submitted access removal requests within one week of the employee's termination for five out of the 21 (24%) former employees.
  - **Untimely Access Revocation:** Criminal Justice Services submitted untimely access removal requests for 16 out of 21 (76%) former employees. Requests were made between 15 and 368 days after the employees' last day.
- **OMS Access:**
  - **Access Management by Criminal Justice Services:** Criminal Justice Services stated that they did not request that the Sheriff's Office revoke access to OMS for terminated employees.
  - **Access Review by the Sheriff's Office:** However, the Sheriff's Office conducted a user access review in late 2023 and independently revoked access for any terminated Criminal Justice Services employees.
- **UWITs Access:**
  - **Access Not Required:** Twenty of the 21 employees did not require access to UWITs to perform their job duties.
  - **Access Revocation for Terminated Employee:** For the one employee who had access, Criminal Justice Services did not request for BHS to revoke access when the employee terminated. However, the user's access was automatically locked due to inactivity 40 days after their termination.
  - **Additional Observation:** During testing, we noted that one of the seven employees with access had previously terminated. This termination occurred outside of the selected sample and audit period.

Management explained that they do not have a routine process or checklist for revoking user access. Additionally, management mistakenly believed that County IT notified the Sheriff's Office and BHS about terminated individuals. Therefore, Criminal Justice Services did not consistently

provide notifications.

Promptly revoking user access to systems containing client information helps ensure that sensitive and confidential data remains secure. Timely access removal prevents unauthorized individuals, including former employees or others using their credentials, from viewing, editing, or deleting sensitive information. This proactive approach protects data confidentiality, integrity, and availability.

2.1	RECOMMENDATION	Establish Internal Policies and Procedures

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 RESPONSE: AGREE

IMPLEMENTATION DATE: COMPLETED ON 2/12/2025

SEE PAGE 26 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

2.2	RECOMMENDATION	Implement a Termination Checklist

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 RESPONSE: AGREE

IMPLEMENTATION DATE: COMPLETED ON 2/12/2025

SEE PAGE 27 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

FINDING 3 AND RECOMMENDATIONS

Opportunities to Improve Data Entry Consistency in eSupervision

Risk Rating: Significant Risk Finding

The eSupervision data entry for drug testing at Criminal Justice Services shows some inconsistencies and gaps, which could impact the efficiency of case management.

Criminal Justice Services used a urinalysis testing provider called Averhealth for client drug testing. Averhealth hosted a web-based software called Aversys, which Criminal Justice Services used to track and manage client test scheduling and results. Aversys data was manually entered by Criminal Justice Services staff into the agency's client case management system, eSupervision. Staff used one of three methods to record the information, 1) as a case note, 2) under compliance within the agreement, or 3) within the drug test portion of the system.

We reviewed a sample of 45 out of 24,247 client testing dates in Aversys to ensure accurate and complete entry of client results in eSupervision. Six of the 45 (13%) sampled client tests dates were entered into eSupervision accurately and completely. For the remaining sampled client test dates, we found that:

- For 21of the 45 (47%) scheduled test dates, staff did not record data in eSupervision using any of the allowed methods.
- For 18 of the 45 (40%) scheduled test dates, staff entered date ranges and general descriptions instead of specific test dates.

Salt Lake County Criminal Justice Services Policy 03-100: Case Note Policy, Part eSupervision Expectations, Section 5. Compliance Actions/ Note (Probation and Pretrial Programs only), states, "*To be used to document urinalysis a. Update all Compliance Actions as they occur or at least monthly. b. Examples include urinalysis results, community service progress, IID compliance, classes and treatment progress, etc. c. Urinalysis results must be documented in this field as defined: i. Positive/missed/dilute urinalysis results must be logged as noncompliant within 24 to 48 business hours of notification. ii. Negative urinalysis results should be logged monthly. iii. Before the end of every month, case managers must print an Averhealth log of all tests submitted and the related results, then upload the printout in the filing cabinet."

Criminal Justice Services Management stated that each program that requires urinalysis testing may have different methods to enter the information in eSupervision. Additionally, despite the written policy stating that Probation and Pretrial Services must record results in eSupervision, management stated those programs, as well as Specialty Court, were encouraged to document test results within eSupervision.

They also noted that compliance for Specialty Court Clients was captured in phase agreements and that all results were available in the Aversys application.

Accurate and complete client data entry into eSupervision aids in effective case management and client oversight. Missing or inaccurate information may limit staff's ability to access a full client history, including program compliance verification, which could impact the quality of support provided.

Additionally, when policies are not consistently enforced or appear to conflict with day-to-day guidance, it can reduce the emphasis placed on written policies and potentially weaken the overall control environment.

3.1	RECOMMENDATION	Update Criminal Justice Services 03-100: Case Note Policy

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 RESPONSE: DISAGREE

IMPLEMENTATION DATE: 6/1/2025

SEE PAGE 28 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

3.2	RECOMMENDATION	Periodic Review of eSupervision Entries for Policy Compliance

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 RESPONSE: DISAGREE

IMPLEMENTATION DATE: 6/1/2025

SEE PAGE 29 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

FINDING 4 AND RECOMMENDATIONS

Opportunities to Improve Controls for the Disposal of Surplus Assets Containing Hard Drives

Risk Rating: Moderate Risk Finding

The surplus asset disposal process at Criminal Justice Services could benefit from enhanced controls, particularly around the destruction of hard drives. This would help mitigate the risk of sensitive data exposure.

When County assets such as furniture, equipment, computers, and other items become outdated, replaced, or otherwise no longer needed for operational purposes, they are designated as surplus. County Form PM-2 is used to transfer, dispose of, or sell surplus assets. According to County policy, all surplus hard drives, which may contain sensitive or confidential information, must be destroyed.

Criminal Justice Services transferred assets containing hard drives to an E-Waste disposal vendor using Form PM-2, which included a check box titled "E-Waste Disposal." The completed Form PM-2 was signed by both a representative of Criminal Justice Services and the E-Waste vendor upon transfer of the asset(s).

During the audit period, Criminal Justice Services disposed of 511 assets. We reviewed a sample of 41 assets to verify proper use of Form PM-2, specifically confirming the selection of the "E-Waste Disposal" checkbox for all assets containing hard drives. We found that Form PM-2 was on file for all 41 assets sampled. Of these, 22 assets did not require E-Waste disposal. However, for the 19 assets containing hard drives, we found the following:

- **Form PM-2 Completion:** For all 19 assets containing hard drives (including laptops and printers), the "E-Waste Disposal" checkbox was not selected on the Form PM-2.
- **Vendor Identification:** We found no evidence that the individual receiving the assets represented the E-Waste vendor. The name of the vendor was not recorded on the Form PM-2, and no receipt was provided by the vendor to confirm the asset transfer.
- **Asset Verification:** We found no evidence that either the Criminal Justice Services representative or the vendor reviewed, counted, or verified the accuracy of the assets designated listed for disposal. For example, we identified a laptop listed as disposed of on a signed Form PM-2 from 2023 that was still listed on the 2024 asset list. Additionally, the laptop was also observed by the auditors in storage at Criminal Justice Services during 2024, indicating that it had not been disposed of as documented.

Salt Lake County Criminal Justice Service Policy: 01.07 Controlled Asset Management, Part 7 Surplus, Section 7.1, states, "When an asset is scheduled for surplus the Fiscal Team will do the following:

7.1.1. Complete a PM2 Form.
7.1.2. Update the database.
7.1.3. Use a County approved vendor to dispose of all equipmentwhich includes the destruction of all hard drives."

The Criminal Justice Services Property Manager acknowledged that human error contributed to the error on Form PM-2 not being detected during a review for accuracy and proper completion by either the Criminal Justice Services employee or the vendor. There were no check marks on the form or other documentation demonstrating that each item listed was verified as being transferred to the vendor.

Prompt and accurate completion of Form PM-2s helps minimize the risk of fraud, waste, and abuse. Additionally, when the "E-Waste Disposal" checkbox is not selected, there is an increased risk that hard drives containing sensitive and confidential County and Criminal Justice Information (CJI) data may not be properly destroyed. Proper hard drive destruction is crucial for preventing data breaches, reputational damage, and legal penalties.

4.1	RECOMMENDATION	Establish Internal Policies and Procedures

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 RESPONSE: AGREE

IMPLEMENTATION DATE: COMPLETED ON 2/12/2025

SEE PAGE 30 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

FINDING 5 AND RECOMMENDATIONS

Opportunities to Enhance Network Access Controls to Safeguard Data Integrity in a Dynamic Work Environment

Risk Rating: Moderate Risk Finding

Some network folder permissions may benefit from further review to ensure they continue to align with current roles and responsibilities, given the evolving nature of team assignments and responsibilities.

Criminal Justice Services utilized network drive folders for storing various files, including client related files, administrative files, policies and procedures, and other work related documents. Criminal Justice Services controlled access by assigning network folder permissions using Active Directory security groups. Security groups were designed to be based on what section of Criminal Justice Services employees were assigned to, as well as their job duties.

The Salt Lake County Information Technology division provided a report that indicated which security groups had access to each Criminal Justice Services network folder. They also provided a report of which employees were assigned to each security group. We selected a judgmental sample of 21 file folders for review and inquired with Criminal Justice Services Information Systems Manager regarding each folder's contents and who should have access to that based on business need.

We found that for the majority of folders sampled, security groups with access, and individuals in those groups, aligned with expectations based on organizational structure or job titles and what was indicated by the Information Systems Manager.

However, for a portion of the folders sampled, security groups with access, or individuals in the security group, did not align with expectations based on organizational structure or job titles and what was indicated by the Criminal Justice Services Information Systems Manager.

Salt Lake County Countywide Policy 1400-1: Information Technology Security: Acceptable Use Policy, Section 3.12 Access and Control, states, "Salt Lake County reserves and exercises all rights relating to all information assets. County agency management is responsible for granting users' access to County IT resources and systems, which is limited to that which is required to do their work, and for revoking user access in a timely manner…"

Criminal Justice Services Management stated that the inconsistencies in folder permissions and security group assignments stemmed from individuals who transitioned between work groups within Criminal Justice Services, and that staff are often assigned to multiple different teams for training purposes and as client's needs dictate. As a result

of the need for flexibility, active directory security groups no longer reflected the current environment.

Criminal Justice Services Management additionally stated that no unauthorized data was exposed and that no individual had excessive access. As a result of our audit, Criminal Justice Services reported that they have initiated an internal process as an administrative team to review the members of all their security groups. Additionally, they are assessing the content and visibility of the information on their shared network drive.

When active directory security is not routinely monitored and adjusted to fit current business needs, there is an increased risk that the confidentiality, integrity, and availability of data may be compromised in the future. Security settings that reflect the current environment help prevent unauthorized individuals from viewing, editing, or deleting sensitive information.

5.1	RECOMMENDATION	Security Group Reviews

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 RESPONSE: AGREE

IMPLEMENTATION DATE: 6/1/2025

SEE PAGE 31 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

5.2	RECOMMENDATION	Active Directory Management and Review

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 RESPONSE: AGREE

IMPLEMENTATION DATE: 6/1/2025

SEE PAGE 32 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

FINDING 6 AND RECOMMENDATIONS

Opportunity to Enhance UWITS User Permissions to Align with Business Needs

Risk Rating:Moderate Risk Finding

Criminal Justice Services UWITS users have excessive "Full-Access" permissions, exceeding their job requirements and increasing the risk of unauthorized data modification.

As described in Finding 2, Utah Web Infrastructure for Treatment Services (UWITS) application was used by Criminal Justice Services to obtain client treatment information. UWITS was administered by the State of Utah and Salt Lake County Behavioral Health Services (BHS) managed access for Salt Lake County employees.

Criminal Justice Services Management stated that all seven employees using UWITs required view and download access. Our review found the following:

- **Limited Access Granted:** One user (14%) had access correctly restricted to the required view and download access only.
- **Full Access Granted:** Six users (86%) were given "Full-Access" permissions, which allowed them to enter and edit data, exceeding the required access level.

Salt Lake County Countywide Policy 1400-1: Information Technology Security: Acceptable Use Policy, Part 3.0 Policy Statement, Section 3.12 states, "Salt Lake County reserves and exercises all rights relating to all information assets. County agency management is responsible for granting users' access to County IT resources and systems, which is limited to that which is required to do their work, and for revoking user access in a timely manner…"

Criminal Justice Services Management stated that assigning Full Access permissions was likely required in the past when Criminal Justice Services performed additional job duties and that the permissions were never updated.

Limiting employee access to only the information and permissions necessary for their job duties enhances data security and minimizes the risk of unauthorized changes or data loss.

6.1	RECOMMENDATION	Limiting UWITS User Permissions

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 RESPONSE: AGREE

IMPLEMENTATION DATE: COMPLETED ON 2/20/2025

SEE PAGE 33 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

6.2	RECOMMENDATION	Monitoring and Updating User Application Access

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

AGENCY RESPONSE: AGREE

IMPLEMENTATION DATE: 5/1/2025

SEE PAGE 34 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

FINDING 7 AND RECOMMENDATIONS

Opportunity to Enhance Workstation Privacy to Safeguard Sensitive Information

Risk Rating:Moderate Risk Finding

To safeguard sensitive client information from being seen by unauthorized personnel, Criminal Justice Services strategically positions desktop monitors in the County's Government Center away from open public access areas. This orientation prevents non-Criminal Justice Services personnel from being able to view sensitive information from behind or in adjacent spaces.

Due to limited space within the Criminal Justice Services offices, some Criminal Justice Services staff were temporarily stationed at the Mayor's Financial Administration (MFA) section of the Government Center. Auditors observed that computers in this temporary work area had screens facing areas accessible by MFA personnel. Non-Criminal Justice Services personnel may have been able to view sensitive criminal justice information.

Some computer screens in temporary workspaces were positioned in a way that could allow unauthorized personnel to view sensitive criminal justice information, potentially compromising data security.

Salt Lake County Criminal Justice Services Policy: Utah Criminal Justice Information Systems 06-200, Part 2.0 The Security of UCJIS Records, Sections 2.3 – 2.5, states,

> "2.3 All computer screens with BCI information displayed on them must be out of public view.
> 2.4 BCI Users shall log off UCJIS upon leaving their workstation.
> 2.5 The public will not be allowed into private offices until it is determined all protected information, including computer screen, is secure from unauthorized sight."

Criminal Justice Services Management implemented a temporary arrangement using MFA space to ensure operational continuity. They also confirmed that the same safeguards used throughout the Criminal Justice Services were in place within this space shared with MFA.

Criminal Justice Services Management indicated that they are unable to disclose the specific BCI controls or safeguards employed to prevent unauthorized access to sensitive information, citing the information is considered confidential and cannot be disseminated.

Taking appropriate precautions to prevent unauthorized access is essential for protecting sensitive criminal justice information. Without these measures, there is a potential risk that such information could be accessed by individuals without proper clearance. This could inadvertently compromise the confidentiality and integrity of critical data, increasing the likelihood of unauthorized disclosure or misuse.

7.1	RECOMMENDATION	Protect Screen Information

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 RESPONSE: AGREE

IMPLEMENTATION DATE: 5/1/2025

SEE PAGE 34 FOR THE AGENCY'S FULL RESPONSE TO OUR RECOMMENDATION

COMPLETE LIST OF AUDIT RECOMMENDATIONS

This report made the following 12 recommendations

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

RECOMMENDATION 6.2:

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

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 RESPONSE

SALT LAKE COUNTY
CRIMINAL JUSTICE SERVICES

JENNIFER WILSON
SALT LAKE COUNTY MAYOR

KELLY COLOPY
SALT LAKE COUNTY
HUMAN SERVICES
DEPARTMENT DIRECTOR

KELE GRIFFONE
DIVISION DIRECTOR

JESSICA THAYER
ASSOCIATE DIRECTOR

MADISEN DRURY
ASSOCIATE DIRECTOR

April 14, 2025

Auditor Chris Harding, CPA
Office of the Auditor
Salt Lake County
2001 S State Street
Salt Lake City, UT 84121

Auditor Harding,

Thank you for taking the time to review our internal controls and data access procedures. We appreciate the dedication of you and your team. This report will assist my division's focus on data access and protection.

Criminal Justice Services is committed to providing exceptional services to residents of Salt Lake County. We value the audit process as a tool to help maintain accountability to those we serve.

Please find our response below to each of the recommendations made in your report.

Sincerely,

Kele Griffone Digitally signed by Kele Griffone
Date: 2025.04.22 08:36:42 -06'00'

Kele Griffone
Director
Criminal Justice Services

SALT LAKE COUNTY
CRIMINAL JUSTICE SERVICES
2001 SOUTH STATE STREET
STE. S3-650
SALT LAKE CITY, UT 84190
PHONE (385) 468-3500
FAX (385) 468-3522
TTY: 7-1-1

AUDIT FINDING 1: Opportunity to Strengthen Network Access Termination Processes

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.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and Title of specific point of contact for implementation
Agree	Completed on 2/12/2025	Scott Rasmussen, Fiscal Manager

Narrative for Recommendation 1.1 including action plan.

CJS has strengthened internal controls by modifying procedures regarding terminated employees. This is accomplished through both tracking and written procedures located in a shared document on OneDrive. CJS added additional documented procedures regarding granting network access, revoking network access and documenting the access termination date. The procedures include documenting the party performing terminating activities and backup individuals performing each of the processes. The timeline to complete system terminations is no later than five working days after the termination. CJS also modified the new hire process to grant employee access only to systems according to the needs of the new hire's job duties. The retention of the shared OneDrive tracking sheet with the documentation of actions taken will be retained for five years after the termination date.

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Agree	Completed on 02/12/2025	Scott Rasmussen, Fiscal Manager

Narrative for Recommendation 1.2 including action plan.

CJS has strengthened internal controls by modifying procedures regarding terminated employees. This is being accomplished through both tracking and written procedures located in a shared document on OneDrive. CJS added additional documented procedures regarding granting network access, revoking network access and documenting the access termination date. The procedures include documenting the party performing terminating activities andbackup individuals performing each of the processes. The timeline to complete system terminations is no later than five working days after the termination. CJS also modified the new hire process to grant employee access only to systems according to the needs of the new hire's job duties. The retention of the shared OneDrive tracking sheet with the documentation of actions taken will be retained for five years after the termination date.

AUDIT FINDING 2: Opportunities to Strengthen Timeliness and Consistency of Application Access Removal

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Agree	Completed on 2/12/2025	Scott Rasmussen, Fiscal Manager

Narrative for Recommendation 2.1 including action plan.

CJS has strengthened internal controls by modifying procedures regarding terminated employees. This is being accomplished through both tracking and written procedures located in a shared document on OneDrive. CJS added additional documented procedures regarding granting network access, revoking network access and documenting the access termination date. The procedures include documenting the party performing terminating activities andbackup individuals performing each of the processes. The timeline to complete system terminations is no later than five working days after the termination. CJS also modified the new hire process to grant employee access only to systems according to the needs of the new hire's job duties. The retention of the shared OneDrive tracking sheet with the documentation of actions taken will be retained for five years after the termination date.

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Agree	Completed on 2/12/2025	Scott Rasmussen, Fiscal Manager

Narrative for Recommendation 2.2 including action plan.

CJS has strengthened internal controls by modifying procedures regarding terminated employees. This is being accomplished through both tracking and written procedures located in a shared document on OneDrive. CJS added additional documented procedures regarding granting network access, revoking network access and documenting the access termination date. The procedures include documenting the party performing terminating activities and backup individuals performing each of the processes. The timeline to complete system terminations is no later than five working days after the termination. CJS also modified the new hire process to grant employee access only to systems according to the needs of the new hire's job duties. The retention of the shared OneDrive tracking sheet with the documentation of actions taken will be retained for five years after the termination date.

AUDIT FINDING 3: Opportunities to Improve Data Entry Consistency in eSupervision

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Disagree	6/1/2025	Jessica Thayer, Associate Director

Narrative for Recommendation 3.1 including action plan.

CJS does not agree with a rating of Significant or Moderate risk finding as the location of where something is documented in eSupervision has absolutely no impact on client services. Additionally, no matter the location of U/A results in eSupervision (Chrono note versus Compliance note), CJS case managers all have access to our U/A providers management system (Aversys) which contains a historical record of a client's test dates, results, etc. In other words, results are always accessible to case managers; the risk finding should therefore be reduced to Low.

The purpose of a Case Note Policy is to document staff actions and client activity; the fact that a U/A result was documented in a Chrono note versus a Compliance note (two possible case note locations) does not pose a Significant or Moderate risk to our clients' success on supervision or our staff's ability to monitor that supervision. While our Case Note Policy provides direction on documenting U/A results as a Compliance Note, our Program policies reference alternative locations and practices based on individual client needs, responsivity practices, and court orders. Because we agree that our agency wide Case Note Policy should note those variances, we will make the necessary changes; however, we strongly disagree that this poses any Significant or Moderate risk to our clients or practices.

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Disagree	6/1/2025	Jessica Thayer, Associate Director

Narrative for Recommendation 3.2 including action plan.

As indicated above, CJS does not agree with a rating of Significant or Moderate risk finding as the location of where U/A results are documented in eSupervision has absolutely no impact on client services; instead, the risk rating should be LOW.

CJS Case Manager Supervisors and Managers already perform regular quality assurance audits of caseloads but the focus is on those areas that impact client services; those focus areas, in order of priority, are liability, client contact and related documentation, client barriers and resources, being responsive to client needs, and finally, technical pieces (which includes the documentation of U/A results). These audits vary in frequency and are based on individual case manager skill/need. On average, the audits are conducted quarterly.

While the location of U/A results in eSupervision is not critical to client services, CJS will ensure that moving forward, U/A documentation meets the updated policy direction, and that supervisor and staff audit this practice in at least two of their yearly audits and provide a yearly case note training. To ensure compliance with this practice, CJS supervisors will submit a written report, twice yearly, to their managers and directors documenting the date(s) of specific case note audits and each case manager's adherence (and related follow up if applicable) to case note policy. The first audit and report will be due by 06/30/25 which will be about 60 days after the updated Case Note Policy is issued and reviewed with staff.

AUDIT FINDING 4: Opportunities to Improve Controls for the Disposal of Surplus Assets Containing Hard Drives

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.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and Title of specific point of contact for implementation
Agree	Completed on 2/15/2025	Scott Rasmussen, Fiscal Manager

Narrative for Recommendation 4.1 including action plan.

CJS provided documentation to the internal audit team for 100% of the assets disposed of during the audit period. CJS is committed to continuous improvement. Internal auditors identified a discrepancy in the asset description field for one asset out of the 511 assets submitted (#10393) on the PM-2. CJS listed the asset as a "ThinkPad Yoga 260 Laptop & Docking Station." The PM-2 description should have been "Yoga Docking Station." This error was corrected in the CJS database. This error resulted in a less than 0.2% error entered by CJS. CJS committed to obtaining a 0% error rate.

CJS follows County Policy 1125 and exercises care in disposing of controlled assets. As part of the disposal process, CJS prints a hard copy from the asset database and reconciles this list against the physical assets to be disposed. After a careful reconciliation process has been carried out, CJS then fills out a PM-2 form to list assets to be disposed. The PM-2 is reviewed and signed by CJS and by the other party receiving the asset.

Any assets turned over to TAMS or other County-approved vendors will be marked accordingly on each PM-2 form. CJS will mark the "E-waste Disposal box" on the PM-2 form. The County's

vendor does not receive a copy of the PM-2. The vendor disposes or overwrites the data regardless of the box being checked on the PM-2 per their contract # MA4484 TAMS, LLC which was signed 3/20/2024:

"4. Scope of Work

4.1 Equipment Collection and Processing for Reuse or Surplus

i. The contractor possesses the capability to collect, palletize, transport, store, resell, and/or donate used equipment, as specified by the entity, for its original intended purpose. This includes repairing or replacing parts, upgrading memory or other components, and installing new software.

ii. The process involves disassembly to recover components for resale or reuse in other equipment. ***Contractor must overwrite data on hard drives and electronic information storage devices. If data cannot be wiped, the contractor must destroy the devices to the extent that data recovery is impossible***

4.4 Data Destruction

i. Contractor must ensure data sanitization meets DoD 5220.22-M standards or greater.

ii. If data cannot be wiped, the contractor must destroy the devices to prevent data recovery."

AUDIT FINDING 5: Opportunities to Enhance Network Access Controls to Strengthen Data Security

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Agree	6/1/2025	Dave Nicoll, Information Services Manager

Narrative for Recommendation 5.1 including action plan.

At the time of the audit, staffing constraints and vacancies resulted in a reassignment of job duties related to network access. As part of this transition, all staff were assigned to the correct security groups giving them the required access/information to perform their job duties. However, CJS management agrees that improved communication with the County Auditor's staff throughout the audit process could help avoid potential discrepancies by explaining and justifying agency processes and needs to the internal auditors at the time of inspection and questioning.

Staff are often assigned to multiple work teams for cross-training and as client needs dictate, which can require them to be assigned to multiple security groups. Currently, the Information Systems Manager is working with County IT to review and enhance network access. The Information Systems Manager will review security group roles quarterly to ensure proper access is granted for employees to perform their appropriate job duties. Documentation will be maintained to show the results of these reviews.

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
- Agree	6/1/2025	Dave Nicoll, Information Services Manager

Narrative for Recommendation 5.2 including action plan.

At the time of the audit, staffing constraints and vacancies resulted in a reassignment of job duties related to network access. As part of this transition, all staff were assigned to the correct security groups giving them the required access/information to perform their job duties. However, CJS management agrees that improved communication with the County Auditor's staff throughout the audit process could help avoid potential discrepancies by explaining and justifying agency processes and needs to the internal auditors at the time of inspection and questioning.

Staff are often assigned to multiple work teams for cross-training and as client needs dictate, which can require them to be assigned to multiple security groups. Currently, the Information

Systems Manager is working with County IT to review and enhance network access. The Information Systems Manager will review security group roles quarterly to ensure proper access is granted for employees to perform their appropriate job duties. Documentation will be maintained to show the results of these reviews.

AUDIT FINDING 6: Opportunity to Enhance UWITS User Permissions to Align with Business Needs

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Agree	Completed on 02/20/25	Heidi Marks, Section Manager

Narrative for Recommendation 6.1 including action plan.

CJS adjusted user permission levels in UWITS to reflect the appropriate level of access.

RECOMMENDATION 6.2: We recommend that Criminal Justice Services Management monitor and modify user application access whenever needs change.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Agree	5/1/2025	Heidi Marks, Section Manager

Narrative for Recommendation 6.2 including action plan.

The UWITS Navigator will conduct an audit of UWITS permissions every quarter to ensure they meet the limited access and read only expectations for Clinical Case Managers and submit a written report of findings to the Section Manager and Associate Director of the Specialty Court Programs. At any point prior to that quarterly audit, if access is changed or terminated, the Navigator/Back-Up Navigator, will notify the Associate Director in writing.

AUDIT FINDING 7: Opportunity to Enhance Workstation Privacy to Safeguard Sensitive Information

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and Title of specific point of contact for implementation**
Agree	May 31, 2025	Melissa Slade, Internal Services Manager

Narrative for Recommendation 7.1 including action plan.

The Federal Bureau of Investigation (FBI) and Utah Bureau of Criminal Identification (BCI) have the administrative right to audit compliance. CJS consults with BCI in new working environments to ensure compliance. CJS has passed BCI audits and complies with all BCI requirements. The Auditors recommendation for updating the policy will be addressed to review the language to ensure alignment and clarity across the sections, while maintaining the intent to protect UCJIS information.

AUDITOR ADDENDUM:

Finding 3: Opportunities to Improve Data Entry Consistency in eSupervision

Management disagrees with the risk rating and suggests that the location of urinalysis (U/A) data entry in eSupervision has "absolutely no impact on client services." While we recognize that case managers can access Aversys directly, this audit reviewed compliance with CJS Policy 03-100, which clearly requires that urinalysis results be entered in eSupervision using the Compliance Note format.

Audits conducted by the County Auditor are based not only on external standards (e.g., federal or state regulations) but also on the internal policies adopted by agencies themselves. Per Utah State Code 17-19a-204(2), the Auditor "may audit compliance with a county policy or procedure." CJS Policy 03-100 is one such policy, and we found that the required procedures were not followed in 87% of tested samples.

Further, consistent and accurate documentation within eSupervision is essential for continuity of care, performance measurement, and audit trails. While management may revise policies to allow more flexibility, until such updates occur, the audit team must assess compliance with current policies as written.

We appreciate management's willingness to revise the policy and implement improved monitoring procedures, which we believe will help strengthen internal controls moving forward.