Sheriff's Office – Data Center
Audit of Backup and Recovery Processes
Maricopa County Internal Audit
September 2019

Why This Audit Is Important

The Maricopa County Sheriff's Office (MCSO) data center supports MCSO business operations by managing electronic data collection, storage, and processing. This includes creating a copy of critical booking or inmate data that can be recovered should an unplanned event occur (e.g., hardware or software failure, data corruption, malicious attack, accidental deletion, natural disaster). Effective backup and recovery processes help ensure that the law enforcement community across the state and nation can rely on critical MCSO information required to do their jobs.

We performed this audit to ensure that MCSO has adequate backup and recovery procedures in place for resuming normal information processing.

Key Findings

- Overarching data backup and recovery policies and procedures were not formalized to help ensure critical data is effectively stored.
- Data storage costs and legal risks can be reduced by implementing an electronic data retention policy.
- Disposal and data sanitizing procedures can be improved.

All key findings were addressed through agreed-upon management action plans.

What We Audited

Below is a summary of work performed and findings. Corresponding recommendations and responses are on page 3. The responses were approved by Rich Johnson, MCSO Chief Information Officer, on August 16, 2019. More detailed observations and recommendations were communicated to management throughout the audit process.

Backup Copies

Background – Backup copies allow data to be restored from an earlier point in time to help an organization recover sensitive data after an unplanned event. Effective backup and recovery processes include scheduling regular backup events to reduce the amount of data lost between backups, saving backup copies on a separate medium (e.g., external drive, disk or cloud storage, or tape drive), and storing the copies at a separate location from the primary data.

Observations – We interviewed MCSO personnel and reviewed available documents and found that MCSO has not established overarching policies providing guidance for backup and recovery of data within critical MCSO applications. We also found related desk procedures were incomplete or informal (**Recommendation 1**).

We observed MCSO's processes for backup tape management, including tape rotation and data recovery. We found instances where backup tape management processes could be strengthened. Detailed technical findings and recommendations were communicated directly to MCSO and corrective action plans are in place. For security purposes, further details are restricted from this public report.

Electronic Data Retention

Background – A data retention policy helps an organization track how long it must retain its data. State statute established the Arizona State Library, Archives, and Public Records (AZLAPR) as having sole authority of setting record retention periods, including timelines for law enforcement and criminal history records.

Observations – MCSO has an overarching records retention schedule filed with AZLAPR; however, a records retention schedule specifically addressing electronic data has not been implemented (**Recommendation 2**). Appropriate record retention schedules help reduce legal and financial risks associated with failure to retain criminal records appropriately. Furthermore, keeping data longer than required may be costly and use unnecessary storage space.

Media Disposal

Background – When data stored on media equipment (e.g., tapes, hard drives) is no longer needed, it must be destroyed or sanitized according to federal and state requirements.

Observations – We reviewed MCSO's media protection and disposal procedures and noted they did not describe the specific methods for destroying or sanitizing data, and did not include requirements for tracking media equipment inventory (**Recommendation 3**). Inadequate disposal procedures increase the risk of unapproved data disclosure.

Additional Information

This audit was approved by the Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing. This report is intended primarily for the County Board of Supervisors, County leadership, and other County stakeholders. However, this report is a public record and its distribution is not limited.

Due to unforeseen circumstances, we opted to postpone work in other audit areas of the MCSO data center (e.g., access controls, configuration management). We intend to resume our work as a separate audit once the MCSO's new jail management system is implemented.

If you have any questions about this report, please contact Mike McGee, County Auditor, at 602-506-1585.

Recommendations and Responses

Recommendations	Responses
1 Develop policies and procedures establishing backup, tape management, and recovery expectations based on data criticality.	Concur – in progress The Technology Bureau is in the process of reviewing current policies and processes to formalize overarching backup and recovery policies and procedures, and strengthen areas as listed in the recommendation. Target Date: 12/31/2019
2 Prepare a written electronic data retention policy based on laws, statutes, and operational needs.	Concur – in progress The Technology Bureau will review current data retention requirements and prepare a written data retention policy based on these needs. Target Date: 12/31/2019
3 Update current procedures to ensure appropriate protection, tracking, and sanitization/disposal of media in compliance with Criminal Justice Information Services (CJIS) requirements and National Institute of Standards and Technology (NIST) standards.	Concur – in progress The Technology Bureau is updating IAS SOP 17-3 Media Protection & Disposal to strengthen guidance on end-of-life media inventory, sanitization/disposal, reviews, and validation. Target Date: 12/31/2019