

The seal of the Missouri State Auditor is circular and features a central figure holding a scale and a sword. The text around the seal reads "SEAL OF THE STATE AUDITOR" at the top, "JUSTICE WE STAND DIVIDED" in the middle, and "1820 MISSOURI 1892" at the bottom.

Nicole Galloway, CPA

Missouri State Auditor

Summary of Local Government and Court Audit Findings - Information Security Controls

Report No. 2020-065

September 2020

auditor.mo.gov



Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Summary of Local Government and Court Audit Findings - Information Security Controls

User Access Management	Access to certain systems is not adequately restricted. The user access of former employees is not disabled timely.
User Authentication	Passwords are not required to be changed on a periodic basis. User accounts and passwords for accessing computers and various systems are shared by users. A password is not required to logon and authenticate access to a computer. Passwords are not required to contain a minimum number of characters.
Security Controls	Inactivity controls have not been implemented to lock a computer or system after a certain period of inactivity. Security controls have not been implemented to lock access to a computer or system after a specified number of unsuccessful logon attempts.
Backup and Recovery	Data in various systems is not periodically backed up. Data backups are not stored at a secure off-site location. Periodic testing of backup data is not performed.
Data Management and Integrity	Data management and integrity controls to guard against the improper modification or destruction of data and information have not been implemented.

Because of the nature of this report, no rating is provided.

Summary of Local Government and Court Audit Findings

Information Security Controls

Table of Contents

State Auditor's Report	2
------------------------	---

Audit Issues	
1. User Access Management	3
2. User Authentication.....	3
3. Security Controls	5
4. Backup and Recovery.....	6
5. Data Management and Integrity	7

Appendix	
Audit Reports	8



NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Michael L. Parson, Governor
and
Members of the General Assembly
Jefferson City, Missouri

This report was compiled using local government and court audit reports issued by my office between July 2019 and June 2020 (report numbers 2019-049 through 2019-132 and 2020-001 through 2020-036). The objective of this report was to summarize recent information security control issues and recommendations.

The recommendations address a variety of topics including user access management, user authentication, security controls, backup and recovery, and data management and integrity. The Appendix lists the 10 reports with findings covering these topics.

A handwritten signature in black ink that reads "Nicole R. Galloway".

Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits: Robert E. Showers, CPA
Audit Manager: Alex R. Prenger, M.S.Acct., CPA, CISA, CFE, CGAP
Audit Staff: Zachery Harris

Summary of Local Government and Court Audit Findings

Information Security Controls

Audit Issues

1. User Access Management

1.1 Access rights and privileges

Access to certain systems is not adequately restricted. Access rights and privileges are used to determine what a user can do after being allowed into a system, such as read or write to a certain file. Unrestricted system access allows the capability to make unauthorized changes to records or to delete or void transactions after the transactions have been entered in the system. In addition, adequate supervisory reviews of users are not performed. Access should be limited based on user needs and job responsibilities.

Without adequate user access restrictions, there is an increased risk of unauthorized changes to data and records and of the loss, theft, or misuse of funds.

Recommendation

Ensure user access rights are limited to only what is necessary to perform job duties and responsibilities.

Report Source

2019-068 (Camden County)
2019-069 (Camden County Collector and Property Tax System)
2019-110 (Pemiscot County)
2019-113 (45th Judicial Circuit Lincoln County)

1.2 Terminated employees

The user access of former employees is not disabled timely.

Without effective procedures to remove access upon termination, former employees could continue to have access to critical or sensitive data and records, which increases the risk of the unauthorized use, modification, or destruction of data and information.

Recommendation

Ensure user access is promptly deleted following termination of employment to prevent unauthorized access to computer systems and data.

Report Source

2019-101 (Ozark County)
2019-118 (Barry County)

2. User Authentication

2.1 Passwords not changed

Passwords are not required to be changed on a periodic basis. As a result, there is less assurance passwords are effectively limiting access to computer systems and data files to only those individuals who need access to perform their job responsibilities. Passwords should be changed periodically to reduce the risk of unauthorized access to and use of systems and data.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Without requiring passwords to be periodically changed, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased.

Recommendation

Ensure passwords are periodically changed to prevent unauthorized access to computers and data.

Report Source

2019-050 (Madison County Collector and Property Tax System)
2019-057 (Dent County)
2019-101 (Ozark County)
2019-118 (Barry County)
2020-020 (7th Judicial Circuit City of Excelsior Springs Municipal Division)
2020-029 (City of Monroe City)

2.2 Sharing passwords

User accounts and passwords for accessing computers and various systems are shared by users. The security of a password system is dependent upon keeping passwords confidential. By allowing users to share accounts and passwords, individual accountability for system activity could be lost and unauthorized system activity could occur.

Without strong user account and password controls, including maintaining the confidentiality of passwords, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased.

Recommendation

Ensure unique user accounts and passwords are required to access computers and data. In addition, ensure users understand the importance of maintaining the confidentiality of passwords.

Report Source

2019-050 (Madison County Collector and Property Tax System)
2019-068 (Camden County)
2019-069 (Camden County Collector and Property Tax System)
2019-110 (Pemiscot County)
2019-118 (Barry County)
2020-020 (7th Judicial Circuit City of Excelsior Springs Municipal Division)
2020-029 (City of Monroe City)

2.3 Password not required

A password is not required to logon and authenticate access to a computer.

Without requiring passwords to access a computer or system, there is no assurance the data or system is protected from unauthorized access and use.

Recommendation

Ensure passwords are required to authenticate access to computer systems and data.

Report Source

2020-020 (7th Judicial Circuit City of Excelsior Springs Municipal Division)



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

2.4 Password complexity

Passwords are not required to contain a minimum number of characters. Strong passwords are often the first line of defense into a computer or system. As a result, an appropriate minimum character length should be established so passwords cannot be easily guessed or identified using password-cracking mechanisms.

Without enforcing password complexity by requiring a minimum number of characters, there is an increased risk that passwords can be more easily guessed, allowing unauthorized access to data and systems.

Recommendation

Ensure passwords contain a minimum number of characters so they cannot be easily guessed.

Report Source

2019-050 (Madison County Collector and Property Tax System)
2019-057 (Dent County)
2019-101 (Ozark County)
2019-110 (Pemiscot County)
2019-118 (Barry County)
2020-029 (City of Monroe City)

3. Security Controls

3.1 Inactivity control

Inactivity controls have not been implemented to lock a computer or system after a certain period of inactivity. To reduce the risk of unauthorized individuals accessing an unattended computer and having potentially unrestricted access to programs and data files, users should log off computers when unattended and an inactivity control should be implemented to lock a computer or terminate a user session after a certain period of inactivity.

Without an inactivity control, there is an increased risk of unauthorized access to computers and the unauthorized use, modification, or destruction of data.

Recommendation

Ensure an inactivity control is implemented to lock a computer or system after a certain period of inactivity.

Report Source

2019-101 (Ozark County)
2019-118 (Barry County)
2020-029 (City of Monroe City)

3.2 Unsuccessful logon attempts

Security controls have not been implemented to lock access to a computer or system after a specified number of unsuccessful logon attempts. Logon attempt controls lock the capability to access a computer or system after a specified number of consecutive unsuccessful logon attempts, and are necessary to prevent unauthorized individuals from continually attempting to logon to a computer or system by guessing passwords.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Without effective controls to limit the number of consecutive unsuccessful logon attempts, there is less assurance sensitive data is effectively protected from unauthorized access.

Recommendation

Ensure a security control is implemented to lock access to a computer or system after multiple unsuccessful logon attempts.

Report Source

2019-050 (Madison County Collector and Property Tax System)
2019-057 (Dent County)
2019-101 (Ozark County)
2019-118 (Barry County)
2020-029 (City of Monroe City)

4. Backup and Recovery

4.1 Data backup

Data in various systems is not periodically backed up. Preparation of backup data, preferably on a daily or at least weekly basis, provides reasonable assurance data could be recovered if necessary.

Without regular data backups, there is an increased risk critical data will not be available for recovery should a disruptive incident occur.

Recommendation

Ensure data is regularly backed up.

Report Source

2019-057 (Dent County)

4.2 Off-site storage

Data backups are not stored at a secure off-site location. Data backups are performed; however, the backup files are stored at the same location as the original data leaving the files susceptible to the same damage as that data.

Without storing backup data at a secure off-site location, critical data may not be available for restoring systems following a disaster or other disruptive incident.

Recommendation

Ensure backup data is stored in a secure off-site location.

Report Source

2019-050 (Madison County Collector and Property Tax System)
2019-118 (Barry County)

4.3 Periodic testing

Periodic testing of backup data is not performed. Such testing is necessary to ensure the backup process is functioning properly and to ensure all essential data can be recovered.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Without testing the full backup process, management cannot be assured the entire system can be restored when necessary.

Recommendation

Ensure backup data is tested on a regular, predefined basis.

Report Source

2019-050 (Madison County Collector and Property Tax System)
2019-118 (Barry County)

**5. Data Management
and Integrity**

Data management and integrity controls to guard against the improper modification or destruction of data and information have not been implemented. As a result, critical systems, such as property tax systems, do not prevent users from voiding receipt transactions after they are completed. In addition, systems do not have the audit trail controls or functionality to generate reports of deleted or modified transactions.

Without data management, integrity, and audit trail controls, there is an increased risk of manipulation of data without detection and the loss, theft, or misuse of funds.

Recommendation

Ensure adequate data management, integrity, and audit trail controls are in place to allow for the proper accountability of all transactions.

Report Source

2019-069 (Camden County Collector and Property Tax System)

Summary of Local Government and Court Audit Findings

Information Security Controls

Appendix - Audit Reports

Report Number	Title	Publication Date
2019-050	Madison County Collector and Property Tax System	July 2019
2019-057	Dent County	July 2019
2019-068	Camden County	August 2019
2019-069	Camden County Collector and Property Tax System	August 2019
2019-101	Ozark County	October 2019
2019-110	Pemiscot County	November 2019
2019-113	45th Judicial Circuit Lincoln County	November 2019
2019-118	Barry County	December 2019
2020-020	7th Judicial Circuit City of Excelsior Springs Municipal Division	April 2020
2020-029	City of Monroe City	June 2020