Office of Missouri State Auditor

Nicole Galloway, CPA

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

Report No. 2018-051
August 2018

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. Periodic reviews of users' access to data and other information to ensure access remains appropriate and aligned with job duties are not performed.
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 backups are not stored at a secure off-site location. Periodic testing of backup data is not performed.
Data Management	Data integrity controls to guard against the improper modification or destruction of data and information have not been implemented. The attendance system does not limit the time frame during which changes can be made and there is no review by officials to ensure changes made to current school year attendance records are appropriate.

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

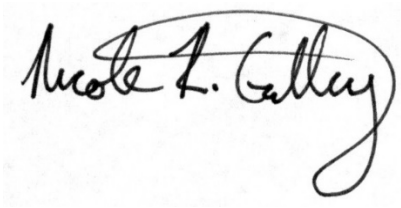
Summary of Local Government and Court Audit Findings
Information Security Controls
Table of Contents

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 2017 and June 2018 (report numbers 2017-060 through 2017-155 and 2018-001 through 2018-043). 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. The Appendix lists the 26 reports with findings covering these topics.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Senior Director:	Douglas J. Porting, CPA, CFE
Audit Manager:	Jeffrey Thelen, CPA, CISA

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

2017-069 (Crawford County)
2017-116 (New Madrid County)
2017-128 (Texas County)
2017-132 (St. Clair County)
2018-012 (Stoddard 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

2017-150 (Pemiscot Memorial Health Systems)

1.3 Periodic review of user accounts

Periodic reviews of users' access to data and other information to ensure access remains appropriate and aligned with job duties are not performed. As users' work assignments and job responsibilities change, access rights to data may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access to data.

Without periodically reviewing user access rights, there is an increased risk that unauthorized alterations of the rights will go undetected or that access rights may not be aligned with current job duties.

Recommendation

Ensure periodic reviews of user access to data and other information resources are performed to ensure access rights remain appropriate and are commensurate with job duties and responsibilities.

Report Source

2017-108 (41st Judicial Circuit/Macon County)
2017-138 (45th Judicial Circuit/Pike 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.

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

2017-064 (Morgan County)
2017-068 (Daviess County)
2017-069 (Crawford County)
2017-087 (Mercer County)
2017-088 (Moniteau County)
2017-107 (Macon County)
2017-109 (City of Lexington)
2017-126 (Scotland County)
2017-127 (Cooper County)
2017-132 (St. Clair County)
2017-144 (Pike County)
2017-150 (Pemiscot Memorial Health Systems)
2018-012 (Stoddard County)
2018-027 (Dade County)
2018-028 (37th Judicial Circuit/City of Winona Municipal Division)
2018-033 (Osage County)
2018-037 (Vernon County Ambulance District)
2018-040 (30th Judicial Circuit/City of Seymour Municipal Division)

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

2017-087 (Mercer County)
2017-088 (Moniteau County)
2017-107 (Macon County)
2017-132 (St. Clair County)
2017-144 (Pike County)
2018-027 (Dade County)
2018-028 (37th Judicial Circuit/City of Winona Municipal Division)
2018-040 (30th Judicial Circuit/City of Seymour Municipal Division)

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

2017-065 (Knox County)
2017-068 (Daviess County)
2017-107 (Macon County)
2017-144 (Pike County)

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	2018-012 (Stoddard County) 2018-033 (Osage County)

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	2017-065 (Knox County) 2017-068 (Daviess County) 2017-088 (Moniteau County) 2017-107 (Macon County) 2017-109 (City of Lexington) 2017-144 (Pike County) 2018-012 (Stoddard County) 2018-025 (Hazelwood School District) 2018-028 (37th Judicial Circuit/City of Winona Municipal Division)

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.

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

2017-065 (Knox County)
2017-088 (Moniteau County)
2017-107 (Macon County)
2017-109 (City of Lexington)
2017-144 (Pike County)
2018-012 (Stoddard County)
2018-027 (Dade County)
2018-028 (37th Judicial Circuit/City of Winona Municipal Division)
2018-040 (30th Judicial Circuit/City of Seymour Municipal Division)

4. Backup and Recovery

4.1 Off-site storage

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

2017-064 (Morgan County)
2017-065 (Knox County)
2017-074 (Putnam County Memorial Hospital)
2017-127 (Cooper County)
2017-144 (Pike County)
2018-012 (Stoddard County)
2018-027 (Dade County)
2018-031 (Village of Centertown)

4.2 Periodic testing

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

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

2017-065 (Knox County)
2017-144 (Pike County)
2017-150 (Pemiscot Memorial Health Systems)

2018-027 (Dade County)
2018-031 (Village of Centertown)

5. Data Management

5.1 Data Integrity

Data integrity controls to guard against the improper modification or destruction of data and information have not been implemented. In addition, audit trail controls to provide evidence demonstrating how a specific transaction was initiated, processed, and recorded have not been established. As a result, critical systems, such as property tax systems do not prevent users from changing the date used to calculate penalties, commissions, and fees. In addition, systems do not have the functionality to generate audit trail reports of voided or deleted transactions.

Without data 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 integrity, and audit trail controls are in place to allow for the proper accountability of all transactions.

Report Source

2017-065 (Knox County)
2017-128 (Texas County)

5.2 Student attendance data

The attendance system does not limit the time frame during which changes can be made and there is no review by officials to ensure changes made to current school year attendance records are appropriate. In addition, an audit trail report of changes made is not generated and reviewed to ensure all changes made to attendance records are accurate and appropriate.

Without limiting the time frame during which changes can be made or reviewing changes made, data is subject to erroneous changes that may significantly affect the reliability of official attendance reports.

Recommendation

Ensure student attendance data is accurately recorded and reported, including restricting the time frame during which changes can be made and ensure an audit trail of changes made to attendance data be prepared and reviewed for accuracy.

Report Source

2018-025 (Hazelwood School District)

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

Report Number	Title	Publication Date
2017-064	Morgan County	July 2017
2017-065	Knox County	July 2017
2017-068	Daviess County	July 2017
2017-069	Crawford County	July 2017
2017-074	Putnam County Memorial Hospital	August 2017
2017-087	Mercer County	August 2017
2017-088	Moniteau County	August 2017
2017-107	Macon County	October 2017
2017-108	41st Judicial Circuit/Macon County	October 2017
2017-109	City of Lexington	October 2017
2017-116	New Madrid County	October 2017
2017-126	Scotland County	October 2017
2017-127	Cooper County	November 2017
2017-128	Texas County	November 2017
2017-132	St. Clair County	November 2017
2017-138	45th Judicial Circuit/Pike County	November 2017
2017-144	Pike County	November 2017
2017-150	Pemiscot Memorial Health Systems	December 2017
2018-012	Stoddard County	March 2018
2018-025	Hazelwood School District	May 2018
2018-027	Dade County	May 2018
2018-028	37th Judicial Circuit/City of Winona Municipal Division	May 2018
2018-031	Village of Centertown	May 2018
2018-033	Osage County	June 2018
2018-037	Vernon County Ambulance District	June 2018
2018-040	30th Judicial Circuit/City of Seymour Municipal Division	June 2018