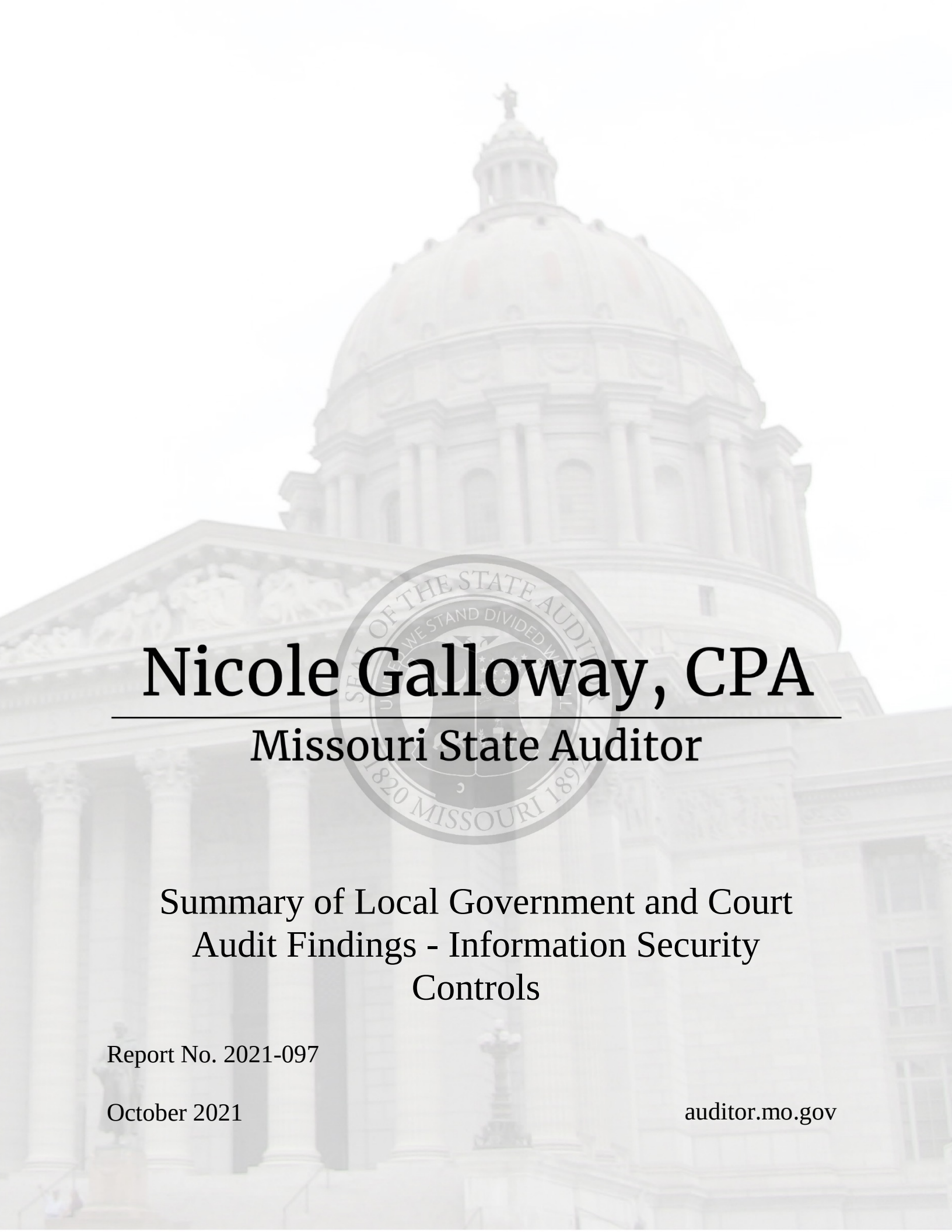


Nicole Galloway, CPA

Missouri State Auditor

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

Report No. 2021-097

October 2021

auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of 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. 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. Management has not developed a formal contingency plan to ensure business operations and computer systems can be promptly restored in the event of a disaster or other disruptive incident.
Data Management and Integrity	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 records area appropriate. Network access logs were always not maintained or monitored, because the logging function had been disabled.

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

All reports are available on our website: auditor.mo.gov

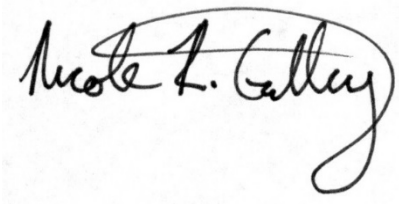
Summary of Local Government and Court Audit Findings
Information Security Controls
Table of Contents

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 2020 and June 2021 (report numbers 2020-037 through 2020-131 and 2021-001 through 2021-036). 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 11 reports with findings covering these topics.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	Robert E. Showers, CPA, CGAP
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. System access is typically restricted 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	2020-040 (Valley R-VI School District Attendance Procedures) 2020-118 (Thirty-Second Judicial Circuit Cape Girardeau 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	2020-115 (New Madrid County) 2021-001 (Jackson County Departmental and Other County Policies and Procedures)

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. Changing passwords periodically helps 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

2020-049 (Warren County)
2020-052 (Monroe County)
2020-100 (Madison County)
2020-101 (Dunklin County)
2020-115 (New Madrid County)
2021-012 (City of Forsyth)

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

2020-038 (City of Parma)
2020-052 (Monroe County)
2020-115 (New Madrid County)
2021-012 (City of Forsyth)
2021-033 (Jefferson County Collector and Property Tax System)

2.3 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, establishing an appropriate minimum character length makes it more difficult for passwords to easily be 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	2020-052 (Monroe County) 2020-100 (Madison County) 2020-115 (New Madrid 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. Having users log off computers when unattended and implementing an inactivity control to lock a computer or terminate a user session after a certain period of inactivity will help reduce the risk of unauthorized individuals accessing an unattended computer and having potentially unrestricted access to programs and data file.

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	2020-052 (Monroe County) 2020-100 (Madison County) 2021-012 (City of Forsyth)

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	2020-052 (Monroe County) 2020-100 (Madison County) 2020-101 (Dunklin County)

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 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

2020-038 (City of Parma)
2020-101 (Dunklin County)
2021-012 (City of Forsyth)

4.2 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.

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

2020-101 (Dunklin County)

4.3 Contingency plan

Management has not developed a formal contingency plan to ensure business operations and computer systems can be promptly restored in the event of a disaster or other disruptive incident. A comprehensive written contingency plan typically includes plans for a variety of disaster situations and specify detailed recovery actions required to reestablish critical business, computer, and network operations. Once a contingency plan has been developed and approved, periodic testing and review is necessary.

Without an up-to-date and tested contingency plan, management has limited assurance the organization's business and computer operations can be promptly restored after a disruptive incident.

Recommendation

Develop a formal contingency plan and periodically test and evaluate the plan.

Report Source

2020-038 (City of Parma)

5. Data Management and Integrity

5.1 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 records area appropriate. In addition, an audit trail report of changes made is not generated and reviewed to ensure all changes made to attendance records are appropriate and accurate. 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	2020-040 (Valley R-VI School District Attendance Procedures)
5.2 Network access logs	The network access logs were not maintained or monitored for a period of time, because the logging function had been disabled. Without an effective method to identify, log and monitor significant security-relevant events, there is an increased risk that unauthorized or inappropriate system activity may not be detected.
Recommendation	Ensure network access logs are maintained and monitored.
Report Source	2021-001 (Jackson County Departmental and Other County Policies and Procedures)

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

Report Number	Title	Publication Date
2020-038	City of Parma	July 2020
2020-040	Valley R-VI School District Attendance Procedures	July 2020
2020-049	Warren County	August 2020
2020-052	Monroe County	August 2020
2020-100	Madison County	November 2020
2020-101	Dunklin County	November 2020
2020-115	New Madrid County	December 2020
2020-118	Thirty-Second Judicial Circuit Cape Girardeau County	December 2020
2021-001	Jackson County Departmental and Other County Policies and Procedures	January 2021
2021-012	City of Forsyth	March 2021
2021-033	Jefferson County Collector and Property Tax System	June 2021