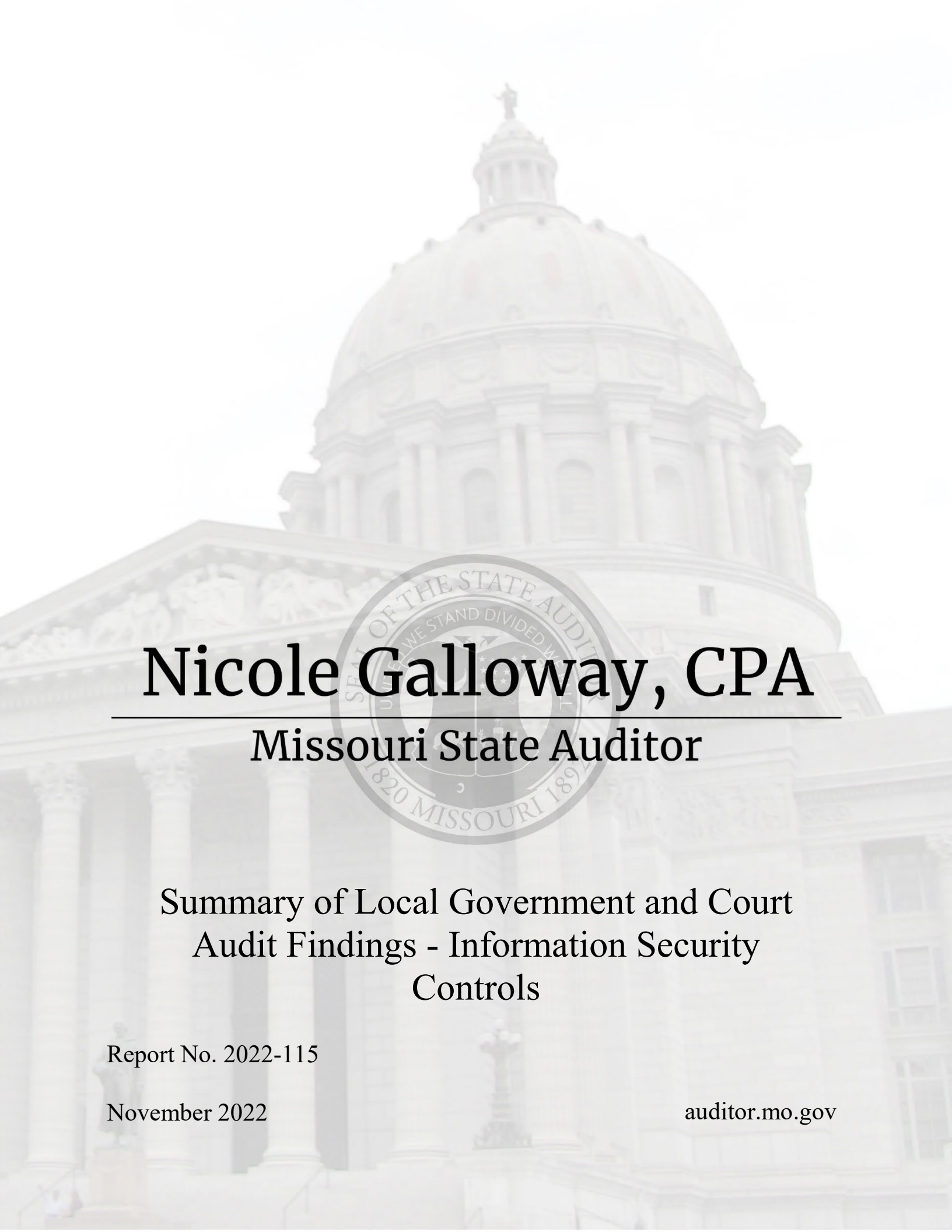


# Nicole Galloway, CPA

## Missouri State Auditor

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

Report No. 2022-115

November 2022

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 always 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. Antivirus protection software to detect and eradicate malicious code has not been installed on computer systems. |
| 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. Management has not developed a plan for resuming normal business operations and recovering computer systems and data in the event of a disaster or other extraordinary situation. |

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

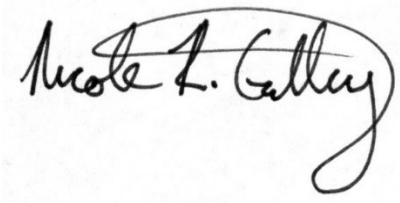
# Summary of Local Government and Court Audit Findings
# Information Security Controls
# Table of Contents

# 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 2021 and June 2022 (report numbers 2021-037 through 2021-134 and 2022-001 through 2022-037). 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, and backup and recovery. The Appendix lists the 16 reports with findings covering these topics.



Nicole R. Galloway, CPA
State Auditor

# 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. System access is typically restricted based on user needs and job responsibilities. Excessive system access can result in users having opportunities to perform unintended or undesired actions that are not aligned with their responsibilities. Potential consequences include unauthorized access or changes to sensitive records, or a failure to segregate duties. In addition, periodic evaluations of system access against assigned responsibilities, and/or independent reviews of changes made to records, are not performed.<br><br>Without adequate user access restrictions, there is reduced assurance that duties are properly segregated, and increased risk of improper activity occurring. |
| Recommendation | Ensure user access rights are limited to only what is necessary to perform job duties and responsibilities. |
| Report Source | 2021-073 (Marshall Public Schools)<br>2021-087 (Sixth Judicial Circuit Platte County)<br>2022-009 (Ralls County) |
| 1.2 Terminated employees | The user access of former employees is not disabled timely.<br><br>Without effective procedures to remove access, terminated employees could continue to have access to critical or sensitive resources or have opportunities to sabotage or otherwise impair operations or assets. The failure to timely remove access for terminated employees increases the risk of unauthorized access and may compromise the confidentiality and integrity of data. |
| Recommendation | Ensure user access is promptly deleted following termination of employment. |
| Report Source | 2021-073 Marshall Public Schools |

## 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

2021-038 (Henry County)
2021-042 (Dade County)
2021-069 (Oregon County)
2021-086 (Schuyler County)
2021-107 (Sullivan County)
2021-109 (Wayne County)
2021-110 (Harrison County)
2021-120 (Lawrence County)
2022-020 (City of Cross Timbers)
2022-030 (Worth County)
2022-035 (Reynolds County Collector and Property Tax System)

## 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

2021-069 (Oregon County)
2021-086 (Schuyler County)
2021-109 (Wayne County)
2021-120 (Lawrence County)
2022-035 (Reynolds County Collector and Property Tax System)

## 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** 2022-030 (Worth 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, 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**
2021-038 (Henry County)
2021-042 (Dade County)
2021-086 (Schuyler County)
2021-120 (Lawrence County)
2022-020 (City of Cross Timbers)

## 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 files.

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**
2021-038 (Henry County)
2021-051 (Macon County)
2021-107 (Sullivan County)

| | |
|---|---|
| 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.<br><br>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 | 2021-038 (Henry County)<br>2021-042 (Dade County)<br>2021-051 (Macon County)<br>2021-107 (Sullivan County)<br>2022-030 (Worth County)<br>2022-035 (Reynolds County Collector and Property Tax System) |
| 3.3 Antivirus protection | Antivirus protection software to detect and eradicate malicious code has not been installed on computer systems.<br><br>Without adequate antivirus protection, there is an increased risk that computers will be infected and that unauthorized processes will have an adverse impact on the confidentiality, integrity, or availability of a system. |
| Recommendation | Ensure computers and systems are adequately protected from computer viruses. |
| Report Source | 2022-020 (City of Cross Timbers) |

# 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.<br><br>Without regular data backups, there is an increased risk critical data will not be available for recovery should a disruptive event occur. |
| Recommendation | Ensure data is regularly backed up. |

| | |
|---|---|
| Report Source | 2021-069 (Oregon County)<br>2021-107 (Sullivan County)<br>2022-020 (City of Cross Timbers) |
| 4.2 Off-site storage | Data backups are not stored at a secure off-site location. Some 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.<br><br>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 | 2021-107 (Sullivan County)<br>2022-020 (City of Cross Timbers) |
| 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.<br><br>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 | 2022-017 (Clay County) |
| 4.4 Disaster recovery plan | Management has not developed a plan for resuming normal business operations and recovering computer systems and data in the event of a disaster or other extraordinary situation.<br><br>A formal, written disaster recovery plan is needed to guide an organization through computer system and overall operation recovery following a disaster or other extraordinary event. Periodic evaluation, testing and updating of the plan helps ensure the recovery process will be effective if the plan has to be implemented. |
| Recommendation | Develop a formal disaster recovery plan and periodically test and evaluate the plan. |
| Report Source | 2022-017 (Clay County) |

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

| Report Number | Title | Publication Date |
|---|---|---|
| 2021-038 | Henry County | July 2021 |
| 2021-042 | Dade County | July 2021 |
| 2021-051 | Macon County | August 2021 |
| 2021-069 | Oregon County | September 2021 |
| 2021-073 | Marshall Public Schools | September 2021 |
| 2021-086 | Schuyler County | October 2021 |
| 2021-087 | Sixth Judicial Circuit Platte County | October 2021 |
| 2021-107 | Sullivan County | November 2021 |
| 2021-109 | Wayne County | November 2021 |
| 2021-110 | Harrison County | November 2021 |
| 2021-120 | Lawrence County | December 2021 |
| 2022-009 | Ralls County | February 2022 |
| 2022-017 | Clay County | March 2022 |
| 2022-020 | City of Cross Timbers | March 2022 |
| 2022-030 | Worth County | June 2022 |
| 2022-035 | Reynolds County Collector and Property Tax System | June 2022 |