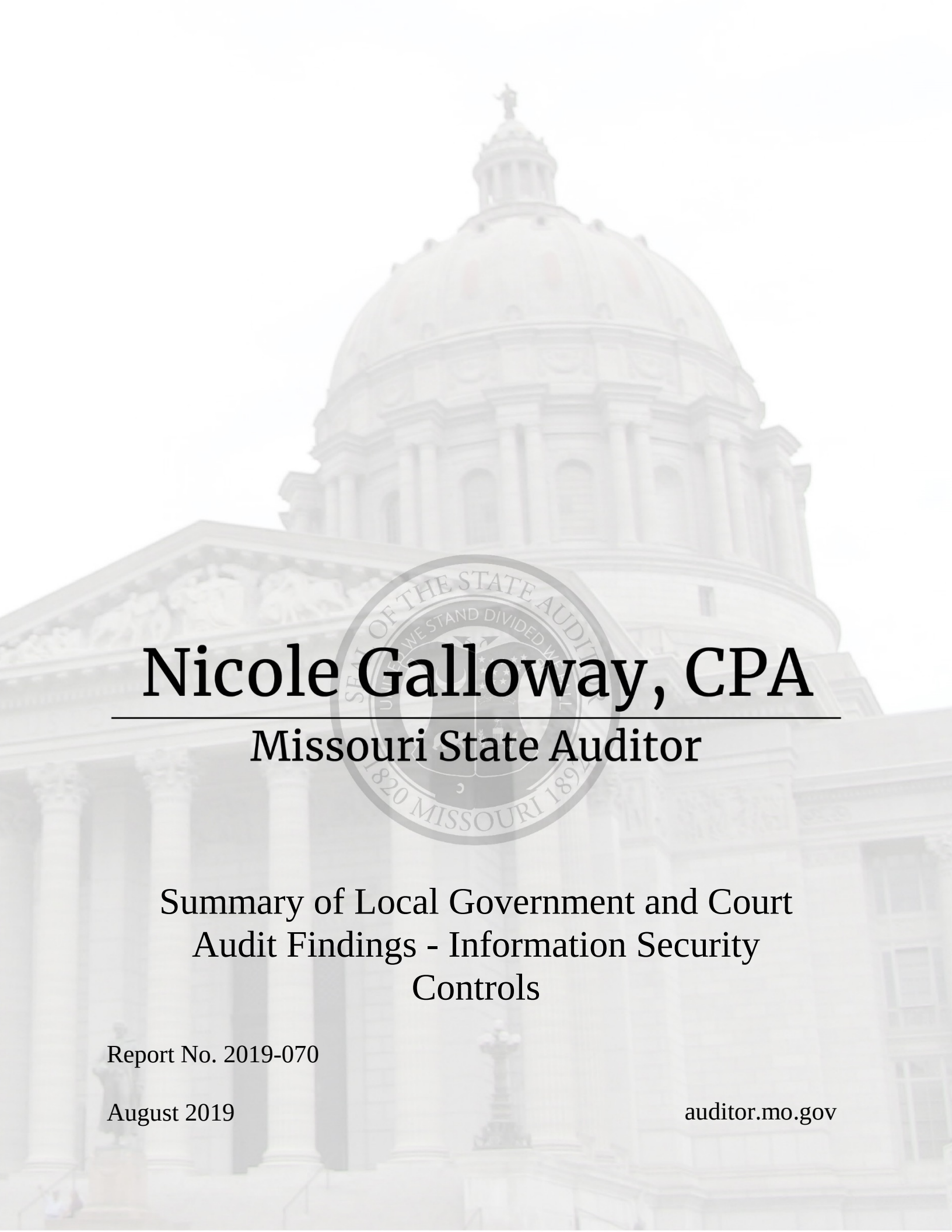


Nicole Galloway, CPA

Missouri State Auditor

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

Report No. 2019-070

August 2019

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. Policies and procedures are not fully established or documented to ensure areas housing information technology resources are properly controlled, monitored, and restricted.
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. Malware or 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 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	Data management and integrity controls to guard against the improper modification or destruction of data and information have not been implemented.
Vendor Security	Contracts for software acquired or outsourced from information technology vendors do not always contain security requirements. Security practices used by vendors are not always reviewed.

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

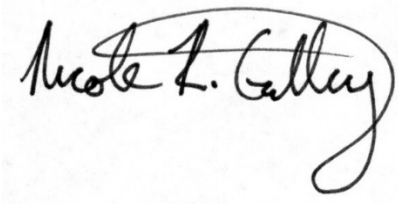
Summary of Local Government and Court Audit Findings
Information Security Controls
Table of Contents

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 2018 and June 2019 (report numbers 2018-044 through 2018-140 and 2019-001 through 2019-048). 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, data management and integrity, and vendor security. 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:	Alex R. Prenger, M.S.Acct., CPA, CISA, CFE, CGAP

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

2018-097 (Callaway County Collector and Property Tax System)
2019-002 (Miller County)
2019-013 (Crawford County Collector and Property Tax System)
2019-037 (Cape Girardeau County Collector and Property Tax System)
2019-043 (Howell 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

2019-009 (Gasconade County)
2019-019 (Village of Ferrelview)

1.3 Physical security

Policies and procedures are not fully established or documented to ensure areas housing information technology resources are properly controlled, monitored, and restricted. Such procedures include requesting, granting, periodically reviewing, and removing physical access.

Physical security is the protection of technology resources, including computers and network servers, from theft or damage. Physical security makes technology resources physically unavailable to unauthorized users and

can include locked rooms and cabinets, and other measures to protect assets from unauthorized access.

Inadequate physical security could lead to the loss of property, the disruption of service and functions, and the unauthorized disclosure of data and information. Without appropriate procedures to grant, periodically review, and remove access to sensitive areas, individuals may receive inappropriate or unauthorized access.

Recommendation

Establish and document physical access policies and procedures, ensure access to sensitive technology assets is necessary with job responsibilities, implement independent periodic reviews of access, and timely remove unnecessary access.

Report Source

2019-029 (City of St. Louis Information Technology Services Agency)

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

2018-046 (City of Coffey)
2018-069 (City of Winona)
2018-081 (Andrew County)
2018-110 (Laclede County)
2018-121 (Perry County)
2018-122 (Iron County)
2018-130 (Lewis County)
2018-139 (Washington County)
2018-140 (Clinton County)
2019-009 (Gasconade County)
2019-019 (Village of Ferrelview)
2019-035 (City of Miller)
2019-038 (Dallas County)
2019-041 (St. Francois County Prosecuting Attorney)

2019-043 (Howell County)
2019-046 (Hickory County)

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

2018-063 (Scott County)
2018-069 (City of Winona)
2018-081 (Andrew County)
2018-130 (Lewis County)
2019-007 (City of Hamilton)
2019-009 (Gasconade County)
2019-035 (City of Miller)
2019-043 (Howell County)

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

2018-049 (City of Bethany)
2018-122 (Iron 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

2018-046 (City of Coffey)
2018-069 (City of Winona)
2018-081 (Andrew County)
2019-009 (Gasconade County)
2019-035 (City of Miller)
2019-043 (Howell 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

2018-046 (City of Coffey)
2018-069 (City of Winona)
2018-081 (Andrew County)
2018-139 (Washington County)
2019-007 (City of Hamilton)
2019-035 (City of Miller)
2019-038 (Dallas County)
2019-043 (Howell County)
2019-046 (Hickory 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.

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: 2018-046 (City of Coffey)
2018-069 (City of Winona)
2018-099 (Smithville Area Fire Protection District)
2018-130 (Lewis County)
2018-139 (Washington County)
2019-009 (Gasconade County)
2019-043 (Howell County)

3.3 Malware protection

Malware or antivirus protection software to detect and eradicate malicious code has not been installed on computer systems.

Without adequate malware protection, there is an increased risk that computers will be infected by malware 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 malware.

Report Source: 2018-046 (City of Coffey)

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: 2018-120 (City of Greenville)

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

2018-046 (City of Coffey)
2018-049 (City of Bethany)
2018-069 (City of Winona)
2018-120 (City of Greenville)
2019-009 (Gasconade County)
2019-019 (Village of Ferrelview)

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.

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

2018-049 (City of Bethany)
2018-069 (City of Winona)
2018-099 (Smithville Area Fire Protection District)
2018-120 (City of Greenville)
2019-009 (Gasconade County)
2019-019 (Village of Ferrelview)
2019-035 (City of Miller)

4.4 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 should include 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, the plan should be periodically tested and reviewed.

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

2018-069 (City of Winona)
2018-120 (City of Greenville)
2019-019 (Village of Ferrelview)
2019-035 (City of Miller)

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

2018-097 (Callaway County Collector and Property Tax System)
2019-013 (Crawford County Collector and Property Tax System)

6. Vendor Security

Contracts for software acquired or outsourced from information technology vendors do not always contain security requirements. Security practices used by vendors are not always reviewed.

Accepted standards require organizations to identify and manage risk relating to a vendor's ability to securely deliver services; and when preparing contracts, to clearly define service requirements, including security and protection of intellectual property. Further security insight can be obtained by requesting independent reviews of vendor internal practices and controls, and/or reviewing vendor-supplied descriptions of security practices. Without consistently defining security requirements or assessing vendor security practices, there is less assurance in a vendor's ability to ensure services meet current and future data privacy and security needs.

Recommendation

Consistently ensure that vendor contracts contain security requirements, and review vendor security practices.

Report Source

2019-029 (City of St. Louis Information Technology Services Agency)