Office of Missouri State Auditor

Nicole Galloway, CPA

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

Report No. 2017-094
September 2017

auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in summary report of common cybersecurity mistakes

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. 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. In addition, audit trail controls to provide evidence demonstrating how a specific transaction was initiated, processed, and recorded have not been established.

Because of the nature of this report, no rating has been provided.

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

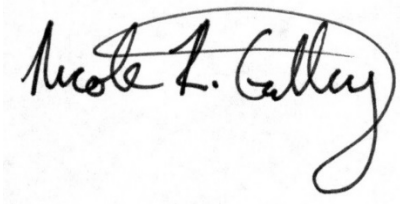
Summary of Local Government and Court Audit Findings
Information Security Controls
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Eric R. Greitens, 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 2016 and June 2017 (report numbers 2016-043 through 2016-147 and 2017-001 through 2017-059). This summary excludes the three audit reports issued during this period as part of the Cyber Aware School Audits Initiative (report numbers 2016-058, 2016-084, and 2016-089). These reports have been included in a separate summary for that initiative (report number 2016-112). 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 29 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:	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

2016-122 (Ripley County)
2016-123 (Mississippi County)
2016-135 (Polk County)
2017-025 (21st Judicial Circuit/City of Ferguson Municipal Division)

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

2016-118 (Wright County)
2016-123 (Mississippi County)
2016-136 (Lawrence 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

2016-048 (Vernon County)
2016-086 (Cedar County)
2016-088 (Carter County)
2016-090 (Putnam County)
2016-094 (City of Sparta)
2016-096 (Clark County)
2016-099 (McDonald County)
2016-117 (City of Rich Hill)
2016-118 (Wright County)
2016-119 (Chariton County)
2016-123 (Mississippi County)
2016-125 (Montgomery County)
2016-135 (Polk County)
2016-136 (Lawrence County)
2016-138 (Sullivan County)
2016-139 (Caldwell County)
2017-002 (41st Judicial Circuit/City of Shelbina Municipal Division)
2017-036 (Taney County Collector and Property Tax System)
2017-042 (Webster County)
2017-044 (Livingston County)
2017-046 (Barton County)
2017-049 (Bates County)
2017-056 (Shelby 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

2016-044 (38th Judicial Circuit/City of Sparta Municipal Division)
2016-048 (Vernon County)
2016-056 (26th Judicial Circuit/City of Linn Creek Municipal Division)
2016-088 (Carter County)
2016-094 (City of Sparta)
2016-099 (McDonald County)
2016-118 (Wright County)
2016-123 (Mississippi County)
2016-139 (Caldwell County)
2017-036 (Taney County Collector and Property Tax System)
2017-044 (Livingston County)
2017-046 (Barton 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

2016-096 (Clark County)
2016-136 (Lawrence County)
2017-046 (Barton 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

2016-099 (McDonald County)
2016-118 (Wright County)
2016-135 (Polk County)
2017-002 (41st Judicial Circuit/City of Shelbina Municipal Division)

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

2016-048 (Vernon County)
2016-094 (City of Sparta)
2016-096 (Clark County)
2016-136 (Lawrence County)
2016-139 (Caldwell County)
2017-044 (Livingston County)
2017-046 (Barton 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

2016-048 (Vernon County)
2016-094 (City of Sparta)
2016-096 (Clark County)
2016-118 (Wright County)
2016-136 (Lawrence County)
2017-002 (41st Judicial Circuit/City of Shelbina Municipal Division)

	2017-044 (Livingston County) 2017-046 (Barton 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	2016-119 (Chariton County)

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	2016-044 (38th Judicial Circuit/City of Sparta Municipal Division) 2016-094 (City of Sparta)
4.2 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	2016-044 (38th Judicial Circuit/City of Sparta Municipal Division) 2016-048 (Vernon County) 2016-094 (City of Sparta) 2016-096 (Clark County)

2016-117 (City of Rich Hill)
2016-119 (Chariton County)
2016-136 (Lawrence County)
2016-138 (Sullivan County)
2017-049 (Bates County)

4.3 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

2016-044 (38th Judicial Circuit/City of Sparta Municipal Division)
2016-048 (Vernon County)
2016-094 (City of Sparta)
2016-096 (Clark County)
2016-099 (McDonald County)
2016-136 (Lawrence County)
2016-138 (Sullivan County)
2017-049 (Bates County)

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

2016-094 (City of Sparta)

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. 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, including accounting systems, property tax systems, and case management systems do not prevent users from manually entering dates or from changing system amounts and code settings. For example, critical systems do not prevent users from (1) postdating or backdating receipts, (2) changing system-generated totals, including cash and check totals, (3) adjusting amounts and costs on cases after the initial judgement has been entered, or (4) entering codes to change a case status to closed even if an outstanding balance is still due. In addition, systems do not have the functionality to generate audit trail reports of voided or deleted transactions or receipts by date.

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

2016-088 (Carter County)
2016-090 (Putnam County)
2016-094 (City of Sparta)
2016-097 (Benton County)
2016-099 (McDonald County)
2016-122 (Ripley County)
2016-132 (Wright County Collector and Property Tax System)
2016-138 (Sullivan County)
2017-002 (41st Judicial Circuit/City of Shelbina Municipal Division)
2017-025 (21st Judicial Circuit/City of Ferguson Municipal Division)

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

Report Number	Title	Publication Date
2016-044	38th Judicial Circuit/City of Sparta Municipal Division	July 2016
2016-048	Vernon County	July 2016
2016-056	26th Judicial Circuit/City of Linn Creek Municipal Division	August 2016
2016-086	Cedar County	September 2016
2016-088	Carter County	September 2016
2016-090	Putnam County	September 2016
2016-094	City of Sparta	September 2016
2016-096	Clark County	September 2016
2016-097	Benton County	September 2016
2016-099	McDonald County	September 2016
2016-117	City of Rich Hill	November 2016
2016-118	Wright County	November 2016
2016-119	Chariton County	November 2016
2016-122	Ripley County	November 2016
2016-123	Mississippi County	November 2016
2016-125	Montgomery County	November 2016
2016-132	Wright County Collector and Property Tax System	December 2016
2016-135	Polk County	December 2016
2016-136	Lawrence County	December 2016
2016-138	Sullivan County	December 2016
2016-139	Caldwell County	December 2016
2017-002	41st Judicial Circuit/City of Shelbina Municipal Division	January 2017
2017-025	21st Judicial Circuit/City of Ferguson Municipal Division	April 2017
2017-036	Taney County Collector and Property Tax System	May 2017
2017-042	Webster County	June 2017
2017-044	Livingston County	June 2017
2017-046	Barton County	June 2017
2017-049	Bates County	June 2017
2017-056	Shelby County	June 2017