PREPARING FOR A LEGISLATIVE AUDIT

ARKANSAS LEGISLATIVE AUDIT

January 21, 2025

TABLE OF CONTENTS

Kevin William White, CPA, JD
Legislative Auditor
kevin.white@arklegaudit.gov

Joe Archer, CPA
Deputy Legislative Auditor
joseph.archer@arklegaudit.gov

Candice Gasaway, CPA
Audit Manager
candice.gasaway@arklegaudit.gov

Field Audit Supervisors by District:

District 1:

Lance Woodworth, CPA
Field Audit Supervisor (Harrison)
(501) 683-8600 Ext. 1054
lance.woodworth@arklegaudit.gov

District 2:

Christy Chrisman, CPA
Field Audit Supervisor (Waldron)
(501) 683-8600 Ext. 4421
christy.young@arklegaudit.gov

District 4:

Stacie Dearen, CPA
Field Audit Supervisor (Little Rock)
(501) 683-8600 Ext. 4308
stacie.dearen@arklegaudit.gov

Kristin Schmeckenbecher, CPA
Field Audit Supervisor (Little Rock)
(501) 683-8600 Ext. 4306
kristin.schmeckenbecher@arklegaudit.gov

District 5:

Duane Bowden, CPA
Field Audit Supervisor (Nashville)
(501) 683-8600 Ext. 4603
duane.bowden@arklegaudit.gov

Beth Gray, CPA
Field Audit Supervisor (Malvern)
(501) 683-8600 Ext. 4310
beth.gray@arklegaudit.gov

District 6:

Joy Johnson, CPA
Field Audit Supervisor (Monticello)
(501) 683-8600 Ext. 4621
joy.johnson@arklegaudit.gov

Paul McEachern, CPA
Field Audit Supervisor (Monticello)
(501) 683-8600 Ext. 1070
paul.mceachern@arklegaudit.gov

District 7:

Wade Townsend, CPA
Field Audit Supervisor (Hope)
(501) 683-8600 Ext. 4646
wade.townsend@arklegaudit.gov

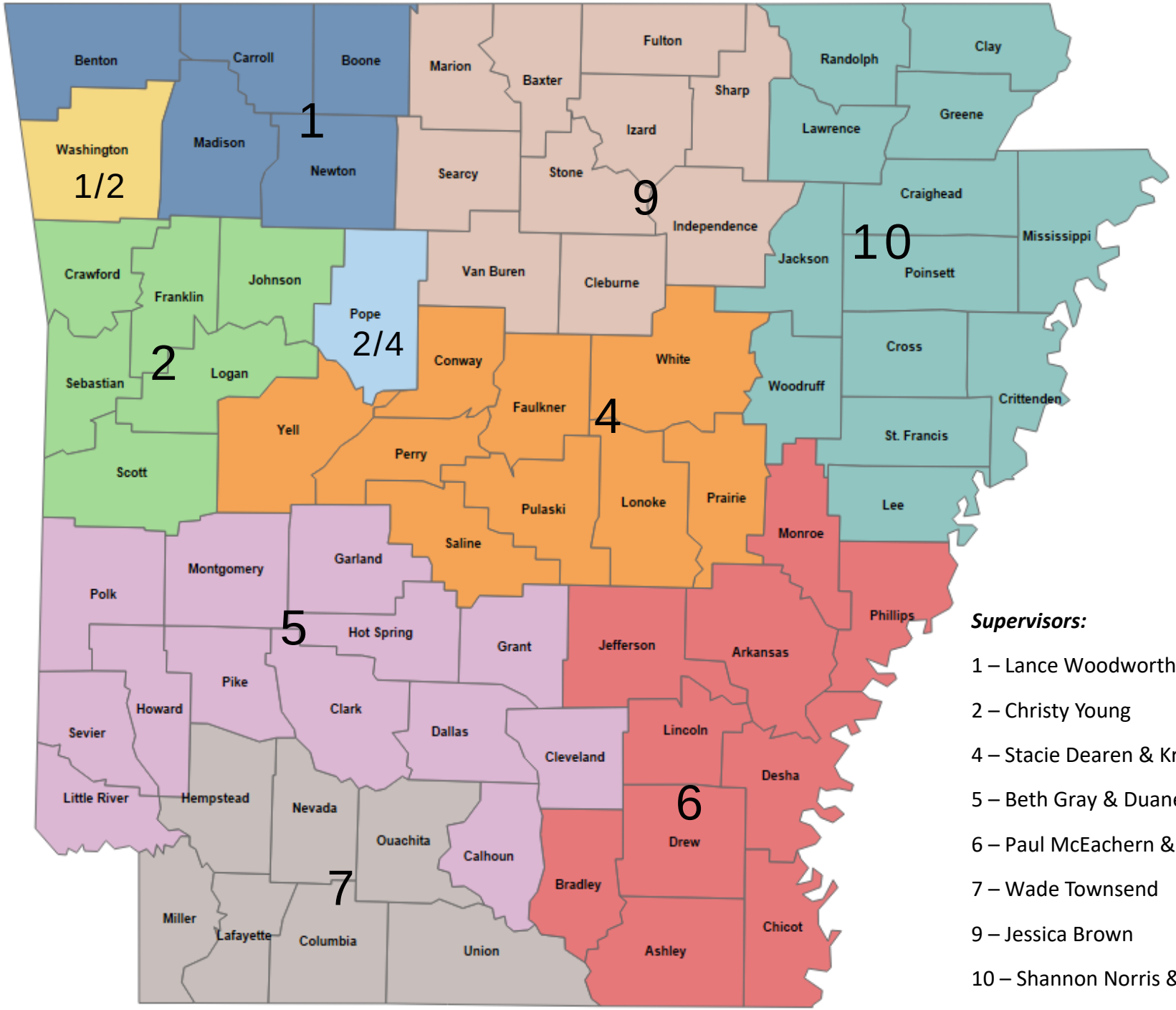
District 9:

Jessica Brown, CPA
Field Audit Supervisor (Batesville)
(501) 683-8600 Ext. 4503
jessica.brown@arklegaudit.gov

District 10:

Jeff McMillin, CPA, CFF
Field Audit Supervisor (Jonesboro)
(501) 683-8600 Ext. 4518
jeff.mcmillin@arklegaudit.gov

Shannon Norris, CPA
Field Audit Supervisor (Jonesboro)
(501) 683-8600 Ext. 1061
shannon.norris@arklegaudit.gov



Supervisors:

1 – Lance Woodworth

2 – Christy Young

4 – Stacie Dearen & Kristin Schmeckenbeker

5 – Beth Gray & Duane Bowden

6 – Paul McEachern & Joy Johnson

7 – Wade Townsend

9 – Jessica Brown

10 – Shannon Norris & Jeff McMillin

LEGISLATIVE JOINT AUDITING COMMITTEE

The Legislative Joint Auditing Committee is responsible for the independent auditing of entities and political subdivisions of the State to furnish the General Assembly with information vital to the discharge of its constitutional duties. When the General Assembly is not in session, the full Committee meets on the second Friday of each month, with the three Standing Committees meeting on the preceding Thursday. For the purpose of reviewing audit reports, members of the Committee are assigned to the Standing Committee on State Agencies, the Standing Committee on Educational Institutions, and the Standing Committee on Counties and Municipalities.

The Legislative Joint Auditing Committee is made up of 44 members as follows:

- 16 Members selected by the Senate
- 20 Members selected by the House of Representatives
- President Tempore of the Senate, ex-officio
- Speaker of the House of Representatives, ex-officio
- Immediate past Co-Chairs of the Committee, ex-officio
- Co-Chairs and Co-Vice Chairs of the Legislative Council, ex-officio

2025-26 Co-Chairs – Senator Jim Petty and Representative Robin Lundstrum

2025-26 Co-Vice Chairs – Senator Jim Dotson and Representative RJ Hawk

ARKANSAS LEGISLATIVE AUDIT

The mission of Arkansas Legislative Audit is to serve the General Assembly, the Legislative Joint Auditing Committee, and the citizens of the State of Arkansas by promoting sound financial management and accountability of public resources entrusted to various governmental entities. To assist the Legislature in oversight of state and local government, Arkansas Legislative Audit is responsible for over 1,000 engagements, including audits, financial and compliance reports, and special reports. Arkansas Legislative Audit continually strives to promote an atmosphere of mutual trust, honesty, and integrity among its staff members, various governmental entities, and the people it is privileged to serve.

Arkansas Legislative Audit currently has 250 professional staff and 11 support staff. As of January 13, 2025 professional staff had achieved the following designations:

- 158 Certified Public Accountants (CPA)
- 37 Certified Fraud Examiners (CFE)
- 5 Certified in Financial Forensics (CFF)
- 9 Certified Information Systems Auditors (CISA)
- 2 Attorneys (JD)

RECORDS NECESSARY FOR AN AUDIT

All funds

Bank statements for entire year plus Jan. & Feb. of succeeding year

Receipt books for entire year plus Jan. & Feb. of succeeding year

Cash receipt and disbursement journals

For manual records:

Total monthly and year to date

Add across and down

For computerized records:

Maintain printout of transaction records every month

Maintain printout of detail general ledger every month

Check stubs or extra copy of check

Deposit books

Receipt ranges should be indicated on each deposit ticket

Investment records

Detail of certificates of deposits, interest rates and renewal dates

Form 1099 interest statements

Bank reconciliations for every month

Paid invoices

Separate by fund and by year

General ledger

Print a general ledger every month and at the end of the year print a detail general ledger

Agency funds

Police bond and fine fund and Court fund

Arrest reports

Court reports

Ticket log

Court dockets

Time payment records

Monthly settlements

Completed ticket books

Records relating to the collection of hot checks

Printer's certificates for ticket books

Detailed listing of pending balances

Payroll fund

Individual payroll records

Quarterly 941 payroll reports, W-2s, W-3, W-4s, 1099s

Time sheets

Monthly federal/state tax remittances

PERS records

Compensated absences listing

Other miscellaneous records

Council minutes up to the present date

Pension Board minutes up to the present date

Six-month financial statements and proofs of publications

Copy of 2 months of the council member packets (to include financial report

Insurance policies

Collateralization documentation, including pledged securities

Lease agreements and other debt agreements

Fixed asset records:

- Description of item
- Cost of item
- Date purchased
- Serial number, if available

Personnel policies

- Vacation & sick leave
- Travel reimbursement

Budgets

Ordinances and resolutions

List of accounts receivable and payable

Franchise fee records

Audit reports of funds performed by other auditors

Act 833 reports (Fire Training and Equipment)

Listing of all credit cards and authorized users

First class cities <u>only</u>

- Mayor's end of the year report
- Quarterly financial reports
- Bids and proofs of publication

BUDGETING LAWS

14-58-201. Annual submission.

On or before December 1 of each year, the mayor of all cities and incorporated towns having the mayor-council form of government shall submit to the governing body of the city or town, for its approval or disapproval, a proposed budget for operation of the city or town from January 1 to December 31 of the forthcoming year.

HISTORY: Acts 1959, No. 28, § 1; 1981, No. 344, § 1; A.S.A. 1947, § 19-4421.

14-58-202. Adoption of budget.

Under this subchapter, the governing body of the municipality shall, on or before February 1 of each year, adopt a budget by ordinance or resolution for operation of the city or town.

HISTORY: Acts 1959, No. 28, § 2; 1981, No. 344, § 2; A.S.A. 1947, § 19-4422; Acts 2011, No. 622, § 1.

14-58-203. Appropriations and changes.

(a) The approval by the municipal governing body of the budget under this subchapter shall, for the purposes of the budget from time to time amount to an appropriation of funds which are lawfully applicable to the items therein contained.

(b) The governing body may alter or revise the budget and unpledged funds appropriated by the governing body for any purpose may be subsequently, by action of the governing body, appropriated to another purpose, subject to the following exceptions:

(1) Funds resulting from taxes levied under statutes or ordinances for specific purposes may not be diverted to another purpose;
(2) Appropriated funds may not be diverted to another purpose where any creditor of the municipality would be prejudiced thereby.

HISTORY: Acts 1959, No. 28, § 3; A.S.A. 1947, § 19-4423.

PUBLISHING REQUIREMENTS LAW

14-55-206. Publishing or posting requirements.

(a)

(1)

(A) All bylaws or ordinances of a general or permanent nature and all those imposing any fine, penalty, or forfeiture shall be published in some newspaper published in the municipality.

(B) In municipalities in which no newspaper is published, written or printed notice posted in five (5) of the most public places designated by the governing body in an ordinance or minutes of the governing body shall be deemed a sufficient publication of any law or ordinance.

(2) It shall be deemed a sufficient defense to any suit or prosecution of such fine, penalty, or forfeiture to show that no notice was given as provided herein.

(b) As to ordinances establishing rules and regulations for zoning, construction of buildings, the installation of plumbing, the installation of electric wiring, or other similar work, where such rules and regulations have been printed as a code in book form, the code or provisions thereof may be published by the municipality by reference to title of the code without further publication or posting thereof. However, no fewer than three (3) copies of the code shall be filed for use and examination by the public in the office of the clerk or recorder of the municipality after the adoption thereof if there is no electronic form of the code available for examination by the public.

HISTORY: Acts 1949, No. 36, § 1; A.S.A. 1947, § 19-2404; Acts 1993, No. 295, § 2; 2009, No. 25, § 1.

SEGREGATION OF DUTIES

CASH/RECEIPTS

a. Mail	1.) One employee opens the mail and 2.) another employee writes the receipts or enters the check or cash collected into a book or journal to be receipted later.
b. Collections	Employee(s) writes the receipts as funds are received.
c. Deposits	Employee prepares and makes the deposit.
d. Reconciles	Employee receives unopened bank statements and reconciles bank balance and deposits with book balance and cash receipts journal.
e. Posts	Employee posts the cash receipts journal.

COMPATIBLE FUNCTIONS

Employee (1)	Employee (2)
a.(1.), c. and e.	**a.(2.), b., d. and e.**

DISBURSEMENTS/ RECEIVING

a. Purchasing	Employee(s) orders goods from vendors.
b. Receiving	Employee(s) receives goods from vendor and documents that the goods have been received by signing and dating the invoice or a receiving report.
c. Processing	Employee prepares the check and verifies the accuracy of the invoice for payment and cosigns the check.
d. Approving	1.) Employee reviews and approves invoices for payment by initialing and dating the invoice. 2.) The approver or another employee cosigns the check and mails the payment.
e. Reconciles	Employee receives unopened bank statements and reconciles bank balance and withdrawals with the book balance and disbursements journal.
f. Posts	Employee posts the cash disbursements journal.

COMPATIBLE FUNCTIONS

Employee (1)	Employee (2)	Employee (3)
a. and c.	**d.**	**b., e., and f.**
a., c., e. and f.	**d.**	**b.**
a., c. and e.	**d. and f.**	**b.**

SEGREGATION OF DUTIES

PAYROLL

a. Individual Personnel Files	Employee has custody of individual personnel files including, but not limited to, W-4's, health ins., and other withholding information and establishes new employees for payroll purposes.
b. Individual Payroll Records	Employee has custody of individual payroll record (name, identification #, pay period, hours, rate of pay, amount, withholdings, etc.)
c. Time Records	Employee(s) prepares time record for work performed for each pay period including time charged for vacation, sick and other leave.
d. Approval	Employee(s) other than the preparer of the time record approves the time record and gives the original to the employee processing payroll.
e. Processing	Employee(s) process payroll from the time and payroll records including calculation of each individual's pay based on these records and prepares the check or information for direct deposit to each individual account.
f. Posts	Employee post payroll to the individual payroll records and to the proper accounts in the cash disbursements journal.
g. Reconciles	Employee reconciles payroll to the appropriate federal and state reports and to the individual payroll records and cash disbursements journal.
h. Payroll Distribution	Payroll employee delivers checks to department supervisor for distribution or payroll employee reviews distribution and direct deposits made to each employees account.

COMPATIBLE FUNCTIONS

PAYROLL			**DEPARTMENT**	
Employee (1)	**Employee (2)**	**Employee (3)**	**Employee (1)**	**Supervisor**
a., b. and f.	**e.**	**g. and h.**	**c.**	**d.**
a., b. and g.	**e.**	**f. and h.**	**c.**	**d.**
a. and b.	**e. and f.**	**h.**	**c.**	**d.**

MUNICIPAL ACCOUNTING LAW

14-59-101. Title.

This chapter shall be known and cited as the "Arkansas Municipal Accounting Law".

HISTORY: Acts 1973, No. 159, § 1; A.S.A. 1947, § 19-5301; Acts 2011, No. 621, § 1.

14-59-102. Applicability.

This chapter shall apply to all funds under the budgetary control of the council or board of directors of the various municipalities of this state, except water and sewer departments.

HISTORY: Acts 1973, No. 159, § 2; A.S.A. 1947, § 19-5302; Acts 2001, No. 1062, § 1.

14-59-103. Exemption for other systems.

(a) In the event any municipality feels its system of bookkeeping is such that it equals or exceeds the basic system prescribed by this chapter, the municipality may request a review by the Legislative Joint Auditing Committee.

(b) Upon the committee's concurrence with these facts, it may issue a certificate to the municipality stating that the municipality's accounting system is of a degree of sophistication such that the basic requirements of this chapter are being met and exempting the municipality from the requirements of the particulars of the system prescribed by this chapter.

HISTORY: Acts 1973, No. 159, § 14; A.S.A. 1947, § 19-5314.

14-59-104. Bank accounts.

(a) All municipalities of this state receiving state aid in the form of either turnback of general revenues or highways revenues shall maintain all funds in depositories approved for such purposes by law.

(b) The municipalities shall maintain separate bank accounts for general funds and street funds.

(c) The accounts shall be maintained in the name of the municipality.

HISTORY: Acts 1973, No. 159, § 3; A.S.A. 1947, § 19-5303.

14-59-105. Prenumbered checks -- Electronic funds transfers.

(a) All disbursements of municipal funds, except those described in this section and as noted in § 14-59-106, petty cash funds, are to be made by prenumbered checks drawn upon the bank account of that municipality.

(b) The checks shall be of the form normally provided by commercial banking institutions and shall contain as a minimum the following information:

(1) Date of issue;
(2) Check number;
(3) Payee;
(4) Amount; and
(5) Signature of two (2) authorized disbursing officers of the city.

(c) Disbursements of municipal funds used for payment of salaries and wages of municipal officials and employees may be made by electronic funds transfer provided that the municipal employee or official responsible for disbursements maintains a ledger containing at least the:

(1) Name, address, and Social Security number of the employee receiving payment of salary or wages;
(2) Routing number from the bank in which the funds are held;
(3) Account number;
(4) Accounts clearing house trace number pertaining to the transfer;
(5) Date and amount transferred; and
(6) Proof that the employee has been notified of direct deposit of his or her salary or wages by electronic funds transfer.

(d) Disbursements of municipal funds used for payments to federal or state governmental entities may be made by electronic funds transfer.

(e)

(1) Disbursements of municipal funds, other than for payments under subsections (c) and (d) of this section, may be made by electronic funds transfer provided that:
(A) The governing body of the municipality shall establish by ordinance an electronic funds payment system directly into payees' accounts in financial institutions in payment of any account allowed against the municipality;
(B) For purposes of this subsection, municipalities opting for an electronic funds payment system shall establish written policies and procedures to ensure that the electronic funds payment system provides for internal accounting controls and documentation for audit and accounting purposes; and
(C) Each electronic funds payment system established under this subsection shall comply with the information systems best practices approved by the Legislative Joint Auditing Committee before implementation by the municipality.
(2) A single electronic funds payment may contain payments to multiple payees, appropriations, characters, or funds.

(f) A disbursement of municipal funds shall have adequate supporting documentation for the disbursement.

HISTORY: Acts 1973, No. 159, § 5; A.S.A. 1947, § 19-5305; Acts 1997, No. 543, § 1; 2009, No. 316, § 1; 2011, No. 621, § 2; 2019, No. 138, § 2.

14-59-106. Petty cash funds.

(a) Municipalities are permitted to establish petty cash funds, so long as the funds are maintained as set forth in this section.

(b)

(1) The establishment of such a fund must be approved by the city council.
(2)

(A) In establishing such a fund, a check is to be drawn upon the general fund of the municipality payable to "petty cash."
(B) That amount may be maintained in the municipal offices for the handling of small expenditures for items such as postage, light bulbs, delivery fees, etc.

(c)

(1) A paid-out slip is to be prepared for each item of expenditure from the fund and signed by the person receiving the moneys.
(2) These paid-out slips shall be maintained with the petty cash. When the fund becomes depleted, the municipality may then draw another check payable to "petty cash" in an amount which equals the total paid-out slips issued. At that time, the paid-out slips shall be removed from the "petty cash fund," and utilized as invoice support for the check replenishing petty cash.

HISTORY: Acts 1973, No. 159, § 6; A.S.A. 1947, § 19-5306.

14-59-107. Fixed asset records.

(a) The governing body shall adopt a policy defining fixed assets. At a minimum, the policy shall set forth the dollar amount and useful life necessary to qualify as a fixed asset.

(b)

(1) All municipalities shall establish by major category and maintain, as a minimum, a listing of all fixed assets owned by the municipality.
(2) The listing shall be totaled by category with a total for all categories.
(3) The categories of fixed assets shall include the major types, such as:

(A) Land;
(B) Buildings;
(C) Motor vehicles, by department;
(D) Equipment, by department; and
(E) Other assets.

(c) The listing shall contain as a minimum:

(1) Property item number, if used by the municipality;
(2) Brief description;
(3) Serial number, if available;
(4) Date of acquisition; and
(5) Cost of property.

HISTORY: Acts 1973, No. 159, § 7; A.S.A. 1947, § 19-5307; Acts 2001, No. 1062, § 2; 2011, No. 621, § 3.

14-59-108. Reconciliation of bank accounts.

(a)

(1) On a monthly basis, all municipalities shall reconcile their cash receipts and disbursements journals to the amount on deposit in banks.
(2) The reconciliation under subdivision (a)(1) of this section shall be approved by a municipal official or employee, other than the person preparing the reconciliation, as designated by the chief executive officer of the municipality.

(b) The reconciliations should take the following form:

City of .....
Date .....

Amount Per Bank Statement Dated				$ .00
Add:	Deposits in transit (Receipts recorded in Cash Receipts Journal not shown on this bank statement).			
DATE	RECEIPTS NO.	AMOUNT		
			$ .00	
			.00	
			.00	.00
Deduct:	Outstanding Checks (Checks issued and dated prior to date of bank statement per Cash Disbursements Journal not having yet cleared the bank).			
CHECK NO.	PAYEE	AMOUNT		
			$ .00	
			.00	
			.00	.00
RECONCILED BALANCE				$ .00

This reconciled balance shall agree to either the cash balance as shown on the municipality's check stubs running bank balance or the municipality's general ledger cash balance, whichever system the municipality employs.

HISTORY: Acts 1973, No. 159, § 12; A.S.A. 1947, § 19-5312; Acts 2011, No. 621, § 4.

14-59-109. Prenumbered receipts.

(a) All funds received are to be formally receipted at the time of collection or the earliest opportunity by the use of prenumbered receipts or mechanical receipting devices.

(b)

(1) In the use of prenumbered receipts, the following minimum standards shall be met:
(A) If manual receipts are used, receipts are to be prenumbered by the printer and a printer's certificate obtained and retained for audit purposes. The certificate shall state the date printing was done, the numerical sequence of receipts printed, and the name of the printer;
(B) The prenumbered receipts shall contain the following information for each item receipted:

(i) Date;
(ii) Amount of receipt;
(iii) Name of person or company from whom money was received;
(iv) Purpose of payment;
(v) Fund to which receipt is to be credited; and
(vi) Identification of employee receiving money.

(2) If manual receipts are used, the original receipt should be given to the party making payment. One (1) duplicate copy of the receipt shall be maintained in numerical order in the receipt book and made available to the auditors during the course of annual audit. Additional copies of the receipt are optional with the municipality and may be used for any purposes they deem fit.

(c) If an electronic receipting system is used, the system shall be in compliance with the Information Systems Best Practices Checklist provided by the Legislative Joint Auditing Committee.

HISTORY: Acts 1973, No. 159, § 4; A.S.A. 1947, § 19-5304; Acts 2011, No. 621, § 5.

14-59-110. Cash receipts journals.

(a)

(1) Municipalities shall establish a cash receipts journal or an electronic receipts listing that shall indicate:

(A) The receipt number;
(B) The date of the receipt;
(C) The payor;
(D) The amount of the receipt; and
(E) Classification or general ledger account.

(2) The classification of the receipts shall include the major sources of revenue, such as:

(A) State revenues;
(B) Property taxes;
(C) Sales taxes;
(D) Fines, forfeitures, and costs;
(E) Franchise fees;
(F) Transfers in; and
(G) Other.

(b)

(1) All items of receipts shall be posted to and properly classified in the cash receipts journal or electronic receipts listing.

(2)

(A) The journal shall be properly balanced and totaled monthly and on a year-to-date basis.

(B) The journal shall be reconciled monthly to total bank deposits as shown on the municipalities' bank statements.

(3) The electronic receipts listing shall be posted to the general ledger at least monthly. The general ledger shall be reconciled monthly to total bank deposits as shown on the municipalities' bank statements.

HISTORY: Acts 1973, No. 159, § 10; A.S.A. 1947, § 19-5310; Acts 2001, No. 1062, § 3; 2011, No. 621, § 6.

14-59-111. Cash disbursements journals.

(a)

(1) Municipalities shall establish a cash disbursements journal or electronic check register that shall indicate the date, payee, check number or transaction number, amount of each check written or transaction, and classification or general ledger account.
(2) The classifications of expenditures shall include the major type of expenditures by department, such as:

(A) Personal services;
(B) Supplies;
(C) Other services and charges;
(D) Capital outlay;
(E) Debt service; and
(F) Transfers out.

(b)

(1) The cash disbursements journal shall be properly balanced and totaled monthly and on a year-to-date basis.
(2) The cash disbursements journal shall be reconciled monthly to total bank disbursements as indicated on the monthly bank statements.
(3) The electronic check register shall be posted to the general ledger at least monthly. The general ledger shall be reconciled monthly to total bank disbursements as indicated on the monthly bank statements.

HISTORY: Acts 1973, No. 159, § 11; A.S.A. 1947, § 19-5311; Acts 2001, No. 1062, § 4; 2011, No. 621, § 7.

14-59-112, 14-59-113. [Repealed.]

14-59-114. Maintenance and destruction of accounting records.

(a) Accounting records can basically be divided into the following three (3) groups:

(1)

(A) Support Documents. Support documents consist primarily of the following items:

(i) Cancelled checks;
(ii) Invoices;
(iii) Bank statements;
(iv) Receipts;
(v) Deposit slips;

(vi) Bank reconciliations;
(vii) Check book register or listing;
(viii) Receipts listing;
(ix) Monthly financial reports;
(x) Payroll records;
(xi) Budget documents; and
(xii) Bids, quotes, and related documentation.

(B) These records shall be maintained for a period of at least four (4) years and in no event shall be disposed of before being audited for the period in question.

(2)

(A) Semipermanent Records. Semipermanent records consist of:

(i) Fixed assets and equipment detail records;
(ii) Investment and certificate of deposit records;
(iii) Journals, ledgers, and subsidiary ledgers; and
(iv) Annual financial reports.

(B)

(i) These records shall be maintained for a period of not less than seven (7) years and in no event shall be disposed of before being audited for the period in question.
(ii) For investment and certificate of deposit records, the seven (7) years of required maintenance begins on the date of maturity.

(3)

(A) Permanent Records. Permanent records consist of:

(i) City or town council minutes;
(ii) Ordinances;
(iii) Resolutions;
(iv) Employee retirement documents; and
(v) Annual financial audits.

(B) These records shall be maintained permanently.

(b) When documents are destroyed, the municipality shall document the destruction by the following procedure:

(1)

(A) An affidavit is to be prepared stating which documents are being destroyed and to which period of time they apply, indicating the method of destruction;
(B) This affidavit is to be signed by the municipal employee performing the destruction and one (1) council member.

(2)

(A) In addition, the approval of the council for destruction of documents shall be obtained, and an appropriate note of the approval indicated in the council minutes

along with the destruction affidavit;
(B) This council approval shall be obtained before the destruction.

HISTORY: Acts 1973, No. 159, § 15; 1979, No. 616, § 2; A.S.A. 1947, § 19-5315; Acts 2011, No. 621, § 8.

14-59-115. Duties of municipal treasurer.

(a) Each municipal treasurer of this state or the designated representative that has been approved by the governing body shall submit a monthly financial report to the council or board of directors.

(b)

(1) Municipal treasurers shall maintain the accounting records prescribed in this chapter.
(2)

(A)

(i) If the municipal treasurer does not comply with this chapter or requests that specific duties be assigned to another employee or contracting entity, the governing body of a municipality may assign specific duties outlined in this chapter to another employee, or it may contract for the services to be performed by a private, qualified person or entity.
(ii)

(a)

(1) Before the governing body of a municipality assigns or contracts with a person or entity for the disbursing of funds, the governing body of a municipality shall establish by ordinance a method that provides for internal accounting controls and documentation for audit and accounting purposes.
(2) The municipal treasurer shall approve the disbursement of funds before the private, qualified person or entity disburses the funds.

(b) The governing body of a municipality shall ensure that the person or entity is adequately insured and bonded and conforms to best practices and standards in the industry.

(B)

(i) The governing body of a municipality may not assign duties relating to the collecting of funds to anyone other than an employee of the municipality.
(ii) The governing body of a municipality may assign or contract with a private, qualified person or entity for the duties relating to the disbursing of funds for payroll, bonded debt, or construction projects funded with bond proceeds.

HISTORY: Acts 1973, No. 159, § 13; A.S.A. 1947, § 19-5313; Acts 2001, No. 1062, § 5; 2011, No. 621, § 9; 2015, No. 582, § 1.

14-59-116. Annual publication of financial statement.

(a)

(1) The governing body of each municipality shall publish annually a financial statement of the municipality, including receipts and expenditures for the period and a statement of the indebtedness and financial condition of the municipality. The financial statement shall be published one (1) time in a newspaper published in the municipality.
(2) This financial statement shall be at least as detailed as the minimum record of accounts as provided in this chapter.
(3) This financial statement shall be published by April 1 of the following year.

(b) In municipalities in which no newspaper is published, the financial statement shall be posted in two (2) of the most public places in the municipality.

HISTORY: Acts 1973, No. 159, §§ 18, 19, as added by 1977, No. 308, § 1; A.S.A. 1947, §§ 19-5316, 19-5317; Acts 2011, No. 621, § 10.

14-59-117. Withholding of turnback for noncompliance.

(a)

(1) If Arkansas Legislative Audit determines that a municipal treasurer is not substantially complying with this chapter, Arkansas Legislative Audit shall report the findings to the Legislative Joint Auditing Committee.
(2)

(A) If a public official or a private accountant determines that a municipal treasurer is not substantially complying with this chapter, the official or accountant shall notify the Legislative Joint Auditing Committee of his or her findings.
(B) Upon notification, the Legislative Joint Auditing Committee shall direct Arkansas Legislative Audit to confirm that the municipal treasurer is not substantially complying with this chapter.
(C) Upon confirmation, Arkansas Legislative Audit shall report the findings to the Legislative Joint Auditing Committee.

(b)

(1) Upon notification of noncompliance by Arkansas Legislative Audit, the Legislative Joint Auditing Committee shall notify in writing the mayor and the city council or town council that the municipality's accounting records do not substantially comply with this chapter.
(2) The municipality has sixty (60) days after the date of notification to bring the accounting records into substantial compliance with this chapter.
(3)

(A) After the sixty (60) days allowed for compliance or upon request by the appropriate municipal officials, Arkansas Legislative Audit shall review the records to determine if the municipality substantially complies with this chapter.
(B) Arkansas Legislative Audit shall report its findings to the Legislative Joint

Auditing Committee.

(c)

(1)

(A) If the municipality has not achieved substantial compliance within the sixty-day period, the Legislative Joint Auditing Committee may report the noncompliance to the Treasurer of State.

(B) Upon receipt of the notice of noncompliance from the Legislative Joint Auditing Committee, the Treasurer of State shall place fifty percent (50%) of the municipality's turnback in escrow until the Legislative Joint Auditing Committee reports to the Treasurer of State that the municipality has substantially complied with this chapter.

(2) If the municipality has not achieved substantial compliance within the sixty-day period, the governing body of the municipality shall assign specific duties outlined in this chapter to another employee or shall contract for the services to be performed by a qualified person or entity.

(3)

(A) Arkansas Legislative Audit shall notify the Legislative Joint Auditing Committee when the municipality has substantially complied with this chapter.

(B)

(i) The Legislative Joint Auditing Committee shall notify the Treasurer of State that the municipality has substantially complied with this chapter.

(ii) Upon notice of compliance from the Legislative Joint Auditing Committee, the Treasurer of State shall remit all turnback due to the municipality.

(d)

(1) If Arkansas Legislative Audit has not received a request for a review of the records from the municipality before the end of the one-hundred-twenty-day period after the first date of notification of noncompliance, the Legislative Joint Auditing Committee may notify the municipality and the Treasurer of State of the continued noncompliance.

(2) Upon notice by the Legislative Joint Auditing Committee, the Treasurer of State shall withhold all turnback until such time that the accounting records have been reviewed and determined by Arkansas Legislative Audit to be in substantial compliance with this chapter.

(e)

(1) If Arkansas Legislative Audit has not received a request for a review of the records from the municipality before the end of six (6) months after the initial notification of noncompliance, the Legislative Joint Auditing Committee may notify the municipality and the Treasurer of State of the continued noncompliance.

(2) Upon notice of noncompliance for six (6) months, the municipality forfeits all escrowed funds, and the Treasurer of State shall redistribute all escrowed turnback funds applicable to the municipality among all other municipalities receiving turnback.

(3) The municipality shall not be eligible to receive any additional turnback from the state until the Legislative Joint Auditing Committee notifies the Treasurer of State that the municipality has substantially complied with this chapter.

HISTORY: Acts 2001, No. 1062, § 6; 2009, No. 288, § 1.

14-59-118. Penalty.

(a) Any municipal treasurer who refuses or neglects to maintain the books and records provided in this chapter shall be deemed guilty of malfeasance.

(b) Upon conviction in circuit court, the treasurer shall be fined in any sum not less than one hundred dollars ($100) nor more than one thousand dollars ($1,000) and shall be removed from office.

HISTORY: Acts 2001, No. 1062, § 7.

14-59-119 Debit card and credit card payments.

(a) A municipality may accept a legal payment and any associated costs through a debit card or credit card in accordance with applicable state and federal law.

(b)

(1) A municipality may enter into a contract with a credit card or debit card company and pay any fee normally charged by the credit card or debit card company for allowing the municipality to accept the credit card or debit card as payment as authorized under subsection (a) of this section.

(2) When a payment is made through a credit card or debit card, the municipality shall assess a transaction fee equal to the amount charged to the municipality by the credit card or debit card company.

(3) A municipality shall not assess a transaction fee for payments made through a credit card or debit card if the governing body of the municipality determines that the transaction fee is included in the amount charged for the service or product for which a credit card or debit card payment is made.

HISTORY: Acts 2019, Nos. 195, § 1; 773, § 1.

MUNICIPAL ETHICS LAW

14-42-107. Interest in offices or contracts prohibited.

(a)

(1) A council member or elected official of a municipal corporation, during the term for which he or she has been elected or one (1) year thereafter, shall not be appointed to any municipal office that was created or the emoluments of which have been increased during the time for which he or she has been elected except to fill a vacancy in the office of mayor, council member, clerk, clerk-treasurer, recorder, or recorder-treasurer.
(2) A council member shall not be appointed to any municipal office, except in cases provided for in this subtitle, during the time for which he or she may have been elected.

(b)

(1) A council member, official, or municipal employee shall not be interested, directly or indirectly, in the profits of any contract for furnishing supplies, equipment, or services to the municipality unless the governing body of the city has enacted an ordinance specifically permitting council members, officials, or municipal employees to conduct business with the city and prescribing the extent of this authority.
(2) The prohibition prescribed in this subsection does not apply to contracts for furnishing supplies, equipment, or services to be performed for a municipality by a corporation in which no council member, official, or municipal employee holds any executive or managerial office or by a corporation in which a controlling interest is held by stockholders who are not council members.

HISTORY: Acts 1875, No. 1, § 86, p. 1; C. & M. Dig., § 7520; Pope's Dig., § 9580; Acts 1963, No. 182, § 1; 1981, No. 485, § 1; A.S.A. 1947, § 19-909; Acts 2003, No. 1299, § 1; 2009, No. 403, § 1; 2017, No. 879, § 11.

CHECK IMAGING LAWS

19-2-501. Purpose.

The State of Arkansas and its political subdivisions have the responsibility to properly account for all financial transactions. In order to help fulfill this responsibility, the State of Arkansas and other public entities are required to maintain books and records of transactions. The State of Arkansas and its political subdivisions recognize that through the use of computers and electronic data, banking and the flow of information are continuing to change. With this change, it is important that the State of Arkansas and its political subdivisions continue to receive evidentiary information concerning financial transactions. The purpose of this subchapter is to permit public entities to accept photographic copies or digital images of financial transactions and to require financial institutions to furnish the needed documentation in a readable, meaningful, permanent format.

HISTORY: Acts 1999, No. 648, § 1.

19-2-502. Definition.

As used in this subchapter, "public entity" means state agencies, including all constitutional offices and agencies, boards, and commissions, state institutions of higher education, municipalities, counties, school districts, education service cooperatives, improvement districts, and other public officials or public offices. Public entities shall maintain records of all transactions with financial institutions.

HISTORY: Acts 1999, No. 648, § 2; 2007, No. 617, § 39.

19-2-503. Eligibility to accept public funds.

In order for a financial institution to be eligible to be a depository of public funds, the financial institution must furnish the public entity documentation, as required in this subchapter, of transactions with or through that institution.

HISTORY: Acts 1999, No. 648, § 3.

19-2-504. Transaction summaries.

On a monthly basis, financial institutions shall furnish public entities with statements summarizing all transactions of the public entity. Unless the public entity and the financial institution have a written agreement to receive digital images or copies in compliance with the provisions of this subchapter, the financial institutions shall return all original canceled checks to the public entity along with the transaction summary or statement.

HISTORY: Acts 1999, No. 648, § 4.

19-2-505. Approval by Arkansas Legislative Audit.

(a) A financial institution desiring to provide public entities with images of canceled checks as provided in this subchapter shall provide a sample of imaged documents in one (1) or more of the following formats to Arkansas Legislative Audit for review.

(1) Stored on a CD-ROM or similar tangible digital media;

(2) Accessible through the internet; or

(3) On paper.

(b) Upon receipt of imaged documents submitted under subsection (a) of this section, Arkansas Legislative Audit shall immediately review and notify the financial institution whether or not the imaged documents are in compliance with this subchapter.

HISTORY: Acts 1999, No. 648, § 5; 2019 No. 255, § 1.

19-2-506. Digital images or copies of documentation.

(a) After a financial institution has received written notification from Arkansas Legislative Audit that the submitted samples of its imaged documents under § 19-2-505 comply with this subchapter and upon agreement with the public entity, the financial institution may provide the public entity canceled check images in the format and quality approved by Arkansas Legislative Audit.

(b) The canceled check images of financial transactions provided to the public entity by the financial institution under this subchapter shall be legible and show both the front and back images of the canceled checks.

(c)

(1) If a financial institution provides canceled check images on tangible digital media under this subchapter, the images shall be provided on a read-only CD-ROM or other agreed upon digital media that would provide a permanent and tamper-proof record.

(2)

(A) If particular software is needed to view or search the digital images provided under this subchapter, the financial institution shall provide the software to the public entity and, upon request, to Arkansas Legislative Audit.

(B) Software provided under subdivision (c)(2)(A) of this section shall make canceled check images clear and readable.

(3) Before delivery of a CD-ROM or other tangible digital media to a public entity, a financial institution shall perform random verification of the legibility of the contents of the data.

(d)

(1) If a financial institution provides canceled check images to a public entity through internet access to online banking documents under this subchapter, the financial

institution may provide Arkansas Legislative Audit read-only internet access to the public entity's online banking documents.

(2) Read-only internet access granted under subdivision (d)(1) of this section shall permit viewing and copying of each public entity's bank statements, canceled check images, deposit slips, and other financial transaction documentation made available to the public entity.

(3)

(A) If particular software is needed to view or search images made available under this subsection, the financial institution shall provide the necessary software to the public entity and, upon request, to Arkansas Legislative Audit.

(B) Software provided under subdivision (d)(3)(A) of this section shall make canceled check images clear and readable.

(4) An online banking document made available to a public entity under this subsection shall be available for read-only internet access for at least five (5) years after the document is made available to the public entity online.

(e) If a financial institution provides canceled check images on paper under this subchapter, the images shall be of such clarity and size that the details may be read without the aid of a magnifying device.

(f)

(1) If a financial institution provides canceled check images under this subchapter, the financial institution shall implement one (1) of the following procedures to provide verification of the authenticity of the records retained by the public entity:

(A) A duplicate copy of the check images on paper and statements mailed to Arkansas Legislative Audit on a monthly basis;
(B) The use of an identifying mark unique to the financial institution on the paper images of checks sent to the public entity;
(C) The delivery of a duplicate copy of the check images stored on tangible digital media, conforming to the digital imaging specifications stated in this subchapter, to Arkansas Legislative Audit on a monthly basis;
(D) The provision to Arkansas Legislative Audit of read-only internet access to the public entity's online banking documents in accordance with the requirements of this subchapter; or
(E) Any other authenticating method approved by Arkansas Legislative Audit.

(2) A financial institution may elect which of the procedures listed in subdivision (f)(1) of this section it shall implement to provide authentication of images relating to the accounts of each public entity.

(g) A financial institution shall be able to, and, at the request of Arkansas Legislative Audit, shall provide duplicate copies of any checks and statements delivered to a public entity:

(1) With the same clarity and size as the imaged documents previously delivered; and
(2) In the format requested by Arkansas Legislative Audit if the format is currently available to the financial institution.

HISTORY: Acts 1999, No. 648, § 6; 2019 No. 255, § 1.

19-2-507. Request of records by Legislative Auditor.

(a) Upon request by the Legislative Auditor, a financial institution shall provide a copy of a public entity's financial information directly to Arkansas Legislative Audit staff without delay or approval from the public entity.

(b) The financial institutions may provide the digital transaction statements and digital canceled check images to Arkansas Legislative Audit in a media format allowed under the provisions of this subchapter for public entities or other media mutually agreed upon by the financial institution and Arkansas Legislative Audit.

(c) No bank shall be liable for making available to Arkansas Legislative Audit staff any of the information required under the provisions of this subchapter.

(d) Any cost associated with providing this information to Arkansas Legislative Audit shall be borne by the public entity being audited or investigated.

HISTORY: Acts 1999, No. 648, § 7.

19-2-508. [Repealed.]

19-2-509. Effect on other laws.

The provisions of this subchapter do not change, amend, or repeal any laws or rules regarding a financial institution's normal obligations and responsibilities to maintain customer financial records.

HISTORY: Acts 1999, No. 648, § 9; 2019, No. 315, § 1702.

PURCHASING LAWS

14-58-303. Purchases and contracts generally.

(a) In a city of the first class, city of the second class, or incorporated town, the mayor or the mayor's duly authorized representative shall have exclusive power and responsibility to make purchases of all supplies, apparatus, equipment, materials, and other things requisite for public purposes in and for the city and to make all necessary contracts for work or labor to be done or material or other necessary things to be furnished for the benefit of the city, or in carrying out any work or undertaking of a public nature in the city.

(b)

(1)

(A) Except as provided under § 14-58-104, the governing body of any city of the first class shall provide by ordinance the procedure for making all purchases that do not exceed the sum of thirty-five thousand dollars ($35,000)(as of January 1,2025, $42,921).
(B) Except as provided under § 14-58-104, the governing body of any city of the second class or incorporated town may provide by ordinance the procedure for making all purchases.

(2)

(A)

(i) Except as provided under § 14-58-104, in a city of the first class in which the amount of expenditure for any purpose or contract exceeds the sum of thirty-five thousand dollars ($35,000))(as of January 1,2025, $42,921), the mayor or the mayor's authorized representative shall invite competitive bidding on the purpose or contract by legal advertisement in any local newspaper.
(ii) Bids received pursuant to the advertisement shall be opened and read on the date set for receiving the bids in the presence of the mayor or the mayor's authorized representative.
(iii) The mayor or the mayor's authorized representative has exclusive power to award the bid to the lowest responsible bidder, subject to the provisions in subdivision (b)(2)(A)(iv) of this section, and may reject any and all bids received.
(iv) For the purchase of supplies, apparatus, equipment, materials, and other items under subdivision (b)(2), the city may base its award on the following method of evaluation if notice of the method of evaluation is stated in the bid notice:

(a) The lowest immediate cost;
(b) The lowest demonstrated life cycle cost;
(c) The lowest demonstrated term costs; or
(d) A combination of two (2) or more of the lowest immediate cost, the lowest demonstrated life cycle cost, and the lowest demonstrated term cost.

(v) A bid, quote, and the documentation related to a bid or quote shall be maintained as required under § 14-59-114(a)(1).

(B) The governing body by resolution may waive the requirements of competitive bidding in exceptional situations where this procedure is deemed not feasible or practical or as provided under § 14-58-104.
(C) Cities of the first class, cities of the second class, and incorporated towns may accept competitive bids in the following forms:

(i) Written; or
(ii) Electronic media.

(3)

(A) Beginning January 1, 2025, and on each January 1 at subsequent five-year intervals, the amounts under this subdivision shall be adjusted to reflect the percentage increase in the Consumer Price Index for All Urban Consumers or it successor, as published by the United States Department of Labor for the five (5) years immediately preceding the percentage increase, and rounded to the nearest whole number.
(B) Following a percentage increase under subdivision (c)(1) of this sections, the Department of Finance and Administration shall provide each city of the first class and Arkansas Legislative Audit with the percentage increase and the corresponding updated amounts under this section.

(c)

(1) In a city of the first class, a city of the second class, or an incorporated town, the governing body by ordinance shall have the option to make purchases by participation in a reverse Internet auction, except that purchases and contracts for construction projects and materials shall be undertaken pursuant to subsections (a) and (b) of this section and § 22-9-203.
(2) The ordinance shall include, but is not limited to, the following procedures:

(A) Bidders shall be provided instructions and individually secured passwords for access to the reverse Internet auction by either the city or the town, or the reverse Internet auction vendor;
(B) The bidding process shall be timed, and the time shall be part of the reverse Internet auction specifications;
(C) The reverse Internet auction shall be held at a specific date and time;
(D) The reverse Internet auction and bidding process shall be interactive, with each bidder able to make multiple bids during the allotted time;
(E) Each bidder shall be continually signaled his or her relative position in the bidding process;
(F) Bidders shall remain anonymous and shall not have access to other bidders or bids; and
(G) The governing body shall have access to real-time data, including all bids and bid amounts.

(3) The governing body may create by an additional ordinance reverse Internet auction specifications for the anticipated purchase of a specific item or purchase.
(4)

(A) The governing body is authorized to pay a reasonable fee to the reverse Internet auction vendor.

(B) The fee may be included as part of the bids received during the reverse Internet auction and paid by the winning bidder or paid separately by the governing body.

(5) The governing body retains the right to:

(A) Refuse all bids made during the reverse Internet auction; and

(B) Begin the reverse Internet auction process anew if the governing body determines it is in the best interest of the city or town.

(d) As Used this section:

(1) "Lowest demonstrated life cycle cost" means the cost of an asset as determined by the mayor or the mayor's authorized representative to be credibly established by a bidder over the life cycle of the asset, taking into consideration the asset's initial capital costs, maintenance costs, operating costs, and residual value at the end of the life of the asset;

(2) "Lowest demonstrated term cost" means the cost of an asset as determined by the mayor or the mayor's authorized representative to be credibly established by a bidder over a portion of the life cycle of the asset, taking into consideration the asset's initial capital costs, maintenance costs, and operating costs during the portion of the life cycle of the asset;

(3) "Lowest responsible bidder" means the bidder who offers trustworthiness and responsibility concerning the subject purchase and whose bid offers the lowest cost to the city under subdivision (b)(2)(A) of this section;

(4) "Reverse Internet auction" means an Internet-based process in which bidders:

(A) Are given specifications for items and services being sought for purchase by a municipality; and

(B) Bid against one another in order to lower the price of the item or service to the lowest possible level; and

(5) "Reverse Internet auction vendor" means an Internet-based entity that hosts a reverse Internet auction.

HISTORY: Acts 1959, No. 28, § 5; 1979, No. 154, § 1; 1985, No. 745, § 3; A.S.A. 1947, § 19-4425; Acts 1995, No. 812, § 1; 2001, No. 508, § 1; 2005, No. 1435, § 2; 2005, No. 1957, § 1; 2009, No. 756, § 24; 2017, No. 170, § 2; 2021, No. 435, § 5; 2023, No. 208, §§ 1,2.

14-58-305. Payment of claims.

(a) In a city of the first class, city of the second class, or incorporated town, the mayor or his or her duly authorized representative may approve or disapprove for payment out of funds previously appropriated for that purpose, any legal claims asserted or brought against the city or town.

(b) The municipal governing body shall, by ordinance, establish in that connection a maximum amount, and the payment or disapproval of such bills, debts, or liabilities exceeding that amount shall require the confirmation of the governing body.

HISTORY: Acts 1959, No. 28, § 6; A.S.A. 1947, § 19-4426; 2021, No. 435, § 7.

Ark. Const. Art. 12, § 5 (2017)

§ 5. Political subdivisions not to become stockholders in or lend credit to private corporations -- Exceptions.

(a) No county, city, town or other municipal corporation, shall become a stockholder in any company, association, or corporation; or obtain or appropriate money for, or loan its credit to, any corporation, association, institution or individual.

(b) However, a county, city, town, or other municipal corporation may obtain or appropriate money for a corporation, association, institution, or individual to:

(1) Finance economic development projects; or
(2) Provide economic development services.

(c) As used in this section:

(1) "Economic development projects" means the land, buildings, furnishings, equipment, facilities, infrastructure, and improvements that are required or suitable for the development, retention, or expansion of:

(A) Manufacturing, production, and industrial facilities;
(B) Research, technology, and development facilities;
(C) Recycling facilities;
(D) Distribution centers;
(E) Call centers;
(F) Warehouse facilities;
(G) Job training facilities; and
(H) Regional or national corporate headquarters facilities;

(2) "Economic development services" means:

(A) Planning, marketing, and strategic advice and counsel regarding job recruitment, job development, job retention, and job expansion;
(B) Supervision and operation of industrial parks or other such properties; and
(C) Negotiation of contracts for the sale or lease of industrial parks or other such properties; and

(3) "Infrastructure" means:

(A) Land acquisition;
(B) Site preparation;
(C) Road and highway improvements;
(D) Rail spur, railroad, and railport construction;
(E) Water service;
(F) Wastewater treatment;
(G) Employee training which may include equipment for such purpose; and
(H) Environmental mitigation or reclamation.

(d) The General Assembly, by a three-fourths vote of each house, may amend the provisions of subsections (b) and (c) of this section so long as the amendments are germane to this section and consistent with its policy and purposes. [As amended by Const. Amend. 97.]

PURCHASE AND SALE OF REAL AND PERSONAL PROPERTY

14-54-302. Purchase, lease, and sale authorized.

(a) A municipality may:

(1) Sell, convey, lease, rent, let or dispose of any real estate or personal property owned or controlled by the municipality, including real estate or personal property that is held by the municipality for public or governmental purposes;
(2) Buy any real estate or personal property; and
(3)

(A) Donate real estate or personal property, or any part of the real estate or personal property, to the United States Government or any agency of the United States Government, for any one (1) or more of the following purposes, that is, having the real estate or personal property, or both, activated, reactivated, improved, or enlarged by the donee.
(B) The municipality may donate the fee simple title and absolute interest, without any reservations or restrictions, in and to all real estate or personal property, or both, or any part of the real estate or personal property, to the United States Government, if this real estate or personal property was previously conveyed or otherwise transferred by the United States Government to the municipality without cost to the municipality.
(C) All other donation instruments shall contain provisions by which the title to the property donated shall revert to the municipality when the donated property is no longer used by the donee for the purposes for which it was donated.

(b) The execution of all contracts and conveyances and lease contracts shall be performed by the mayor and city clerk or recorder, when authorized by a resolution in writing and approved by a majority vote of the governing body of the municipality present and participating.

(c) The mayor or his or her authorized representative may sell or exchange any municipal personal property with a value of twenty thousand dollars ($20,000) or less, unless the governing body of the municipality shall by ordinance establish a lesser amount.

(d) Municipal personal property to be disposed of as one (1) unit shall not be sold without competitive bidding if the amount exceeds twenty thousand dollars ($20,000) or the maximum provided by resolution, unless the mayor certifies in writing to the governing body of the municipality that in his or her opinion the fair market value of the item or lot is less than the amount established by ordinance.

(e)

(1) If personal property of the municipality becomes obsolete or is no longer used by a municipality, the personal property may be:

(A) Sold at public or Internet auction;
(B) Sent to the Marketing and Redistribution Section of the Office of State Procurement of the Department of Finance and Administration;

(C) Transferred to another governmental entity within the state; or
(D) Donated under this section.

(2) If an item of personal property is not disposed of under subdivision (e)(1) of this section, the item may be disposed of in the landfill used by the municipality if the mayor or his or her authorized representative certifies in writing and the governing body of the municipality approves that:

(A) The item has been rendered worthless by damage or prolonged use; or
(B) The item has:

(i) Only residual value; and
(ii) Been through public auction and not sold.

(f)

(1) A record shall be maintained of all items of personal property disposed of under this section and reported to the governing body of the municipality.
(2) The municipal fixed asset listing shall be amended to reflect all disposal of real estate and personal property made under this section.

HISTORY: Acts 1935, No. 176, § 2; Pope's Dig., § 9539; Acts 1953, No. 13, § 1; 1959, No. 159, § 1; 1977, No. 823, § 1; 1983, No. 183, § 2; A.S.A. 1947, § 19-2310; Acts 2005, No. 436, § 1; 2017, No. 470, § 1; 2019, No. 575, § 1.

ARKANSAS SPEED TRAP LAW

12-8-402. Definitions.

As used in this subchapter:

(1) "Abusing police power" means exercising police power to enforce criminal and traffic laws for the principal purpose of raising revenue for an affected municipality and not for the purpose of public safety and welfare;

(2) "Affected highway" means a highway which:

(A) Is part of the state highway system; and

(B) Has a decrease in the posted speed limit upon entering an affected municipality;

(3) "Affected municipality" means a city of the first class, a city of the second class, or an incorporated town through which passes an affected highway;

(4) "Enterprise fund" means a proprietary fund type used to report an activity for which a fee is charged to external users for goods or services;

(5) "Fiduciary fund" means a fund type used to report assets held in a trustee or agency capacity and which cannot be used to support an affected municipality's own programs; and

(6)(A) "Revenue" means moneys resulting from fines and costs from traffic offense citations written by or arrests made by an affected municipality's law enforcement agency, if the traffic offense is a:

(i) Misdemeanor;

(ii) Violation of state law; or

(iii) Violation of a local ordinance.

(B) "Revenue" does not include moneys:

(i) Received by an affected municipality and remitted to another governmental entity;

(ii) Resulting from ancillary actions related to the enforcement of a traffic offense, including failure to appear and failure to pay;

(iii) Resulting from late fees assessed on any traffic offense citation; or

(iv) Received from a traffic offense citation written by or an arrest made by a law enforcement officer who does not belong to the affected municipality's law enforcement agency as required under subdivision (6)(A) of this section, including without limitation a law enforcement officer who is a county sheriff, a constable, or employed by:

(a) A county sheriff's office;

(b) The Division of Arkansas State Police; or

(c) The Arkansas Highway Police Division of the Arkansas Department of Transportation.

HISTORY: Acts 1995, No. 855, § 2; 1997, No. 211, § 1; 2019, No. 364, § 1; 2023, No. 825, §§ 1, 2.

12-8-403. Inquiry to determine abuse.

(a)(1) Upon the request of the prosecuting attorney of a judicial district in which an affected municipality is located, the Director of the Department of Arkansas State Police may investigate and determine whether the affected municipality is abusing police power by conducting an unlawful speed trap.

(2)(A) The investigation shall require the affected municipality to submit a certified record of all fines, costs, citations, and municipal expenditures, as well as the percentage of speeding citations that are written for persons speeding ten miles per hour (10 m.p.h.) or less than the posted speed limit.

(B) The records required under subdivision (a)(2)(A) of this section may encompass a reasonable time period as requested by the Department of State Police but shall contain at least ninety (90) days' worth of documentation.

(C)(i) The affected municipality shall submit the requested records within thirty (30) days, unless an extension for submission is approved by the director, and shall cooperate with all other aspects of the investigation.

(ii) Failure to comply with a requirement of this section shall result in automatic sanctions.

(b) It is presumed that the affected municipality is abusing police power by conducting an unlawful speed trap upon a finding by the director that:

(1) The amount of revenue for the affected municipality exceeded thirty percent (30%) of the affected municipality's total expenditures, less capital expenditures, water department expenditures, sewer department expenditures, fiduciary fund expenditures, enterprise fund expenditures, and debt service, in the preceding year; or

(2) More than fifty percent (50%) of the summons written for the traffic offense of speeding that is a misdemeanor, a violation of state law, or a violation of a local ordinance in the affected municipality are written for speed limit violations that are ten miles per hour (10 m.p.h.) or less than the posted speed limit.

HISTORY: Acts 1995, No. 855, § 3; 1997, No. 842, § 1; 2001, No. 1425, § 1; 2019, No. 364, § 2; 2019, No. 910, §§ 5798, 5799.

12-8-404. Sanctions.

(a)(1) Upon the completion of an inquiry, the Director of the Department of Arkansas State Police shall forward all information to the prosecuting attorney of the affected municipality, who will make the determination as to whether the municipality has abused its police power.

(2) The prosecuting attorney shall have the power to issue the following sanctions:

(A) Order that a municipality abusing police power cease patrolling any or all affected highways; or

(B) Order that all or any part of future fines and court costs received from traffic law violations or misdemeanor cases where the location of the offense is an affected highway be paid over to a county fund for the maintenance and operation of the public schools located in the county in which the municipality is located.

(b) Any violation of the sanction ordered under subdivision (a)(2)(A) of this section by any police officer shall constitute a Class A misdemeanor for each citation or summons issued or misdemeanor arrest made in violation of the prosecuting attorney's order.

HISTORY: Acts 1995, No. 855, §§ 4, 5; 1997, No. 842, § 2; 2001, No. 1425, § 2; 2005, No. 1962, § 27; 2019, No. 910, § 5800.

12-8-405. Required audit inquiry.

An audit of an affected municipality under § 10-4-412 or § 14-58-101 shall include an inquiry to determine whether the affected municipality is potentially abusing police power.

HISTORY: Acts 2019, No. 364, § 3.

DISTRIBUTION TO COUNTY AND CITY FUNDS

27-70-207. Definitions.

(a) As used in this section, "public transportation" means a conveyance of human passengers by bus, van, or any other ground surface vehicle that is:

(1) Provided to the general public or selected groups of the public on a regular or continuing basis; and
(2) Operated by a city, county, or any other person or entity under a contract or agreement with a city or county.

(b)

(1)
(A) All highway revenues transferred to the County Aid Fund under this subchapter shall be paid over by the Treasurer of State to the treasurers of the respective counties of this state for credit to the county highway fund, there to be used for transportation projects as deemed beneficial by the county to include without limitation:
(i) The maintenance, construction, and reconstruction of roads and bridges in the county highway system and for other surface transportation;
(ii) Public transportation; or
(iii) Any other transportation system improvement or service within the political subdivision, including without limitation those projects defined as a transportation system under § 27-76-103 regardless of whether or not the political subdivision is a member of a regional mobility authority.
(B) A county may also use these funds to construct and maintain parking for county courthouses, county administration buildings, county health units, and county parks and to construct and maintain sidewalks that serve county courthouses, county administration buildings, county health units, county parks, public schools, and other publicly owned property.
(C) A county may use these funds to pay for local projects eligible for funding under state programs of the Arkansas Department of Transportation and the State Highway Commission and under federal programs of the Federal Highway Administration and the Federal Transit Administration.
(D) Furthermore, the funds may be used to install and maintain traffic signals where needed to preserve public health, safety, and welfare.
(E) A county may provide these funds to a regional mobility authority to match federal transportation funds for the financing of surface transportation system improvements on state highways, county roads, and city streets.
(2) The Treasurer of State shall on or before the tenth day next following the last day of each calendar month make distribution of the revenues on the following basis:
(A) Thirty-one percent (31%) of the amount according to area, with each county to receive the proportion that its area bears to the area of the state;
(B) Seventeen and one-half percent (17.5%) of the amount according to the amount of state motor vehicle license fees collected in the calendar year next preceding any distribution as certified to the Treasurer of State by the Secretary of the Department of Finance and Administration, with each county to receive the proportion that the total of fees collected from the county bears to the total of fees collected in the state;

(C) Seventeen and one-half percent (17.5%) of the amount according to population based upon the most recent federal decennial census, with each county to receive the proportion that its population bears to the population of the state;
(D) Thirteen and one-half percent (13.5%) of the amount according to rural population based upon the most recent federal decennial census, with each county to receive the proportion that its rural population bears to the rural population of the state; and
(E) Twenty and one-half percent (20.5%) of the amount shall be divided equally among the seventy-five (75) counties.

(c)

(1)
(A) All highway revenues transferred to the Municipal Aid Fund under this subchapter shall be paid over by the Treasurer of State by direct deposit to the treasurers of the respective cities of the first class, cities of the second class, and incorporated towns for credit to the street fund, there to be used for transportation projects as deemed beneficial by the governing body of the political subdivision to include without limitation:
(i) The maintenance, construction, and reconstruction of streets that are not continuations of state highways and for other surface transportation;
(ii) Public transportation; or
(iii) Any other transportation system improvement or service within the political subdivision, including without limitation those projects defined as a transportation system under § 27-76-103, regardless of whether or not the political subdivision is a member of a regional mobility authority.
(B) A city may provide these funds to a regional mobility authority to match federal transportation funds for the financing of surface transportation system improvements on state highways, county roads, and city streets.
(C) A city may use these funds to construct and maintain parking for city administration buildings, city recreation buildings, and city parks, and to construct and maintain sidewalks that serve city administration buildings, city recreational buildings, city-owned parking lots, city-owned parking decks, and city parks.
(2)
(A) The Treasurer of State shall on or before the tenth day next following the last day of each calendar month make distribution of the funds on the basis of population according to the most recent federal census, with the amount to be paid over to each city or incorporated town in the proportion that its population bears to the total population of all cities and towns.
(B) If a municipality incorporates during a year in which a federal decennial census is conducted, then for purposes of this section and until data from a federal decennial or special census is made available to the municipality, the population of the municipality shall be based on the most recent federal decennial census as calculated by the Arkansas Geographic Information Systems Office.
(3)
(A)
(i) As used in this subdivision (c)(3), "general revenue" means any revenue deposited into a general fund account that is not:
(a) Restricted by the source of that revenue; or
(b) Transferred from another municipal fund account.
(ii) Beginning on July 28, 2021, if a city or incorporated town has spent funds credited to the street fund in a manner inconsistent with the purposes required by subdivision (c)(1) of this section, the city or incorporated town shall repay the

funds that were not used in accordance with subdivision (c)(1) of this section to the street fund from the city's or incorporated town's general revenue by the end of the following fiscal year.

(B) A city or incorporated town is not eligible to receive highway revenues under subdivision (c)(1) of this section until the city or incorporated town:

(i) Repays the entirety of the funds owed to the street fund, including any funds owed prior to July 28, 2021, as required under subdivision (c)(3)(A) of this section; or

(ii) Passes an ordinance or a resolution committing to pay and pays ten percent (10%) of the city's or incorporated town's general revenue to the street fund each year until the funds owed are repaid.

(C) However, if a city or incorporated town is unable to repay the funds owed as required by subdivision (c)(3)(B) of this section, the city or incorporated town may request the approval of the Legislative Joint Auditing Committee to pass an ordinance or resolution committing to pay a percentage less than ten percent (10%) of the city's or incorporated town's general revenue to the street fund each year until the funds owed are repaid.

(4)

(A) If the Legislative Joint Auditing Committee is presented with a finding that a city or incorporated town spent funds credited to the street fund in a manner inconsistent with the purposes specified in subdivision (c)(1) of this section or that the city or incorporated town failed to make a repayment owed under subdivision (c)(3)(B)(ii) or subdivision (c)(3)(C) of this section, the Legislative Joint Auditing Committee may provide notice of the finding to the:

(i) Treasurer of State; and

(ii) The city's or incorporated town's officials or employees authorized to prevent or correct the inconsistent spending.

(B) Upon notice of a finding from the Legislative Joint Auditing Committee under subdivision (c)(4)(A) of this section, the Treasurer of State shall:

(i) Confirm with Arkansas Legislative Audit within thirty (30) days of being notified by the Legislative Joint Auditing Committee that a city or incorporated town spent funds credited to the street fund in a manner inconsistent with the purposes required by subdivision (c)(1) of this section or failed to make a repayment owed under subdivision (c)(3)(B)(ii) or subdivision (c)(3)(C) of this section; and

(ii) Withhold highway revenues under subdivision (c)(1) of this section until the entirety of the funds owed are repaid by the city or incorporated town to the street fund.

(d)

(1) All highway revenues transferred to the State Highway and Transportation Department Fund under the provisions of this subchapter shall be used for the construction, reconstruction, and maintenance of highways and bridges in the state highway system.

(2)

(A) However, the Arkansas Department of Transportation may use highway revenues transferred to the State Highway and Transportation Department Fund for the installation, upgrading, or improvement of any highway-railroad crossing safety device, railroad crossing traffic control device, warning lights, crossing gates, or other railroad crossing safety devices at public highway railroad crossings and for the construction, reconstruction, and maintenance of any highway-railroad crossing, including the construction or installation of any underpasses or overpasses.

(B) Except for the construction or installation of underpasses or overpasses, the Arkansas Department of Transportation's goal is to expend one dollar ($1.00) of state funds for each dollar of federal funds received to improve railroad crossing safety and to reduce railroad crossing accidents.

(C) It is the intent of this subdivision (d)(2) to encourage the State Highway Commission to continue to upgrade the state's highway-railway crossings with traffic control devices, warning lights, crossing gates, and other appropriate devices in order to increase the safety of persons using the state's highways.

(e) The Department of Finance and Administration shall:

(1) Deposit a total of one cent (1¢) per gallon from revenues distributed under this subchapter from the proceeds derived from existing motor fuel taxes and distillate fuel taxes; and

(2)

(A) Permanently dedicate the revenues to the State Aid Street Fund created under § 27-72-407.

(B) The State Aid Street Fund shall aid city streets under the law.

HISTORY: Acts 1965 (1st Ex. Sess.), No. 39, § 5; 1967, No. 11, § 1; 1967, No. 41, § 1; 1967, No. 417, § 1; 1968 (1st Ex. Sess.), No. 10, § 1; A.S.A. 1947, § 76-334; Acts 1989, No. 371, § 1; 1997, No. 361, § 1; 1999, No. 724, § 1; 2001, No. 1216, § 1; 2003, No. 208, § 1; 2005, No. 2275, § 7; 2007, No. 389, § 2; 2007, No. 1100, § 3; 2011, No. 752, § 1; 2013, No. 1010, § 1; 2017, No. 607, § 1; 2017, No. 707, §§ 411, 412; 2019, No. 133, § 1; 2019, No. 747, § 13; 2019, No. 910, § 4817; 2021, No. 438, § 3; 2021, No. 517, § 1; 2021, No. 709, § 1; 2023, No. 127, § 1.

REPORT OF SECURITY INCIDENT

10-4-429. Definitions.

(a) As used in this section:

(1) "Public entity" means an entity of the state, political subdivision of the state, or school; and
(2) "Security incident" means any compromise of the security, confidentiality, or integrity of an information system maintained by a public entity, a contractual provider of an information system that contracts with a public entity, or other computer-related services of a public entity, that is caused by any unauthorized:
(A) Access to an information system of a public entity;
(B) Destruction of an information system of a public entity or the data of an information system of a public entity; or
(C) Acquisition of data from an information system of a public entity.

(b)

(1) A public entity that experiences a security incident shall disclose, in writing, an initial report of the known facts of the security incident to the Legislative Auditor within five (5) business days after learning of the security incident.
(2) A public entity shall provide regular updates of the security incident to the Legislative Auditor until the investigation of the security incident is closed.

(c) The Legislative Auditor shall:

(1) Maintain a list of all security incidents reported by a public entity; and
(2) Annually on or before December 15, report the information required by subdivision (c)(1) of this section to the Legislative Council, Legislative Joint Auditing Committee, and Joint Committee on Advanced Communications and Information Technology.

(d) If the Legislative Auditor believes the security incident significantly compromises citizens' data, creates a significant security concern, or involves significant theft, then the Legislative Auditor shall notify:

(1) The Governor;
(2) The President Pro Tempore of the Senate;
(3) The Speaker of the House of Representatives;
(4) The House and Senate cochairs of the Legislative Council;
(5) The cochairs and the co-vice chairs of the Legislative Joint Auditing Committee; and
(6) The cochairs of the Joint Committee on Advanced Communications and Information Technology.

(e) A report, update, notification, or list created or maintained under this section is exempt from disclosure under the Freedom of Information Act of 1967, § 25-19-101 et seq., as a security function under § 25-19-105(b)(11).

HISTORY: Acts 2021, No. 260, § 1; 2023, No. 175, § 2.

DATA COMPANY

19-11-107. Definitions.

(a) As used in this section:

(1) "Contractor" means a person having a public contract with a public entity for storage services or software services;
(2) "Data" means recorded information, regardless of form or characteristic;
(3) "Data company" means a contractor that provides software and stores data for a public entity or provides storage services for a public entity;
(4) "Entity of the state" means any department, institution of higher education, board, commission, agency, quasi-public organization, official, office, or employee, or any agency, instrumentality, or function thereof;
(5) "Political subdivision of the state" means any county, municipality, quasi-public organization, district, official, office, or employee, or any agency, instrumentality, or function thereof;
(6)
(A) "Public contract" means an agreement for the purchase of commodities and services by a public entity.
(B) "Public contract" includes supplemental agreements;
(7) "Public entity" means an entity of the state or a political subdivision of the state or a school;
(8) "School" means any public school district, charter school, or education service cooperative, or any publicly supported entity having supervision over public educational entities; and
(9) "Storage services" means the storage of data of a public entity.

(b)

(1) Data that is stored by a data company for a public entity is the property of the public entity.
(2) A data company shall not sell, disclose, or otherwise use the data that is stored for any other purpose without express authorization from the public entity unless the data is:
(A) Considered open; or
(B) Released in the public domain by the public entity.
(3) A data company shall comply with the Arkansas Information Systems Act of 1997, § 25-4-101 et seq.

(c)

(1) Upon the expiration or termination of a public contract, a data company shall return all data to the public entity in the format specified in the public contract and in a secure manner.
(2)
(A) If the public contract does not specify a format for return of the data, as an express term of the public contract, the data company shall return all data to the public entity in a secure common data format specified by the public entity in writing and delivered to the data company within thirty (30) days after the expiration or termination of the public contract.

(B) Notwithstanding the requirement of a public entity to specify in writing the secure common data format for return of the data and to deliver the data in that format to a data company under subdivision (c)(2)(A) of this section, a data company shall return all data to a public entity in a usable format within sixty (60) days after the expiration or termination of a public contract unless there is a contractual agreement that specifies what data can be kept, how long the data can be kept, and the purposes for which the data can be used by the data company.

(d)

(1) A data company shall provide for the destruction of data still in its possession in a secure manner such that data cannot be reconstructed with backups or duplicate copies of data.
(2) The data company shall provide a certificate of destruction and describe the methods used for destruction.
(3) Destruction of the data shall be effected:
(A) Upon written approval by the public entity that acknowledges destruction of the data; and
(B) No later than six (6) months after the expiration or termination of the public contract.

(e) This section does not prevent a public entity and a data company from negotiating a public contract to determine the type of data format that is acceptable for transferring data from a data company or from negotiating a public contract that expressly contemplates alternate terms with regard to data return or data destruction, which alternate terms shall prevail over this section.

HISTORY: Acts 2021, No. 763, § 1.

Arkansas Legislative Audit

Information Systems Best Practices

October 2024

TABLE OF CONTENTS

Page

PURPOSE

Arkansas Legislative Audit (ALA) has established Information System (IS) Best Practices that are widely used in both industry and government. These best practices provide practical information about internal controls and are meant to encourage organizations to develop, implement, and maintain IS policies and procedures that adhere to current best practices. ALA recommends that entity management conduct a formal risk assessment and use the results to determine which best practices are suitable for their specific environment. Since each situation is unique, management should use these guidelines as a self-monitoring tool to understand, assess, and mitigate potential information security risks to the organization's operations and assets. These best practices should be used as a resource to enhance the design of existing internal controls and to implement new policies and procedures required by changes in risk to assets and operations. It's important to note that these best practices are not comprehensive, and they do not replace locally developed internal control policies and procedures. Ideally, control policies and procedures should be documented and distributed to all employees, as the application of these control procedures is the responsibility of every employee. The effectiveness of internal controls depends on the commitment of both management and staff to protecting resources.

ALA encourages organizations to adopt the CIS 18 Critical Security Controls developed by the Center for Internet Security. These controls, available at https://www.cisecurity.org/controls/cis-controls-list, provide best practices to strengthen cybersecurity posture and protect against prevalent threats. They address vulnerabilities caused by poor cyber hygiene and help establish good cyber hygiene to defend against cyber threats. Note: If links in this document are not clickable, please copy and paste them into a web browser.

Internal Controls

Management is responsible for ensuring proper controls and functioning as intended. Therefore, internal controls are essential for the effective and efficient operation at all levels of government. Internal controls encompass activities, policies, and procedures designed to reasonably ensure that operations meet stated objectives. Well-designed and functioning controls assist an organization in adapting to changing situations, demands, and threats while reducing the likelihood of significant errors or fraud occurring and going undetected.

External auditors are not responsible for the design and effectiveness of internal controls, but they evaluate them as part of their audit planning process. Management is responsible for ensuring proper internal controls are in place and performing as intended. A governing body's responsibility is to adopt written policies established by management to provide oversight, authorization, and ethical leadership. Additionally, management should be aware of the impact information technology (IT) has on the internal control framework and the challenges associated with a digital environment.

Information technology (IT) is an integrated part of state and local government financial operations and should be considered in conjunction with overall internal controls planning. Internal IT controls affect financial operations and should be implemented and reviewed by each office, department, or functional area of responsibility.

To execute responsibilities effectively, management must understand how an integrated internal control framework should work. State and local governmental entities may also adopt the Standards for Internal Control in the Federal Government "Green Book," which can be found at https://www.gao.gov/greenbook.

Assessing Risk

Each governmental entity remains unique in its circumstances and risks that affect the design and implementation of internal controls. Before determining which controls should be implemented, entities should conduct a formal risk assessment to identify, analyze, and respond to potential risks, fraud, or errors that may occur and remain undetected.

After identifying risks, entities should implement controls to mitigate or reduce those risks. The relationship between the cost of implementing controls and the benefits gained during the design process should be considered. When implementing specific controls is not practical or cost-effective, other controls should be considered to mitigate risk.

Monitoring

Identifying risks and implementing adequate controls will only protect assets and produce reliable financial information if management and employees follow established procedures. Policies and procedures should be regularly reviewed to confirm that controls are being executed as designed. It is also important to consider feedback received from employees. Some control procedures may appear to be reasonable solutions to an identified risk; however, they may cause unforeseen problems or inefficiencies once implemented. At the same time, other activities may not need controls, yet upon further analysis, some control may be warranted.

While this document is intended to establish minimum levels of compliance for auditing purposes, it is not all-inclusive. Because the IT environment is dynamic and ever-changing, these guidelines will be modified periodically to reflect industry changes as closely as possible. Guidelines have been generalized, where possible, to allow for broad application to various types and sizes of entities. Current IT trends, business processes, and cost considerations specific to the individual entity should be considered when applying these guidelines.

INTRODUCTION

General and Application Controls are the main control activities applicable to the IS environment. All IS controls throughout the industry may be broadly categorized as such and are presented here as follows:

Part One: General Controls

General Controls are established to provide reasonable assurance that the information technology an entity uses operates as intended to produce properly authorized, reliable data when needed and that the entity complies with applicable laws and regulations. Typically, General Controls include the following elements:

IS Management	(Best Practices 1-1)
Contract/Vendor Management	(Best Practices 1-2)
Network Security	(Best Practices 1-3)
Wireless Networking Security	(Best Practices 1-4)
Physical Access Security	(Best Practices 1-5)
Logical Access Security	(Best Practices 1-6)
Disaster Recovery/Business Continuity	(Best Practices 1-7)

Part Two: Application Controls

Application Controls relate to the transactions and data produced by each computer-based automation system; they are, therefore, specific to each application. Application controls should be designed to ensure accounting records' confidentiality, completeness, accuracy, and the validity of entries made. Typically, Application Controls contain the following elements:

Data Input	(Best Practices 2-1)
Data Processing	(Best Practices 2-2)
Data Output	(Best Practices 2-3)
Application-Level General Controls	(Best Practices 2-4 through 2-7)

Part Three: Other Technology

To manage risk with other technology, entities must understand it and its associated risks. Risk can be managed by being technologically proficient and establishing practices related to governance. Other technology elements include:

Electronic Signatures and Digital Signatures	(Best Practices 3-1)
Payment Cards (Debit or Credit)	(Best Practices 4-1)
Bring Your Own Device (BYOD)	(Best Practices 5-1)
Electronic Banking	(Best Practices 6-1)

Note: Items underlined have been modified since the last published date of August 2023.

BEST PRACTICES – GENERAL CONTROLS

IS Management

1-1: IS management must ensure adequate internal controls are in place to achieve the organization's established and developing goals and objectives.

1-1.1: Develop an IS Department organizational chart and update it as the environment changes.

1-1.2: Conduct a formal, organization-wide IT risk assessment utilizing a standard risk assessment framework to:

- Identify "what could go wrong" events resulting from malicious or unintentional acts that can lead to negative consequences.
- Determine the levels of cybersecurity risk and the probability of exposure or loss resulting from an organization's security event or data breach.
- Dedicate adequate resources to implement safeguards to mitigate risks.
- Conduct a risk assessment involving engaging employees at all levels to identify risks and how those risks affect organizational objectives.

IS management should monitor and manage ongoing risks associated with information technology, understand current practices, and involve end users in addressing these risks and mitigating negative impacts.

1-1.3: Develop and maintain a process to identify and address hardware and software security vulnerabilities.

1-1.4: Develop and maintain a formally approved IS Operational Policy and Procedure Manual. The manual may be one or more documents and should be reviewed and updated annually and as the operating environment changes.

1-1.5: Ensure that the duties of software developers and end users are distinctly segregated and documented.

1-1.6: Develop policies and procedures addressing non-business use of entity equipment, facilities, and Internet services. Require employees to sign a technology use policy. This policy should clarify that information processed and stored on government computers is not considered private. Stipulate that computers and other government resources should not be used for personal purposes, the policy may allow for incidental personal use, and penalties for misuse of equipment should be outlined.

1-1.7: Develop and maintain an up-to-date inventory of all hardware devices attached to the network physically, virtually, or remotely. Ensure only authorized devices are allowed to connect. Establish a process to identify and address unauthorized devices. Include information about the asset (location, tag number, owner, operating system, IP, and MAC address, if applicable). Review and update bi-annually.

1-1.8: Develop and maintain an accurate inventory of all software running on your systems and network. Identify unauthorized and unmanaged software and prevent its installation or execution. If appropriate, include vendor name, version, install date, and asset tag. Review and update bi-annually.

1-1.9: Obtain proper replacement insurance for production software and hardware/equipment.

1-1.10: Establish and maintain a data management policy/process that addresses data sensitivity, ownership, retention periods, location, storage, and disposal.

1-1.11: Develop and document database and network backup processes, including how often data are backed up and how copies of backups will be maintained.

1-1.12: Assign and communicate database and network backup responsibilities to designated staff.

1-1.13: Establish access to an environmentally safe, geographically separate, secure off-site location to retain database and network backups.

1-1.14: Establish and formally document the frequency of backups, ensuring that minimum industry standards (e.g., daily, weekly, monthly, annually) are met. For critical processes, backups should occur daily or at longer intervals based on the significance of the information and the rate of changes.

1-1.15: Establish and formally document the method of backup:

a. Full Backup: All files and software.
b. Incremental Backup: Files that have changed since the previous backup.
c. Differential Backup: All the data that have changed since the last full backup.
d. Mirror Backup: Straight copy of the selected folders and files at a given time.
e. Maintain offline copies of backups in case a cyberattack renders online files unusable.

1-1.16: Ensure the selected backup process and retention policy comply with laws and regulations. Retention policy may include retaining periodic snapshots of data backups if data becomes corrupted and contaminates the backup.

1-1.17: Maintain documented security configuration standards for all hardware and software update documentation annually or when significant enterprise changes could impact this safeguard.

1-1.18: Routinely copy operating system software, application software, hardware configurations, and production information to backup media based on frequencies set by management. This applies to all systems (e.g., local area network [LAN] or wide area network [WAN] servers, client/server database servers, special-purpose computers, etc.).

1-1.19: Maintain and annually test offline data backups of critical systems and data storage.

1-1.20: Establish and maintain user and administrative accounts inventory. At a minimum, the inventory should contain the person's name, username, start/stop dates, and department.

1-1.21: Ensure administrator/super user accounts are limited and properly approved.

1-1.22: Develop a breach notification policy that requires individuals to be notified when a security incident occurs and confidential information is compromised.

1-1.23: Regularly evaluate network availability and reliability and provide ongoing improvements to services and security as needed.

1-1.24: Establish and maintain a formal cybersecurity awareness program to ensure that all end users receive education on current and emerging cybersecurity threats, the importance of protecting assets and the associated risks.

1-1.25: Ensure employees are aware of social engineering threats, which are attacks that involve persuading authorized users or administrators to reveal confidential information to people they don't know over the phone or through emails from unknown parties. Employees should be trained never to open or download suspicious attachments.

1-1.26: Periodically host cybersecurity training for employees. Examples of relevant discussion and training topics include but are not limited to:

a. Tabletop discussions on cybersecurity or security policy review.
b. Emerging cybersecurity threats.
c. Trending social engineering methods.
d. Limiting the types of sensitive information collected, transported, and stored.
e. Hazards of viruses, malware, ransomware, and spyware.
f. Accessing malicious websites.
g. Download files from the Internet or clicking links.
h. Embedded email links and downloading attachments that may appear reasonably valid.

1-1.27: Establish a formal Security Incident Response plan. This plan should outline the strategy for responding to information security incidents. Given the wide variety of security incidents that an organization could face and the rapidly evolving threats, this document should be designed to guide a response to security incidents, determine the scope and risk of security events, and ensure an appropriate response to information security incidents, including communication of incidents to the relevant parties. Please refer to NIST 800-61 revision 2 for guidance on developing a security incident plan.

1-1.28: In accordance with Arkansas Act 260 of the 2021 Regular Session, a public entity or a contractual provider of a public entity is required to provide a written initial report of known facts regarding a security incident to the Legislative Auditor within five business days of becoming aware of the incident. Furthermore, the public entity must provide regular updates. Any report, update, notification, or list created or maintained under this section is exempt from the Freedom of Information Act (FOIA) as it is considered a security function under Ark. Code Ann §25-19-105(b)(11).

The Security Incident Reporting form is located at www.arklegaudit.gov

Contract/Vendor Management

1-2: Outsourced IT vendors must adhere to laws, regulations, and the organization's policies and procedures.

1-2.1: Ensure that all contracts are reviewed before approval to guarantee compliance with Ark. Code Ann. § 10-4-424, which grants Arkansas Legislative Audit access and authority to audit computer applications supplied by vendors. It is also crucial to confirm that business processes and applicable legal requirements are thoroughly addressed and documented.

1-2.2: Establish a service level agreement for the maintenance and support of each contract, specifically defining each party's performance expectations.

1-2.3: Confirm that the vendor is a going concern. Ensure that provisions are made to hold application source code in escrow.

1-2.4: Limit vendor access to entity resources. Log access, monitor vendor activity, and review for appropriateness.

1-2.5: Vendors of cloud computing services or other hosted solutions should comply with ALA IS Best Practices and the State of Arkansas information security standards through service level agreements and contracts and provide a Service Organization Control Report (SOC), if available.

1-2.6: Prior to transferring data or application services to or from a cloud computing environment, it is vital to understand applicable laws, regulations, duties, and responsibilities imposed on both management and the vendor (e.g., data ownership, data stewardship, data retention, data protection, jurisdictional issues, disclosures).

Network Security

1-3: Network security ensures that network architecture includes controls over hardware, software, and data.

1-3.1: Establish a network security policy that is clearly documented and formally approved. Ensure the policy describes potential security risks (identified in sections 1-1.2) and communicates risks to users. Policies should be kept current through regular review and updated to address emerging security threats.

1-3.2: Ensure network devices (e.g., firewalls, routers, etc.) are appropriately placed and configured to protect internal and external access to devices, applications, and services.

1-3.3: Implement DNS (Domain Name System) filtering to block malicious websites and filter out harmful or inappropriate content.

1-3.4: Limit physical and logical access to network devices (e.g., firewalls, routers, servers, etc.) and ensure that changes to these devices are properly managed. Establish policies for proper tracking, authorization, testing, and approval of changes.

1-3.5: State of Arkansas governmental entities should transition to the government-restricted ".gov" top-level domain. The .gov domain establishes itself as a trusted source for online services like websites or emails. It identifies an entity as a government agency, improves security and trust in services provided at any level of government, and is available at no cost at https://get.gov/registration/

1-3.6: Implement email authentication technology to protect users from spam, phishing scams, and other malicious emails.

1-3.7: Ensure a process exists to identify, detect, and address unauthorized assets on the network.

1-3.8: Obtain anti-virus, anti-malware, and advanced persistent threat software and provide for their continued use. Ensure programs are set for automatic updates and scan devices on an established schedule. Scan any media inserted into hardware (e.g., USB and external hard drives). Ensure the network security policy covers external devices (e.g., USB drives, Smart Devices, etc.).

1-3.9: Establish and maintain a process for performing internal and external network vulnerability scanning, including a remediation process to address critical risks identified.

1-3.10: Develop remote access authentication policies, procedures, and encryption protocols (considering the above-mentioned risks). Consider the use of virtual private networking (VPN) technology. Include procedures for usage restrictions, configuration/connection requirements, implementation guidance for each type of remote access allowed, and monitoring and handling of questionable activity.

1-3.11: Establish encryption methods for sensitive data transmitted externally and across the network, including procedures for keeping protocols current and effective.

1-3.12: Ensure all IT administration duties outsourced to a vendor are evaluated for associated risks. Vendor access to your network should be restricted to files and applications needed to perform the vendor's duties. The contract with the vendor should provide that the vendor agrees to perform services in compliance with the entity's security policies and legal requirements.

1-3.13: Ensure operating systems are set to automatic updates. Turning off or rebooting computers regularly supports the installation of updates and refreshes system resources. Updates and patches for server operating systems are critical and should be reviewed and updated on a regular schedule.

1-3.14: Enable and monitor network audit logs to identify potential misuse of system resources or information. Logging activities shall include regularly monitoring system access to prevent attempts at unauthorized access and confirm access control systems are effective.

1-3.15: Consider a defense-in-depth methodology by implementing multiple layers of security to protect data, networks, and systems. Successive layers of defense mechanisms can reduce the risk of a successful attack by someone with malicious intent. A combination of controls ensures that systems do not become overly dependent on any one control or layer of security and provides added protection in case a layer fails to function correctly or does not prevent or stop a threat to your data or systems.

1-3.16: Apply critical updates and patches to systems and hardware within 14 days. Apply all other updates and patches to systems and hardware not designated as essential within 30 days. Obtain patches, system upgrades, or other vendor releases from trusted sources. Periodically audit and remediate systems and appliances that are missing updates.

Wireless Networking Security

1-4: Wireless security provides a secure network connection to prevent harm to the network and inappropriate access to resources.

1-4.1: Establish security policies and procedures that ensure wireless usage restrictions, configuration, connection, and password requirements, as well as implementation guidance for wireless access, are appropriate. Policies and procedures should identify information resources that should and should not be available to users and the types of prohibited communications, especially when sensitive and/or critical data are involved. Address the use of wireless technology to ensure compliance with IEEE 802.11i Security Standard. Document policies to include the risks (identified above) associated with this technology and ensure that policies are communicated to users.

1-4.2: Ensure that the Administrator credentials and Service Set Identifier (SSID) are changed from the default value and a naming convention that excludes all identifiable information about the entity and the technology in use. The SSID name should be communicated to entity employees but not publicly broadcast.

1-4.3: Establish routine security patch applications for wireless access devices, ensuring that upgrades are applied as they are released.

1-4.4: Maintain an inventory of authorized access points (APs) and periodically conduct site inspections to determine that no unauthorized APs are in use.

1-4.5: Establish physical security controls over wireless network devices to prevent unauthorized access. For example, all devices should be secured with locking mechanisms or kept in a restricted area where only authorized personnel can access.

1-4.6: Review perimeter (external) security established in sections 1-3.2 and ensure that the risks identified for wireless networking (see section 1-4.1) are adequately addressed in the placement and configuration of network devices.

1-4.7: Ensure that entity-approved guest access only allows Internet browsing and requires guest users to agree to terms of use, state that user activity on the wireless network is monitored.

Physical Access Security

1-5: Physical access security controls are implemented to protect system resources and the facilities used to support their operation.

1-5.1: Develop a Physical Access Security Policy based on network devices' criticality and physical placement. The policy should include access key/keycard management, authorization procedures for visitors, new employees, contractors, etc.; and provisions for removing access for terminated employees, consultants, security professionals, etc.

1-5.2: Ensure that the server room and data processing areas are adequately restricted to authorized personnel and located in a discreet area inaccessible to outsiders.

1-5.3: Implement the following physical security controls:

a. Entrance and exit controls.
b. Visitor escorting.
c. Vendor escorting.
d. Logging of entry and exit dates and times.
e. Surveillance cameras.

1-5.4: Implement the following environmental controls, where possible:

a. Fire suppression system.
b. Smoke detector.
c. Temperature/Humidity monitor.
d. Adequate ventilation and air conditioning systems.
e. Uninterruptible power supply (UPS).
f. Emergency power generator.
g. Raised floor.
h. Water detection.

1-5.5: Develop specific procedures to immediately disable terminated employee access and control the issuance/revocation of access keys/keycards. Conduct an annual inventory of keys/keycards to identify facility access and ensure terminated employee access is revoked. If unauthorized access is found, rekey doors and change security codes.

1-5.6: Develop a monitoring system for physical access, ensuring that access violations are detected and violations and corrective actions are documented.

1-5.7: To minimize the risk of exposure, securely wipe or destroy unused data storage devices such as workstations or mobile devices and paper documents containing personal information.

Logical Access Security

1-6: Logical access security controls defend IT systems and data by verifying and validating the identity of authorized users.

1-6.1: Develop a Logical Access Security Policy based on identified risk areas to protect high-risk system resources. The policy should establish user identification, authentication, and account control mechanisms and protect system administration tools and utilities from unauthorized access. Include provisions for monitoring access security best practices to ensure policies remain current.

1-6.2: Establish user security access based on the principle of least privilege, allowing only authorized access necessary for assigned duties in line with the entity's business processes.

1-6.3: Establish a process for granting access to enterprise assets for new hires and role changes, ensuring proper authorization and periodic review by resource owners. Investigate questionable authorizations and limit access to sensitive system resources to users with documented business purposes. Remove or disable unnecessary and unauthorized accounts.

1-6.4: Ensure that, at a minimum, the following password parameters for logical security controls are required:

a. User identification and a password are required.
b. Users are required to change passwords every 90 days, with passwords of at least 12 characters changed every 185 days.
c. Passwords must be at least 8 characters long, mixed with letters and numbers, and not repeating characters. We strongly recommend using 12 characters.
d. The system forces new users to change their initially assigned password.
e. A password history file systematically prevents the reuse of at least the last 24 passwords/phrases.
f. The user account will be locked after five unsuccessful login attempts and will remain locked until reset by an administrator or within a reasonable period of time. After a reasonable period of no activity, computer session timeout requires user authentication to restore the session.
g. Passwords are not revealed to anyone, including management, help desk personnel, security administrators, family members, or co-workers.
h. Passwords should not be stored in plaintext, which means storing a password in clear, readable text.
i. Management establishes and monitors the user Security Event Log.
j. Ensure all employees with access to essential systems and services use multifactor authentication (MFA). This requirement includes access to web-based platforms, such as financial institutions, third-party applications, and webmail services. All administrative accounts, except service accounts, should use MFA.

Note 1: Most operating systems and applications have configurable password settings that systematically require passwords to conform to the above mentioned requirements. Password settings are not considered enforced unless systematically required.

Note 2: Any deviations from established password best practices are evaluated case-by-case.

1-6.5: Ensure Security Event Logs are regularly reviewed for violations. Document any identified violations and associated corrective actions as part of incident handling procedures.

1-6.6: Other technologies for user identification and authentication, such as biometrics (e.g., fingerprint verification, signature verification) and use of hardware tokens (e.g., smart cards) are available and should be considered, if appropriate.

1-6.7: Systems using user ID/password and ID/biometrics should enforce the same password parameters described at 1-6.4.

1-6.8: Restrict administrator privileges from running on workstations. Running in administrator mode increases exposure to security threats, which can compromise the entire network; administrative mode should be disabled by default or, at a minimum, protected with strong credentials and utilized only when necessary to perform administrator functions.

Disaster Recovery/Business Continuity

1-7: Disaster recovery and business continuity planning involves creating plans, policies, procedures, and technical measures to help restore IT operations after an unexpected incident. Organizations should develop a comprehensive plan to minimize the impact of a disaster. Adequate planning should address how to keep critical functions operating in the event of large and small disruptions, ensuring the organization can continue its operations as usual.

1-7.1: Document and approve a Disaster Recovery and Business Continuity Plan that, at a minimum, achieves the following:

a. Ensures that disaster recovery roles and responsibilities are clearly defined.
b. Includes detailed technical instructions and procedures for restoring mission-critical processes and systems (i.e., networking, operating system, and critical applications).
c. Identifies the alternate work/office location and the offsite backup storage facility.
d. Includes necessary contact information for employees, vendors, etc.
e. Ensures manual operating procedures and resources are in place if IT operations are unavailable.
f. Includes application-level contingency planning (established in section 2.7).
g. Covers all systems and operational areas.
h. Has been approved by appropriate governance.
i. Includes details concerning how the plan will be periodically tested.

1-7.2: Ensure a copy of the Disaster Recovery/Business Continuity Plan is stored at the off-site backup location. A copy should also be available to management and employees in either electronic or hardcopy form.

1-7.3: Ensure the Disaster Recovery/Business Continuity Plan is relevant, addresses current risk, and is reviewed and updated annually as conditions and risks change.

1-7.4: Conduct and document annual test scenarios of the Disaster Recovery/Business Continuity Plan. Evaluate test results and update the plan as necessary.

Note: Effective July 1, 2021, management of the Arkansas Continuity of Operations Program (ACOOP) will transfer from the Department of Transformation and Shared Services (TSS) Division of Information Services (DIS) to the Arkansas Division of Emergency Management (ADEM) due to the recent approval of Act 70 of 2021.

Several formats, guidance documents, and other assistance are available for writing and maintaining continuity plans. One example is the FEMA Continuity Plan Template and Instructions for Non-Federal Entities found at this link: https://www.fema.gov/pdf/about/org/ncp/coop/continuity_plan_non_federal.pdf

BEST PRACTICES – APPLICATION CONTROLS

Data Input

2-1: Data input controls are necessary to validate the integrity of data entered into an application.

2-1.1: Establish a properly designed database to reduce redundancies and ensure effective transaction processing. Poor data quality may lead to system control failure, process inefficiencies, and/or inaccurate reporting.

[Example: The County Financial Manual may supply the data structure incorporated into the automated system, followed by users who classify data and perform data entry.]

Manual and/or automated controls should be incorporated into the data structure to prevent the following:

a. Recording or processing of duplicate transactions.
b. Unpopulated data fields.
c. Data formatting inconsistencies.
d. Improper coding to departments, business units, or accounts.

2-1.2: Establish input approval and review policies and procedures. Management should have procedures to identify and correct any errors that occur during the data entry process, providing reasonable assurance that errors and irregularities are detected, reported, and corrected:

a. Ensure that data input is controlled (e.g., proper authorization controls exist, both systematic and manual).
b. Ensure that all inputs have been processed and accounted for.
c. Ensure checks and receipts are systematically pre-numbered and sequenced.
d. Ensure an audit trail is available and enabled with sufficient detail to identify the transactions and events by tracking them from their source.
e. Identify and investigate missing or unaccounted-for source documents or input transactions.
f. Periodically review audit logs to evaluate the extent and status of data errors and changes.
g. Require a monthly exception resolution and ensure all exceptions are resolved before year-end closing.

Data Processing

2-2: Data processing controls provide an automated means to ensure processing is complete, accurate, and authorized.

2-2.1: Ensure that processing errors are identified, logged, and resolved and that incorrect information is identified, rejected, and corrected for subsequent processing. The system should produce edit reports at essential processing stages to trace transactions from beginning to end (e.g., check runs, transaction posting, etc.), and corrections should be required before associated processes are completed.

a. Database transactions or table logs should be available to compare to source documents.
b. Processing logs should be available to identify incomplete or incorrectly processed transactions.
c. Transaction processing overrides should be tracked and monitored.
d. Application should perform edit and validation checks during data processing.
e. Warning and error messages should be produced during all processing phases.
f. Transactions with errors should be rejected or suspended from processing until the error is corrected.

2-2.2: Management should have policies and procedures in place to identify and correct any errors that occur during the data entry process. These policies and procedures should reasonably assure that errors and irregularities are detected, reported, and corrected timely:

a. Ensure that data input controls are in place (e.g., proper authorization controls exist, both systematic and manual).
b. Periodically review user error logs to evaluate the extent and status of data errors.
c. Ensure that all data inputs have been processed and accounted for.
d. Investigate missing source documents or data transactions.
e. Data exception resolution is required before year-end closing.

2-2.3: Establish procedures to ensure that periodic and timely reconciliations and error corrections are performed between the subsidiary and general ledgers.

2-2.4: Establish monitoring procedures to include:

a. Reconciling data inputs to data processed.
b. Maintaining a processing log and reviewing for unusual or unauthorized activity.
c. Monitoring all overrides to transactions.

2-2.5: Ensure that the software/application can prevent data alteration when they are transferred from one process to another.

2-2.6: Ensure that the application can resume processing at the point of interruption.

Data Output

2-3: Data output controls ensure the integrity and reliability of output information and the accuracy and timely distribution of all output produced.

2-3.1: Develop procedures for system output and reporting to ensure:

a. Consistency of content, format, and availability with end users' needs.
b. Sensitivity and confidentiality of data.
c. Appropriate user access to output data.

2-3.2: Establish procedures to enable business process monitoring and tracking of results. Review system-generated reports to ensure the integrity of production data and transaction processing. Review should be performed timely and periodically.

2-3.3: Establish procedures to ensure that output complies with applicable laws and regulations and that legally required reporting is complete and accurate. Review system-generated reports to ensure the integrity of production data and transaction processing. Reviews should be performed timely and periodically.

Application-Level General Controls

Application Security Management

2-4: Application security management identifies criteria and techniques associated with designing and using applications that can be modified to respond to the entity's changing needs.

2-4.1: Identify transactions for financial processes and sub-processes that application security policies should address. Develop a security policy for financial applications that achieves:

a. Establishes security administration procedures.
b. Develop an application access structure based on the principle of least privilege.
c. Outlines ongoing security role management (including monitoring and maintenance procedures).
d. Addresses the roles, responsibilities, and monitoring of third-party vendors.
e. Ensures access security updates, additions, and deletions are properly authorized and supported by a documented business purpose.
f. Periodically verifies that only authorized users have access and that their access privileges are appropriate for their job functions.
g. Addresses encryption of application data (including authentication credentials), both stored and transmitted.
h. Establishes procedures for documenting security and data verification for internal and external system interfaces.
i. Coordinates with overall network securitypolicy.
j. Analyzes application deficiencies and documents corrective actions taken.

2-4.2: Ensure that application access controls (e.g., unique user ID, password configuration, etc.) align with network access security policies established in sections 1-6.

2-4.3: Ensure that public access to applications is controlled by:

a. Restricting access to production systems and data.
b. Distinct security policy covering public access workstations that appropriately restricts access.

2-4.4: Establish procedures for auditing and monitoring application security, including the following:

a. Identification and logging of security exceptions and violations.
b. Set up logging and other parameters to notify administrators of security violations as they occur.
c. Periodic review of exception reports and recommended corrective action by management and security administrators.

2-4.5: Ensure that physical access to application resources has been secured and addressed by security policies as outlined in sections 1-5.

Application Configuration Management

2-5: Configuration management establishes and maintains the integrity of the application throughout its life cycle.

2-5.1: Establish controls over programming to ensure that changes to application functionality in production are authorized and appropriate and that unauthorized changes are detected and reported promptly.

Segregation of Duties

2-6: Segregation of duties is an essential internal control that attempts to ensure that no single individual has the authority to execute two or more conflicting transactions.

2-6.1: Ensure management identifies and documents incompatible activities and transactions based on identified business process and application security risks. Ensure that application security policies address these areas and that users are systematically prevented from executing incompatible transactions. See 1-6.2.

2-6.2: Small governments with limited staff and resources have a reduced capacity to segregate duties. Therefore, Compensating controls should be designed to reduce the risk of error or fraud not being detected. Confirm that user access to transactions or activities that have segregation of duties conflicts is appropriately controlled.

a. Access to incompatible activities is assigned only when supported by a business need.
b. Management periodically reviews user access authorizations for segregation of duties conflicts, considering the position and process changes and updating access to current job assignments.
c. Users with segregation of duties conflicts are documented, and their activity is monitored and reviewed periodically via transaction and audit logs.
d. Management retains documentation that the segregation of duties risk has been mitigated through effective compensating controls.
e. A segregation of duties grid is developed using the "roles and responsibilities" or security master report function within software applications.

Application Contingency Planning

2-7: Application contingency planning provides procedures and capabilities for recovering a major application or general support system. See Disaster Recovery/Business Continuity at 1-7.

2-7.1: Determine mission-critical functions performed by the financial applications, documenting associated vital data and programs. Identify the impacts of automated process disruption and maximum allowable outage times for each application and establish recovery time objectives.

2-7.2: Set a backup retention policy for each application based on recovery time objectives. Ensure that backup intervals support necessary restoration periods. Current application programs and data should be copied according to this policy and securely stored at a geographically distant off-site location.

2-7.3: Establish manual procedures for continuing operations during outage times for the critical functions identified in sections 2-7.1. Incorporate the application-level contingency planning and procedures (including backup policy) into the organization's Disaster Recovery/Business Continuity Plan.

2-7.4: Provide for periodic testing of the application contingency planning. Document test scenario results and corrective actions (including resulting changes to the plan) to be incorporated into organization-wide Disaster Recovery/Business Continuity Plan testing.

BEST PRACTICES – OTHER TECHNOLOGY

Electronic Signatures and Digital Signatures

3-1: Electronic confirmation of signatures is used to authenticate the content of a document.

3-1.1: If electronic or digital signatures are used, management must understand the technology and associated risks. Develop and implement controls to address identified risks and comply with applicable laws and regulations.

3-1.2: Resources include the following: Electronic Signatures in Global and National Commerce Act (15 USC § 7001); Arkansas Electronic Records and Signatures Act (Ark. Code Ann. § 25-31-101); Uniform Electronic Transactions Act or UETA (Ark. Code Ann. § 25-32-101); and Arkansas Department of Information Systems Electronic Signature Standard SS-70-011.

3-1.3: Ensure that implementation of the electronic equivalent of a written signature, which can be recognized as having the same legal status as a written signature, provides adequate security. A digitized written signature can easily be copied from one electronic document to another, with no way to determine whether it is legitimate. On the other hand, electronic signatures are unique to the message being signed and will not verify if they are copied to another document.

3-1.4: A software application that creates a signature on checks and affixes the signature to the check should have an associated access control mechanism. The access control mechanism should only be known by the check custodian and signatory.

3-1.5: Electronic signature disks or any other forms of electronic, digitized, or facsimile signatures should be in a secured location under the control of the signatory. Signature disks or other electronic, digitized, or facsimile signatures should only be used under the direct approval of the official (or deputy) whose signature is on the disk.

Payment Cards (Debit or Credit)

4-1: Payment cards enable the owner (cardholder) to make a payment by electronic fund transfer.

4-1.1: If payment cards are accepted, management must understand the technology and associated risks, develop and implement controls to address identified risks, and comply with applicable laws, regulations, and industry standards.

4-1.2: Develop and maintain written comprehensive policies and procedures that cover the process by which payment cards are accepted and payment card data are processed. Policies and procedures should include but are not limited to:

a. Segregation of duties.
b. Physical security.
c. Storage, transmission, and disposal of the payment card information.
d. Employee criminal background checks.
e. Technology security policies and procedures.
f. Incident response plan.

4-1.3: Adherence to industry standards includes credit card brands' compliance programs and the Payment Card Industry (PCI) Data Security Standards (DSS).

Bring Your Own Device (BYOD)

5-1: Bring Your Own Device (BYOD) is the use of personal electronic devices to access entity systems, data, and resources. Such devices include but are not limited to, smartphones, tablets, laptops, and similar technologies.

5-1.1: If BYOD is allowed, management must understand the technology and associated risks, develop, and implement controls to address identified risks, and comply with applicable laws and regulations.

5-1.2: Ensure the use of the device security features, such as a PIN, password/passphrase, and automatic lock, to help protect the device when not in use.

5-1.3: Keep the device software up to date. Devices should be set to update automatically.

5-1.4: Activate and use encryption services and anti-virus protection if your device features such services. Install and configure tracking and/or wiping services, such as Apple's "Find My iPhone," Android's "Where's My Droid," or Windows' "Find My Phone," if the device has this feature.

5-1.5: Remove promptly after use any entity information stored on your device, including deleting copies of attachments to emails, such as documents, spreadsheets, and data sets.

5-1.6: Before you sell, exchange, or dispose of your device, remove all entity information and return it to the manufacturer's settings.

5-1.7: Promptly report to entity management if your device is lost or stolen or its security is compromised.

5-1.8: Establish a comprehensive BYOD policy that provides standards and behavior rules for using personally owned devices. This policy must be adhered to access organizational resources.

Electronic Banking, Electronic Commerce, and other Electronic Transfer of Funds

6.1: Electronic banking and other electronic funds transfer (EFT) allow bank customers to perform account management and financial transactions over the Internet that directly or indirectly affect funds held by the bank. Despite security controls, there is no absolute way to guarantee the safety of online electronic transactions. Entities should comply with applicable laws and research and understand the risks involved before commencing online electronic transactions.

6-1.1: Develop comprehensive written policies and procedures for all electronic transactions (e-transactions), online banking, and EFT activities. Policies and procedures should include statutory and other legal requirements and responsibilities as well as, but not limited to:

a. Documentation of proper segregation of functions (i.e., the initiator cannot be an approver, etc.).
b. Online banking and EFT activities utilized.
c. Personnel who initiate, approve, transmit, record, review, or reconcile e-transactions.
d. Personnel who approve e-transactions.
e. Personnel who transmit e-transactions.
f. Personnel who record e-transactions.
g. Personnel who review and reconcile e-transactions.
h. Prompt removal or changes to access security for local and online access.
i. Properly maintain all documentation to support transactions for historical review and audit purposes.

6-1.2: Establish a dedicated "hardened" computer with only applications/services loaded that are necessary to perform online banking transactions. This computer should not be used for any other purpose. In cases where a dedicated computer is unavailable, entities must be able to reduce online banking risks to an acceptable level through a combination of other controls.

6-1.3: Install current antivirus, anti-spyware, malware, and adware detection software set to update automatically.

6-1.4: Install firewalls and intrusion prevention systems with continuous monitoring. Any unauthorized and/or suspicious behavior, traffic, or unnecessary file types should be investigated and, if necessary, blocked using access control lists in conjunction with a firewall.

6-1.5: Ensure all employees with access to essential systems and services use multifactor authentication (MFA). This requirement includes access to web-based platforms, such as financial institutions, third-party applications, and webmail services. All administrative accounts, except service accounts, should use MFA.

6-1.6: Limit Internet access to only business-related programs. Frequently delete browsing history, temporary Internet files, and cookies. A hacker or malware program would capture minimal information if the system were compromised.

6-1.7: Ensure the session is secure before undertaking online banking.

6-1.8: Monitor and reconcile bank accounts daily (when feasible).

6-1.9: Periodically (daily, weekly, monthly) review accounts for unauthorized or suspicious activity and report immediately.

6-1.10: Ensure written agreements with banks and/or other payment solutions are reviewed by legal counsel. Ensure written agreements with banks provide appropriate controls for all electronic funds or wire transfers.

6-1.11: Ensure the computer is disconnected from the Internet by unplugging the Ethernet/DSL cable when not in use.

6-1.12: Employ dual authorization of transactions, enforced by bank security where possible (requiring at least two user accounts to submit and approve electronic transactions).

6-1.13: Disallow online account management functions (such as adding users or modifying user security). Account changes should be conducted in person, or at least in writing, with the bank.

6-1.14: Implement out-of-band transaction verification (such as text messages or other security messages to an approver with the entity). Take advantage of other system alerts, including:

a. Balance alerts.
b. Transfer alerts.
c. Password change alerts.
d. Login failure alerts.

6-1.15: Ensure that blank check stock, check reorder forms, canceled checks, check images, and signature stamps are properly safeguarded.

6-1.16: When paying electronically, use a clearing bank account rather than paying directly from the primary account.

6-1.17: Establish transaction and daily limits to lower loss potential.

6-1.18: Consider the cost-benefit of obtaining cybersecurity and data breach insurance. 6-1.21: Restrict browser(s) to sites necessary for EFT.

6-1.19: Ensure that users performing banking transactions use only non-administrative user accounts.

6-1.20: Implement fraud controls, when possible and feasible, to ensure that the bank only processes authorized transactions. Features to consider include:

Implement fraud controls whenever possible and feasible to ensure that the bank only processes authorized transactions. Features to consider include:

a. Positive Pay.
b. Reverse Positive Pay.
c. ACH Positive Pay.
d. ACH Debit Block and Debit Filters.
e. Direct Deposit.

Instruct financial institutions to deny and return all nonconforming transactions as the default procedure.

6-1.21: If possible, implement a processing calendar with the bank to ensure the bank only processes transactions on pre-determined days throughout the year.

6-1.22: Comply with all security requirements outlined in the service level agreement with the bank and all other prudent security measures.

6-1.23: Allow electronic delivery of statements and account information. Ensure any statements or documents containing account information are properly maintained.

6-1.24: Limit access to sensitive information and never share confidential information, tax IDs, Social Security numbers, or account numbers via email.

6-1.25: Establish procedures to verify new or altered employee payroll direct deposit information. Changes should be verified directly with the employee.

CITY/TOWN OF SAMPLE, ARKANSAS
FIXED ASSET LISTING
YEAR ENDING 12/31/2021

Appendix B

Description	Acquisition Date	Property No.	Serial No.	Amount
Land				
Lot 5, Section C	7/2/71			$ 5,000
Buildings				
City Hall	7/2/71			$ 54,257
Fire Station	10/24/81			26,482
TOTAL BUILDINGS				$ 80,739
Motor Vehicles				
General				
1991 Chevy Truck	7/6/05		BR549	$ 10,502
Fire				
1984 Pumper	12/14/07		V187K816G987	35,864
1972 Fire Truck	8/18/97		V1357M751R321	9,762
				45,626
TOTAL MOTOR VEHICLES				$ 56,128
Equipment				
General				
Dell Computer	9/14/08		CW12589KL654	$ 2,500
Power Washer	12/19/10		WKRP325	2,764
				$ 5,264
Fire				
Jaws of Life	4/1/12		682RDL937	$ 2,534
TOTAL EQUIPMENT				$ 7,798
TOTAL FIXED ASSETS				$ 149,665

Note: A list of deletions and additions must be maintained in order to reconcile beginning balance to ending balance. Beginning balance of the current year (or ending balance of the previous year) plus additions less deletions should equal ending balance of the current year.

CITY/TOWN OF SAMPLE, ARKANSAS
GENERAL FUND
CASH RECEIPTS JOURNAL
YEAR ENDING 12/31/2021

Appendix C

Date	Receipt Number	Received from	Total	State Aid	Federal Aid	Property Taxes	Sales Taxes	Franchise Taxes	Fines, Forfeitures and Costs	Local Permits and Fees	Other
1/2/21	1001	State of Arkansas	$ 3,500.00	$ 3,500.00							
1/3/21	1002	County	2,432.15			$ 2,432.15					
1/4/21	1003	District Court	1,436.78						$ 1,436.78		
1/8/21	1004	State of Arkansas	3,427.64				$ 3,427.64				
1/9/21	1005	Entergy	485.98					$ 485.98			
1/10/21	1006	John Doe	75.00							$ 75.00	
1/17/21	1007	US Dept of Justice	10,000.00		$ 10,000.00						
1/18/21	1008	Centerpoint/Arkla	376.25					376.25			
1/18/21	1009	Jan Doe	15.00								$ 15.00
1/18/21	1010	District Court	1,567.38						1,567.38		
		Monthly Totals	23,316.18	3,500.00	10,000.00	2,432.15	3,427.64	862.23	3,004.16	75.00	15.00
		Year-to-date Totals	$ 23,316.18	$ 3,500.00	$ 10,000.00	$ 2,432.15	$ 3,427.64	$ 862.23	$ 3,004.16	$ 75.00	$ 15.00

CITY/TOWN OF SAMPLE, ARKANSAS
GENERAL FUND
CASH DISBURSEMENTS JOURNAL
YEAR ENDING 12/31/2021

Appendix D

				Mayor's Office					Police Department				
Date	Check Number	Payee	Total	Personal Services	Supplies	Other Services & Charges	Capital Outlay	Debt Service	Personal Services	Supplies	Other Services & Charges	Capital Outlay	Debt Service
1/2/21	2001	AT&T	$ 381.25			$ 257					$ 124		
1/3/21	2002	Regions Bank	651.49										$ 651
1/4/21	2003	Bill's Police Supply	125.32							$ 125			
1/8/21	2004	Smith Chevrolet	25,432.97									$ 25,433	
1/9/21	2005	Payroll Account	3,736.23	$ 1,368					$2,368.58				
1/10/21	2006	Farmer's & Merchants Bank	323.85										323.85
1/17/21	2007	Entergy	221.15			100.58					120.57		
1/18/21	2008	Wal-Mart	26.35		$ 26								
1/24/21	2009	Payroll Account	3,860.33	1,367.65					2,492.68				
1/30/21	2010	Centerpoint/Arkla	437.63			153.28					284.35		
		Monthly Totals	35,196.57	2,735.30	26.35	510.75	-	-	4,861.26	125.32	529.28	25,432.97	975.34
		Year-to-date Totals	$35,196.57	$2,735.30	$ 26.35	$ 510.75	$ -	$ -	$4,861.26	$125.32	$ 529.28	$25,432.97	$975.34

Note: Arkansas Code Ann. 14-59-111 states that classifications of expenditures shall include the major type of expenditures (Personal Services, Supplies, etc.) by department (Mayor, Clerk, Treasurer, Police, Fire, etc.). Only 2 departments are shown above for illustrative purposes.

EXAMPLE MUNICIPAL FUND CODES

Appendix E

GENERAL	1000
STREET	2000
SPECIAL REVENUE FUNDS	
LOCAL POLICE AND FIRE RETIREMENT	3001
FIRE EQUIPMENT AND TRAINING - ACT 833	3002
CAPITAL PROJECTS FUNDS	
CITY HALL CONSTRUCTION	4001
DEBT SERVICE FUNDS	
SALES TAX BOND	5001
AGENCY FUNDS	
POLICE BOND AND FINE	6001
DISTRICT COURT	6002
ENTERPRISE FUNDS	
LANDFILL	7001
TRUST FUNDS	
NONUNIFORM	8001
POLICE	8002
FIRE	8003

MUNICIPAL DEPARTMENT CLASSIFICATIONS

General Government		
	Mayor's office	0100
	City Clerk's office	0101
	City Treasurer's office	0102
	City Council	0103
	City Attorney	0104
	Planning Department	0105
	Code Enforcement	0106
	Computer Services	0107
	Economic Development	0108
	Advertising and Promotion	0109
	Tourism	0110
Highways and Streets		
	Street Department	0200
Law Enforcement		
	Police Department	0301
	District/City Court	0302
	Animal Control	0303
	Dispatch	0304
	Police Pension	0305
	Judge and Clerk Retirement	0306
	Drug Control	0307
Public Safety		
	Fire Department	0401
	911	0402
	Fire Pension	0403
Sanitation		
	Sanitation Department	0501
	Landfill	0502
	Recycling	0503
Health		
	Ambulance service	0601
	Mosquito control	0602
Recreation and Culture		
	Parks and recreation	0701
	Library	0702
Social Services		
	Senior Citizen's Center	0801
	Cemetery	0802
Airport		
	Municipal Airport	0901

EXAMPLE CHART OF ACCOUNTS

ASSETS	**1000**
Cash	1010
Investments	1020
Accounts receivable	1030
Interfund receivables	1040
LIABILITIES	**2000**
Accounts payable	2010
Interfund payable	2020
Settlements pending	2030
FUND BALANCE	**3000**
Nonspendable	3100
Restricted	3200
Committed	3300
Assigned	3400
Unassigned	3500
REVENUES	**4000**
State aid	4100
Federal aid	4200
Property taxes	4300
Franchise fees	4400
Sales taxes	4500
Fines, forfeitures, and costs	4600
Interest	4700
Local permits and fees	4800
Sanitation fees	4900
Gas and oil company reimbursements	4910
Other	4950
EXPENDITURES	
Personal services	**5000**
Supplies	**6000**
Other services and charges	**7000**
Capital outlay	**8000**
Debt service	**9000**
OTHER FINANCING SOURCES (USES)	**0000**
Transfers in	0100
Contribution from water department	0110
Transfers out	0150
Contribution to water department	0200

EXAMPLE MUNICIPAL EXPENDITURE CODES CHART

PERSONAL SERVICES - Amounts paid to both permanent and temporary government employees, including personnel substituting for those in permanent positions. This category includes gross salary for personal services rendered while on the payroll of the government and amounts paid by the government on behalf of employees; these amounts are not included in the gross salary, but are in addition to that amount. Such payments are fringe benefits payments and, although not paid directly to employees, are a part of the cost of personal services.

5001	Salaries, Full-Time
5002	Salaries, Part-Time
5003	Extra Help
5004	Contract Labor
5005	Overtime and Other Premium Compensation
5006	Social Security Matching
5007	Retirement Matching
5008	Noncontributory Retirement
5009	Health Insurance Matching
5010	Workmen's Compensation
5011	Unemployment Compensation
5012	Other Fringe Benefits
5013	Car Allowance
5014	Cobraserv
5015	Uniform Allowance
5016	Life Insurance

SUPPLIES - Amounts paid for items that are consumed or deteriorated through use or that lose their identity through fabrication or incorporation into different or more complex units or substances.

SUPPLIES

6001	General Supplies
6002	Small Equipment
6003	Janitorial Supplies
6004	Clothing and Uniforms
6005	Fuels, Oils, and Lubricants
6006	Tires and Tubes

REPAIR AND MAINTENANCE SUPPLIES

6020	Building Materials and Supplies
6021	Paints and Metals
6022	Plumbing and Electrical
6023	Parts and Repairs
6024	Maintenance and Service Contracts
6025	Asphalt
6026	Culvert and Pipe
6027	Gravel, Dirt, and Sand
6028	Lumber and Pilings
6029	Small Tools
6030	Concrete
6031	Bridges and Steel

EXAMPLE MUNICIPAL EXPENDITURE CODES CHART

OTHER SERVICES AND CHARGES

PROFESSIONAL SERVICES - Services that by their nature can be performed only by persons or firms with specialized skills and knowledge. Although a product may or may not result from the transaction, the primary reason for the purchase is the service provided.

7001	Accounting and Auditing
7002	Management Consulting
7003	Computer Services
7004	Engineering and Architectural
7005	Special Legal
7006	Other Professional Services
COMMUNICATIONS	
7020	Telephone and Fax - Landline
7021	Postage
7022	Cell Phones and Pagers
7023	Internet Connection
TRANSPORTATION	
7030	Travel
7031	Common Carrier
ADVERTISING AND PUBLICATIONS	
7040	Advertising and Publications
INSURANCE (OTHER THAN PERSONAL SERVICES)	
7050	Official and Employee Bond
7051	Boilers and Machinery Insurance
7052	Fire and Extended Coverage
7053	Fleet Liability
7054	Other Sundry Insurance
UTILITIES	
7060	Utilities - Electricity
7061	Utilities - Gas
7062	Utilities - Water
7063	Utilities - Water Disposal
RENTALS AND LEASES (NOT LEASE PURCHASE)	
7070	Rent - Land and Buildings
7071	Rent - Machinery and Equipment
7072	Lease - Land and Buildings
7073	Lease - Machinery and Equipment
PUBLIC RECORDS	
7080	Public Records
MISCELLANEOUS	
7090	Dues and Memberships
7091	Miscellaneous Law Enforcement
7092	Meals and Lodging
7093	Vending Machines - Food/Drinks
7094	Other Miscellaneous
7095	Training and Education
7096	Computer Software, Support, and Maintenance Agreement

EXAMPLE MUNICIPAL EXPENDITURE CODES CHART

CAPITAL OUTLAY

8001	Land
8002	Buildings
8003	Improvements Other Than Buildings
8004	Machinery and Equipment (Other Than Vehicles)
8005	Vehicles
8006	Construction in Progress

DEBT SERVICE

9001	Bond Principal
9002	Bond Interest
9003	Note Principal
9004	Note Interest
9005	Lease Purchase Principal
9006	Lease Purchase Interest