ORDINANCE NO. 176

An Ordinance Adopting Electronic Banking, Electronic Commerce, and other Electronic Transfer of funds Best Practices under Ark. Code Ann. 14-59-105

Whereas state law requires municipalities adopt electronic banking and other electronic funds transfer (EFT) best practices approved by the Legislative Joint Auditing Committee prior to use; and;

Whereas EFTs enable bank customers to perform account management and financial transactions over the Internet that directly, or indirectly, affect funds held by the bank; and;

Whereas, despite security controls, there is no absolute way to guarantee the safety of online electronic transactions; and;

Whereas municipalities should comply with applicable laws and research and understand the risks involved before commencing online electronic transactions.

Now therefore be it ordained:

Section 1: The City Recorder-Treasurer shall follow the information systems best practices approved by the Legislative Joint Auditing Committee, attached as **Exhibit A.**

Section 2: Exhibit A shall be reviewed by each employee handing financial matters for the city and followed to the greatest extent possible.

ORDINANCE NO. 176

An Ordinance Adopting Electronic Banking, Electronic Commerce, and other Electronic Transfer of funds Best Practices under Ark. Code Ann. 14-59-105

Section 1: The individual responsible for compliance with the Municipal Accounting Law, Ark. Code Ann. § 14-59-101 et seq., shall 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., initiator cannot be an approver, etc.).
> b. Online banking and EFT activities utilized.
> c. Personnel who initiate 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.

Section 2: Establish a dedicated "hardened" computer with only application/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 not available, entities must be able to reduce online banking risks to an acceptable level through a combination of other controls.

Section 3: Install antivirus, anti-spyware, malware, and adware detection software that is current and set to automatically update.

Section 4: Ensure all updates and patches to operating systems, and hardware drivers are applied timely.

Section 5: Install firewalls and intrusion detection and prevention systems with continuous monitoring. Any unauthorized and/or suspicious behavior or traffic should be investigated and, if necessary, blocked using access control lists in conjunction with a firewall.

Section 6: Employ multi-factor authentication, if possible. Require unique login ids and complex passwords, and ensure computers and browsers are configured to not save passwords. Keep passwords confidential.

ORDINANCE NO. 176

-3-

Section 7: Limit Internet access to only business-related programs. Frequently delete browsing history, temporary Internet files, and cookies. In the event the system is compromised, minimal information would be captured by a hacker or malware program.

Section 8: Check that the session is secure (minimum 128-bit SSL encryption) before undertaking any online banking.

Section 9: Monitor and reconcile bank accounts daily (when feasible).

Section 10 Periodically (daily, weekly, monthly) review accounts for unauthorized or suspicious activity, and report immediately.

6-1-11: Ensure written agreements with banks and/or other payment solutions are reviewed by legal counsel.

Section 12: Ensure written agreements with banks provide appropriate controls for all electronic fund or wire transfers.

Section 13: Ensure computer is disconnected from the Internet by unplugging the Ethernet/DSL cable when not in use.

Section 14: Employ dual authorization of transactions, enforced by bank security where possible (requiring at least two user accounts to submit and approve electronic transactions).

Section 15: 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.

Section 16: When possible, implement use of out-of-band transaction verification (such as text message or other security message 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.

Section 17: Ensure that blank check stock, signature stamps, and facsimile signatures are properly safeguarded with inventory control.

Section 18: Use a clearing bank account when paying electronically rather than paying directly from primary account.

ORDINANCE NO. 176

Section 19: Establish transaction and daily limits to lower loss potential.

Section 20: Consider the cost benefit of obtaining cybersecurity and data breach insurance.

Section 21: Restrict browser(s) to sites necessary for EFT.

Section 22: Ensure that users performing banking transactions use only non-administrative user accounts.

Section 23: Implement use of fraud controls, when possible and feasible, to ensure that the bank only processes authorized transactions, features to consider include:

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

Section 24: Implement use of processing calendar with the bank, if possible, to ensure the bank only processes transactions on pre-determined days throughout the year.

Section 25: Comply with all security requirements outlined in the service level agreement with the bank and all other prudent security measures. Section 26: Allow electronic delivery of statements and account information. Ensure any statements or documents containing account information are properly maintained.
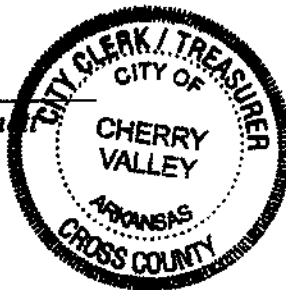
Section 26: Never share any confidential information, tax IDs, Social Security numbers, or account numbers via email.

Dated this __18__ *day of* ___May___ , *2021.*

_____
Mayor Adam Love
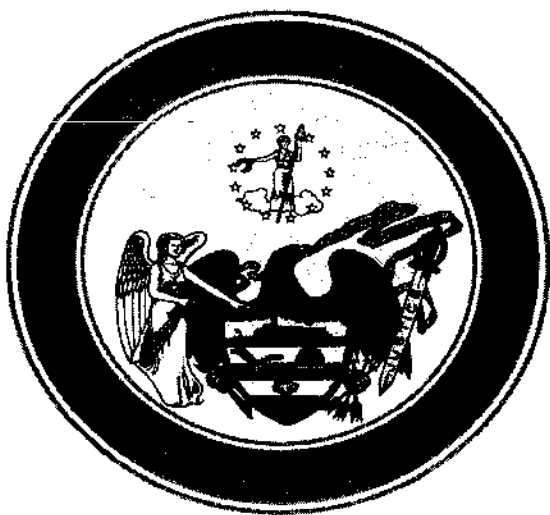
ATTEST:

_____
Recorder-Treasurer Stacey Bennett

Arkansas Legislative Audit

Information Systems Best Practices

TABLE OF CONTENTS

PURPOSE

Arkansas Legislative Audit (ALA) establishes the following Information System (IS) Best Practices, utilized throughout industry and government, to provide practical information about internal controls and encourage entities to develop, implement, and maintain IS policies and procedures that conform to current best practices. ALA recommends entity management conduct a risk assessment and rely on the results of the assessment to establish which best practices are appropriate for their environment. Since each situation is unique, management should utilize these guidelines as a self-monitoring tool to understand, assess, and mitigate potential information security risks to the entity's operations and assets. These best practices should be used as a resource to improve the design of existing internal controls and to implement new policies and procedures required by changes in risk to assets and operations. These best practices are not all-inclusive, nor are they a replacement for locally developed internal control policies and procedures. Optimally, control policies and procedures should be described in a written document and distributed to all employees since the application of these control procedures is every employee's responsibility. Successful internal controls depend on management and staff commitment to the protection of resources.

Internal Controls

It is management's responsibility to ensure that the right controls are in place and that they are performing as intended. Therefore, internal controls are necessary for the effective and efficient operation of all levels of government. Internal controls are policies or procedures put in place to provide reasonable assurance that operations are achieving stated objectives. Properly designed and functioning controls help an entity adjust to ever-changing situations, changing demands, and varying threats and reduce the likelihood that significant errors or fraud will occur and remain undetected.

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. IT internal controls affect many aspects of financial operations and should be implemented and reviewed in conjunction with each office, department, or functional area of responsibility.

To execute responsibilities effectively, management needs to understand how an integrated internal control framework should work. Standards for Internal Control in the Federal Government "Green Book" (which may be found at https://www.gao.gov/products/D08784) may also be adopted by state and local governmental entities.

Assessing Risk

Each governmental entity has its own unique set of circumstances and risks that affect the design and implementation of internal controls. Before determining which controls should be implemented, entities should conduct a risk assessment to identify, analyze, and respond to risk potential, fraud, or errors occurring and remaining undetected.

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

Monitoring

Identifying risks and implementing effective controls will not protect assets and produce reliable financial information if management and employees do not 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 good solutions to an identified risk; however, once implemented, they may cause unforeseen problems or inefficiencies. At the same time, other activities may not appear to need controls, yet upon further analysis, some type of 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 two main types of control activities applicable to the IS environment. All IS controls throughout 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 in use by an entity operates as intended to produce properly authorized, reliable data when needed and that the entity is in compliance 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 confidentiality, completeness, and accuracy of accounting records 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 need to understand the technology 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 June 2019. Modification may include wording being re-ordered changed, or added.

BEST PRACTICES – GENERAL CONTROLS

IS Management

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

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

1-1.2: Conduct an overall risk assessment of the organization's goals, functions, and reputation to identify, monitor, and manage ongoing risks associated with the use of information technology. Gain an understanding of current practices. Involve end users in addressing these risks and mitigating negative impacts.

1-1.3: 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 as the operating environment changes.

1-1.4: Ensure that duties of software developers and end users are distinctly segregated and clearly documented.

1-1.5: Develop policies and procedures addressing non-business use of entity equipment, facilities, and Internet services.

1-1.6: Obtain proper replacement insurance for production hardware/equipment.

1-1.7: Develop and document database and network backup processes to include data and record retention periods, how often data are backed up, and how copies of backups will be maintained.

1-1.8: Assign and communicate database and network backup responsibilities to designated staff.

1-1.9: Establish access to an environmentally safe, geographically separate, and secure off-site location to retain database and network backups.

1-1.10: Establish and formally document frequency of backups, ensuring that minimum industry standards (i.e., daily, weekly, monthly, annually) are met. Backups should occur daily for critical processes or at longer intervals based on the significance of the information and rate of changes.

1-1.11: Establish and formally document the method of backup:

    a. Full Back up: 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 instant in time.

1-1.12: Ensure that the selected backup process and retention policy are in compliance with laws and regulations. Retention policy may include retaining periodic snapshots of all data backups in the event data become corrupted and contaminates the backup.

1-1.13: 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.).

1-1.14: Frequently test data backups to ensure data can be restored and is recoverable. Also, ensure backup settings are in compliance with entity policies.

1-1.15: Ensure administrator/super user accounts are limited and properly approved.

1-1.16: Regularly evaluate network availability and provide ongoing improvements to services and security as needed.

1-1.17: Establish and maintain a formal cybersecurity awareness program that ensures end users are aware of current cybersecurity threats, the importance of protecting assets, and the related risks.

1-1.18: Make employees aware of social engineering threats, which are attacks carried out by 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 to never open or download suspicious attachments.

1-1.19: Periodically host cybersecurity training for employees. Examples of relevant discussion and training topics include but are not limited to:

a. Table top 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 web sites.
g. Downloading files from the Internet or simply clicking links.
h. Embedded email links and downloading attachments that may appear reasonably valid.

Contract/Vendor Management

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

1-2.1: Conduct a risk assessment to identify risks associated with outsourcing IT services. Based on the results of the risk assessment, determine the appropriate course of action to respond to the identified risk.

1-2.2: Review all contract(s) prior to approval to ensure compliance with Ark. Code Ann. § 10-4-424 granting Arkansas Legislative Audit access and authority to audit computer applications supplied by vendors. Additionally, ensure business processes and any applicable legal requirements are adequately addressed and documented.

1-2.3: Establish a service level agreement for the maintenance and support of each contract, specifically defining performance expectations for each party.

1-2.4: Confirm that the vendor is a going concern. Ensure that provisions are made to hold application source code in escrow.

1-2.5: Limit vendor access to entity resources. Log access, monitor vendor activity, and review for appropriateness.

1-2.6: Vendors of cloud computing services or other types of 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 Service Organization Control Report (SOC), if available.

1-2.7: 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 security policy for the network that is clearly documented and formally approved. Ensure that policies describe potential security risks (identified in section 1-1.2) and are clearly communicated to users. Policies should be kept current through regular review and updated to address emerging security threats.

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

1-3.3: 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.

1-3.4: 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 that is inserted into hardware (e.g., USB and external hard drives). Ensure that the network security policy covers the use of external devices (e.g., USB drives, Smart Devices, etc.).

1-3.5: Establish a routine schedule for the performance of network vulnerability scanning, including review of critical risks identified and mitigated.

1-3.6: Conduct a risk assessment to identify risks associated with allowing remote access to entity resources. Gain an understanding of current practices for addressing these risks and mitigating negative impacts.

1-3.7: Develop remote access authentication policies and procedures and encryption protocols (considering the risks identified above). 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.

1-3.8: Establish encryption methods for sensitive data transmitted externally and across the network, including procedures for keeping protocols current.

1-3.9: Ensure that all IT administration duties outsourced to a vendor are evaluated for associated risks. Vendor access to your network should be restricted only 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.

1-3.10: 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.

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: Conduct a risk assessment to identify risks associated with the use of wireless networking. Gain an understanding of current practices for addressing these risks and mitigating negative impacts.

1-4.2: Establish security policies and procedures that ensure wireless usage restrictions, configuration, connection and password requirements, and implementation guidance for wireless access is appropriate. 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 clearly communicated to users.

1-4.3: 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 broadcasted.

1-4.4: Establish routine application of security patches for wireless access devices, ensuring that upgrades are applied as released.

1-4.5: Maintain an inventory of authorized access points (APs), and periodically conduct site inspections to determine that no unauthorized APs are in use.

1-4.6: Establish physical <u>security</u> controls over wireless <u>network</u> devices to prevent unauthorized access, such that all devices are secured with locking mechanisms or kept in a restricted area where access is granted to authorized personnel only.

1-4.7: Review perimeter (external) security established in section 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.

1-4.8: Ensure that entity-approved guest access <u>only</u> allows Internet <u>browsing</u>, require guest users to agree to terms of use, and 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 criticality of network devices and their physical placement. The policy should include access key/keycard management; authorization procedures for visitors, new employees, contractors, etc.; and provisions for <u>removing</u> access for terminated employees, consultants, security professionals, etc.

1-5.2: Ensure that the server room and <u>data processing areas</u> are adequately <u>restricted to authorized personnel</u> 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 detector.
    d. <u>Adequate ventilation and air conditioning systems</u>
    e. Uninterruptible power supply (UPS).
    f. Emergency power generator.
    g. Raised floor.
    h. Water detection.

1-5.5: Develop specific procedures to ensure that terminated employee access is immediately disabled and to control issuance/revocation of access keys/keycards. Conduct a key/keycard inventory to identify those with physical access to facilities and to determine that terminated employee access has been properly removed. If unauthorized access exists, rekey doors, and change security codes to reestablish proper authentication.

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

1-5.7: Ensure that any data storage device, workstations, or other mobile equipment no longer in operation are reformatted/wiped based on current data sanitization methodologies or the hard drive physically destroyed to minimize the risk of exposure. Any paper documents containing personally identifiable information that are no longer in use should be shredded to minimize the risk of exposure.

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 and document a Logical Access Security Policy, based on identified risk areas (identified in section 1-1.2), to protect high-risk system resources. The policy should establish user identification, authentication, and account control mechanisms as well as protect system administration tools and utilities from unauthorized access. Include provisions for monitoring of access security best practices to ensure policies remain current.

1-6.2:   Establish user security access on the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned duties in accordance with the entity's business process and functions.

1-6.3:   Establish security administration procedures that ensure proper authorization of changes and additions to user accounts. Include periodic review of user access security by resource owners (e.g., elected officials, directors, or their designees). Investigate questionable authorizations. Access to security administration and other sensitive system resources should be limited to only users with a documented business purpose; all unnecessary and unauthorized accounts (e.g., system/admin default, guest, terminated users, etc.) should be investigated to be removed or disabled.

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

    a.   User identification and password are required.
    b.   Users are systematically forced to change passwords on a periodic, recurring basis not more than 90 days.
    c.   Passwords are systematically required to be composed of a mixture of alpha and numeric characters and a minimum of 8 characters, with no repeating characters.
    d.   New users are forced by the system to change their initially assigned password.
    e.   A password history file systematically prevents reuse of at least the last five passwords.
    f.   The user account is locked after three unsuccessful logon attempts and remains locked until reset by an administrator or in a reasonable period of time.
    g.   Computer sessions timeout after a reasonable period of no activity, requiring user authentication to restore session.
    h.   Passwords are not revealed to anyone, including management, help desk personnel, security administrators, family members, or co-workers.
    i.   Management establishes and monitors user Security Event Log.

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

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

1-6.5:   Ensure that Security Event Logs are reviewed for violations. Document identified violations and associated corrective actions as a 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 both 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 lead to the entire network being compromised; administrative mode should be disabled by default or, at a minimum, protected with strong credentials and reserved for only when necessary to perform administrator functions.

Disaster Recovery/Business Continuity

1-7: **Disaster recovery/business continuity planning directly supports an organization's goal of continued operations. Organizations should develop a Disaster Recovery and Business Continuity plan so that the effects of a disaster will be minimized. Adequate planning addresses how to <u>maintain their status as a going concern</u>: keeping critical functions operating in the event of disruptions, both large and small.**

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 all critical 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 <u>for employees, vendors, etc.</u>
   e. <u>Ensures</u> manual operating procedures and resources <u>are in place in the event</u> IT operations are <u>unavailable</u>.
   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.

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

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

1-7.4: <u>At least annually</u>, conduct and document <u>rotating test scenarios</u> of the Disaster Recovery/Business Continuity Plan to the fullest extent possible. Document in sufficient detail and evaluate test results, modifying the plan if necessary.

Note: The Arkansas Continuity of Operations Program (ACOOP) provides a methodology, hardware, software, training, and user assistance for the development, maintenance, and testing of disaster recovery plans for Arkansas agencies, boards, commissions, school districts, counties, and cities. These plans are intended to ensure that essential services continue to be provided after any disruptive event. For more information: http://www.dis.arkansas.gov/arkansas-continuity-of-operations-program-acoop

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: After reviewing the following Application Control Best Practices, conduct a risk assessment to identify risks associated with the core financial applications in use. Gain an understanding of current practice for addressing these risks and mitigating negative impacts, through either enhancing automated controls or adding compensating controls to the existing processes.

2-1.2: Ensure that a properly designed database has been established to reduce redundancies and ensure effective transaction processing. Poor data quality may lead to failure of system controls, process inefficiencies, and/or inaccurate reporting.

[Example: The County Financial Manual may supply the data structure incorporated into the automated system and 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.

2-1.3: 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 done in a controlled manner (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 as they happen by tracking transactions 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 exception resolution monthly 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: Based on risk assessment, establish necessary controls over data processing (both automated and manual).

2-2.2: Ensure that processing errors are identified, logged, and resolved and that incorrect information is identified, rejected, and corrected for subsequent processing. Edit reports should be produced by the system at critical processing stages to provide a means 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 transaction or table logs should be available to compare to source documents.
    b. Processing logs should be available to identify incompletely 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.

2-2.3:   Management should have <u>policies</u> 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:

    a.   Ensure that data input <u>controls are in place</u> (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.   Require data exception resolution <u>before year-end closing</u>.

2-2.4:   Establish procedures to ensure that periodic and <u>timely</u> reconciliations and <u>error correction</u> are performed between the subsidiary and general ledgers.

2-2.5:   Establish monitoring procedures to include:

    a.   Reconciling data inputs to data processed.
    b.   <u>Maintaining</u> a processing log and review for unusual or unauthorized activity.
    c.   Monitoring all overrides to transactions.

2-2.6:   Ensure that the software/application has the capability to prevent alteration of data when they are transferred from one process to another.

2-2.7:   Ensure that the application has the capability to resume processing at the point of interruption.

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

2-3.1:   Based on risk assessment, establish necessary controls over data output (both automated and manual).

2-3.2:   Develop procedures for system output and reporting to ensure:

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

2-3.3:   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.

2-3.4:   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 assure the integrity of production data and transaction processing. Reviews should be performed <u>timely</u> and periodically.

Application-Level General Controls

Application Security Management

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

2-4.1: Based on risks identified in section 2-1.1, 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. See 1-6.2
    c. Outlines ongoing security role management (including monitoring and maintenance procedures).
    d. Addresses the roles, responsibilities and monitoring of third party vendors.
    e. Ensures that 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.
    g. Addresses encryption of application data (including authentication credentials), both stored and transmitted.
    h. Establishes procedures for documenting security and verification of data for both internal and external system interfaces.
    i. Coordinates with overall network security policy.
    j. Analyzes application deficiencies and document 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 section 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. Setup of 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 section1-5.

Application Configuration Management

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

2-5.1: Based on risk assessment, 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 a basic internal control that attempts to ensure that no single individual has the authority to execute two or more conflicting transactions.**

2-6.1: Ensure that <u>management has</u> identified and documented 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. <u>See 1-6.2</u>.

2-6.2: Small governments with limited staff and resources have a reduced capacity to segregate duties. Therefore, it may not be practical or cost-effective to segregate conflicting duties in these cases. 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 are appropriately controlled.

    a. Access to incompatible activities is assigned only when supported by a business need.
    b. User access authorizations are <u>periodically</u> reviewed by management for segregation of duties conflicts, considering position, process changes, and updating access to current job assignments.
    c. Users with segregation of duties conflicts are documented, and their activity is monitored and <u>reviewed periodically</u> via transaction and audit logs.
    d. Management retains documentation that segregation of duties risk has been mitigated through effective <u>compensating</u> controls.
    e. A segregation of duties grid is developed by 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 key 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 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 section 2-7.1. Incorporate the application-level contingency planning and procedures (including backup policy) into the organization's Disaster Recovery/<u>Business Continuity</u> Plan.

2-7.4: Provide for periodic testing of the application contingency planning. Include documentation of test <u>scenario</u> results and corrective actions (including resulting changes to the plan) to be incorporated into organization-wide Disaster Recovery/<u>Business Continuity</u> 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 signatures or digital signatures are used, management must understand the technology and associated risks. Develop and implement controls to address risks identified, 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. Electronic signatures, on the other hand, 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.

Payment Cards (Debit or Credit)

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

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

5-1.2: Ensure 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: Remove all entity information from your device and return it to the manufacturer's settings before you sell, exchange, or dispose of your device.

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 rules of behavior for the use of personally-owned devices. This policy must be adhered to in order to access organizational resources.

Electronic Banking, Electronic Commerce and other Electronic Transfer of funds

6-1: **Electronic banking and other electronic funds transfer (EFT) enables 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., initiator cannot be an approver, etc.).
    b. Online banking and EFT activities utilized.
    c. Personnel who initiate 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 application/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 not available, entities must be able to reduce online banking risks to an acceptable level through a combination of other controls.

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

6-1.4: Ensure all updates and patches to operating systems, and hardware drivers are applied timely.

6-1.5: Install firewalls and intrusion detection and prevention systems with continuous monitoring. Any unauthorized and/or suspicious behavior or traffic should be investigated and, if necessary, blocked using access control lists in conjunction with a firewall.

6-1.6: Employ multi-factor authentication, if possible. Require unique login ids and complex passwords, and ensure computers and browsers are configured to not save passwords. Keep passwords confidential.

6-1.7: Limit Internet access to only business-related programs. Frequently delete browsing history, temporary Internet files, and cookies. In the event the system is compromised, minimal information would be captured by a hacker or malware program.

6-1.8: Check that the session is secure (minimum 128-bit SSL encryption) before undertaking any online banking.

6-1.9: Monitor and reconcile bank accounts daily (when feasible).

6-1.10 Periodically (daily, weekly, monthly) review accounts for unauthorized or suspicious activity, and report immediately.

6-1-11: Ensure written agreements with banks and/or other payment solutions are reviewed by legal counsel.

6-1.12: Ensure written agreements with banks provide appropriate controls for all electronic fund or wire transfers.

6-1.13: Ensure computer is disconnected from the Internet by unplugging the Ethernet/DSL cable when not in use.

6-1.14: Employ dual-authorization of transactions, enforced by bank security where possible (requiring at least two user accounts to submit and approve electronic transactions).

6-1.15: 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.

6-1.16: When possible, implement use of out-of-band transaction verification (such as text message or other security message 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.

6.1.17: Ensure that blank check stock, signature stamps, and facsimile signatures are properly safeguarded with inventory control.

6-1.18: Use a clearing bank account when paying electronically rather than paying directly from primary account.

6-1.19: Establish transaction and daily limits to lower loss potential.

6-1.20: Consider the cost benefit of obtaining cybersecurity and data breach insurance.

6-1.21: Restrict browser(s) to sites necessary for EFT.

6-1.22: Ensure that users performing banking transactions use only non-administrative user accounts.

6-1.23: Implement use of fraud controls, when possible and feasible, to ensure that the bank only processes authorized transactions. Features to consider include:

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

6-1.24: Implement use of processing calendar with the bank, if possible, to ensure the bank only processes transactions on pre-determined days throughout the year.

6-1.25: Comply with all security requirements outlined in the service level agreement with the bank and all other prudent security measures.

6-1.26: Allow electronic delivery of statements and account information. Ensure any statements or documents containing account information are properly maintained.

6-1.27: Never share any confidential information, tax IDs, Social Security numbers, or account numbers via email.