City of Keiser Ordinance No. 2023-0[illegible]

An Ordinance Adopting Electronic Banking, Electronic Commerce and other Electronic Transfer of funds 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 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 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.

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.

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

Section 28: Authorized Vendors to Pay - The following vendors are approved and authorized to receive payments via online payments. No payments shall be made to any vendor not listed. If a new vendor is identified for payment both the Ordinance and Policies and Procedures MUST be updated to indicate the new vendor.

- American Express
- Entergy
- Ritter Communications
- Lowe's
- Black Hills Energy

Section 29: EMERGENCY CLAUSE
In accordance with Section 14 of the Arkansas Constitution, an emergency is hereby declared to exist, and this ordinance is necessary for the immediate preservation of the public peace, health, and safety. Therefore, this ordinance shall be in full force and effect immediately upon its passage and approval.

Rick Creecy, Mayor

Peggy Sellars, Recorder/Treasurer