CITY OF WARD
RESOLUTION R-2025-08

A RESOLUTION ADOPTING A CYBERSECURITY POLICY FOR THE CITY WARD IN COMPLIANCE WITH ACT 843 OF 2023; AND FOR OTHER PURPOSES

WHEREAS, ACT 846 OF 2023, ENACTED BY THE ARKANSAS GENERAL ASSEMBLY and codified at Arkansas Code Annotated (A.C.A.) § 21-2-804 et. seq., requires all municipalities to establish a minimum cybersecurity policy for the city.

WHEREAS, establishment of a Cybersecurity Police is mandatory to be covered under the state's Cybersecurity Trust Fund which may be used to offset the costs of exploitation of

WHEREAS, THE ARKANSAS MUNICIPAL LEAGUE has created a sample Municipal Cybersecurity Policy for cities to follow. The modified Policy is attached.

NOW THEREFORE, BE IT RESOLVED BY THE WARD CITY COUNCIL THAT:

SECTION 1: The City hereby adopts the attached Cybersecurity Policy as outlined on the attached

SECTION 2: The City hereby adopts a disciplinary procedure for violations of the Cybersecurity policy, which shall be incorporated into the City's employee handbook and enforced accordingly.

SAID RESOLUTION WAS ADOPTED ON 2-17-26.

Voice Vote: YEAS: 5 NAYS: Ø OR;

Roll Call Vote: YEAS: _____ NAYS: _____ Mayor (if needed) _____

Brooke _____, Chapman _____, Hall _____, Hefner _____, McMinn _____, Ruble _____

APPROVED:

Charles Gastineau, Mayor

ATTEST:

Krystal Rummel, City Clerk

CITY CLERK
Ward
CITY OF WARD, ARKANSAS

CITY OF WARD, ARKANSAS
CYBERSECURITY POLICY[1]

1. **PURPOSE:** This policy establishes the minimum cybersecurity requirements for municipalities based on the standards created by the Arkansas Cyber Response Board (ACRB) pursuant to Act 846 of 2023. It also incorporates recommendations by the Arkansas Legislative Audit's (ALA) Information Services Best Practices (2024). These standards are designed to enhance the security posture of the City of Ward Information Systems and data while complementing existing internal controls.

2. **SCOPE:** This policy applies to all employees, contractors, and third-party service providers who access municipal systems, networks, or data. It covers authentication, data protection, training, access control, patch management, and governance practices.

3. **POLICY STATEMENT:** The City of Ward (hereinafter "The City") shall comply with the following cybersecurity standards and best practices:
    a. Multifactor Authentication (MFA)
        i. All employees with access to vital systems and services shall use multifactor authentication (MFA). This includes:
            1. Access to web-based platforms such as financial services (e.g., online banking, investment portals), cloud-based applications, and webmail services (e.g., Gmail, Outlook.com).
            2. Accounts with elevated privileges, including administrative, cloud service, and vendor system accounts (both on-premise and cloud-based).
            3. Accounts used to manage application user security.
        ii. Service accounts are exempt from MFA requirements.
        iii. Responsible Role: Pure Computer Solution[2]

    b. Offline Data Backups
        i. The city shall maintain offline backups of critical systems and data. These backups shall be tested at least once monthly to ensure integrity and recoverability.
        ii. Responsible Role: Pure Computer Solution
            1. Documentation: Maintain a backup schedule, test logs, and restoration verification reports. Include date, system tested, outcome, and responsible personnel. Store in the Disaster Recovery documentation folder.

---

[1] Implemented via Resolution R-2026-08

[2] Pure Computers Solution is the city's contracted IT Consultant

c. Cybersecurity Awareness Training
    i. All employees shall complete annual cybersecurity awareness training. The training should include topics such as phishing prevention, password hygiene, secure data handling, and incident reporting procedures. OR
    ii. All employees shall complete monthly cybersecurity awareness training. The training should include topics such as phishing prevention, password hygiene, secure data handling, and incident reporting procedures.
    iii. Responsible Role: Human Resources Manager in coordination with the IT Consultant.
        1. Documentation: Maintain a training roster with employee names, completion dates, and training modules covered. Store digitally in HR compliance records and back up in the IT audit folder.

d. Password Management Standards
    i. Passwords are a critical part of network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees of the city are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times. The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.
    ii. Passwords should not be based on a user's personal information or that of his or her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.
        1. Minimum password length of 12 characters (strongly recommended). OR
        2. Passwords with 12 or more characters may be changed every 185 days.
    iii. Passwords shall not be stored in plaintext.
    iv. Enforce password complexity requirements (combination of uppercase letters, lowercase letters, numbers, and special characters).
    v. Prevent reuse of the last 24 passwords or phrases.
    vi. Lock user accounts after five unsuccessful login attempts.
    vii. Default passwords for new users shall require a forced reset upon first login.

viii. Responsible Role: Pure Computer Solution
    1. Documentation: Maintain system policy configuration screenshots and audit logs showing password policy enforcement. Include change history and lockout reports. Store in the access control documentation archive.

4. Patch Management Standards
    a. The city shall maintain a patch management process that includes:
        i. Applying critical updates and patches within 14 days of release.
        ii. Applying all other updates and patches within 30 days.
        iii. Obtaining patches, upgrades, and vendor releases only from trusted sources.
        iv. Conducting periodic audits to identify and remediate systems and appliances missing updates.
    b. Responsible Role: Pure Computer Solution
        i. Documentation: Maintain a patch log detailing system, patch ID, date applied, and source. Include audit reports and remediation actions. Store in the Patch Management folder under IT operations.

5. Compliance and Review
    a. This policy shall be reviewed annually and updated as necessary to reflect changes in technology, emerging threats, and regulatory requirements. Non-compliance may result in disciplinary action and could affect participation in the Arkansas Self-Funded Cyber Response Program. Additionally, it may trigger legal or regulatory consequences.

6. Policies Based Upon Arkansas Legislative Audit Information Systems Best Practices:
    a. The city adopts the following best practices recommended by the Arkansas Legislative Audit's Information Systems Best Practices:

7. Governance and Oversight
    a. Pure Computer Solutions (PCS) of Cabot[3] is designated as the responsible party for cybersecurity oversight.
    b. It is the responsibility of the position designated above to conduct regular IT risk assessments to identify and mitigate vulnerabilities
    c. Review and update user access rights quarterly.
    d. Disable inactive user accounts after 30 days of inactivity.
    e. The Director, Human Resources (HR) is designated as the IT Director as an additional duty.
        i. It is the responsibility of the position designated above to ensure that the IT policies and procedures and documented.

[3] Pure Computer Solution is the contracted IT source for the City of Ward governance

ii. Implement role-based access controls to ensure users have only the permissions necessary for their roles.
iii. Documentation: Maintain signed policy documents, risk assessment reports, and meeting minutes. Store in the Governance and Compliance folder or as appropriate.

8. Access Controls
    a. Responsible Role: Pure Computer Solution
        i. Documentation: Maintain access review logs, user access matrices, and deactivation reports. Store in the Access Management archive.

9. Acceptable Use
    a. All uses of information and information technology resources must comply with city policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including federal, state, local and intellectual property laws.
    b. Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:
        i. Understanding the baseline information security controls necessary to protect confidentiality, integrity, and availability of information.
        ii. Protecting city information and resources from unauthorized use or disclosure.
        iii. Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure.
        iv. Observing authorized levels of access and using only approved IT technology devices or services; and
    c. Immediately reporting suspected information-security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

10. Unacceptable Use
    a. The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities, after approval from city management, in consultation with city IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).
    b. Unacceptable use includes, but is not limited to, the following:
        i. Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information.
        ii. Unauthorized use or disclosure of information and resources.
        iii. Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening,

obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.

iv. Attempting to represent the city in matters unrelated to official authorized job duties or responsibilities.
v. Connecting unapproved devices to the city's network or any IT resource.
vi. Connecting city IT resources to unauthorized networks.
vii. Connecting to any wireless network while physically connected to the city's wired network.
viii. Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with city policies.
ix. Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (Counties must recognize the inherent risk in using commercial email services as email is often used to distribute malware).
x. Using a city's IT resources to circulate unauthorized solicitations or advertisements for non-city purposes including religious, political, or not-for-profit entities.
xi. Providing unauthorized third parties, including family and friends, access to the city's IT information, resources or facilities.
xii. Using organization IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions).
xiii. Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using city IT resources; and
xiv. Tampering, disengaging, or otherwise circumventing an city or third-party IT security controls.

11. Occasional and Incidental Personal Use
    a. Occasional, incidental and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the city's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment about occasional and incidental personal use is important. The city may revoke or limit this privilege at any time.

12. Individual Accountability
    a. Individual accountability is required when accessing all IT resources and city information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure.

Credentials must be treated as confidential information and must not be disclosed or shared.

13. Restrictions on Off-Site Transmission and Storage of Information
    a. Users must not transmit restricted city, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct the city's business unless explicitly authorized. Users must not store restricted city, non-public, personal, private, sensitive, or confidential information on a non-city issued device, or with a third-party file storage service that has not been approved for such storage by the city.
    b. Devices that contain city information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

14. User Responsibility for IT Equipment

a. Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the city and must be immediately returned upon request or at the time an employee is separated from the city. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the city. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The city has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

b. Responsible Role: ALL IT USERS

15. Asset and Configuration Management
    a. Maintain an up-to-date inventory of all hardware and software assets.
    b. Establish and enforce configuration baselines for all systems.
    c. Restrict installation of unauthorized software.
    d. Responsible Role: IT Asset Manager, Finance, or Clerk
        i. Documentation: Maintain asset inventory spreadsheets, configuration baseline documents, and change logs. Store in the Asset Management system and back up quarterly.

16. Network Security
    a. Deploy firewalls and intrusion detection/prevention systems.
    b. Segment networks to isolate sensitive systems and data.
    c. Encrypt sensitive data both in transit and at rest.
    d. Responsible Role: Pure Computer Solution
        i. Documentation: Maintain access review logs, user access matrices, and deactivation reports. Store in the Access Management archive.

17. Incident Response
    a. Develop and maintain a formal incident response plan.
    b. Conduct annual tests of the incident response plan through tabletop exercises or simulations.
    c. Log and retain security events for a minimum of 90 days.
    d. Responsible Role: IT Director
        i. Documentation: Maintain the incident response plan, test results, and incident logs. Store in the Incident Response binder and digital archive.

18. Physical Security
    a. Restrict physical access to servers, networking equipment, and other critical infrastructure.
    b. Implement surveillance and access logging for data centers and server rooms.
    c. Responsible Role: IT Director
        i. Documentation: Maintain access logs, surveillance footage retention policies, and physical access review reports. Store in the Physical Security folder.

19. Vendor and Third-Party Management
    a. Require vendors and third-party service providers with access to the city's intranet to comply with municipal cybersecurity standards.
    b. Review third-party access and contracts annually to ensure continued compliance.
    c. Responsible Role: IT Director
        i. Documentation: Maintain vendor compliance checklists, signed agreements, and access logs.

20. Business Continuity and Disaster Recovery
    a. Maintain a documented disaster recovery plan.
    b. Test recovery procedures annually to ensure effectiveness.
    c. Ensure critical systems can be restored within acceptable timeframes.
    d. Responsible Role: IT Director
        i. Documentation: Maintain the disaster recovery plan, test results, and recovery time objective (RTO) metrics. Store in the Continuity Planning archive.

21. Compliance and Review
    a. This policy shall be reviewed annually and updated as necessary to reflect changes in technology, emerging threats, and regulatory requirements. Non-compliance may result in disciplinary action and could affect participation in the Arkansas Self-Funded Cyber Response Program. Additionally, it may trigger legal or regulatory consequences.
    b. Responsible Role: Mayor and IT Director

22. Employee Acknowledgment of Cybersecurity Policy

a. **I acknowledge that I have received, read, and understand the city's Cybersecurity Policy.**
b. **I understand that it is my responsibility to comply with it to protect the security and integrity of the city's information systems and data.**
c. **I further acknowledge that failure to comply with this policy may result in disciplinary action, up to and including termination of employment.**

Employee Name (Printed): _____

Employee Signature: _____

Date: _____