ARKANSAS
MUNICIPAL
LEAGUE

SECURITY RECOMMENDATIONS & INCIDENT REPORTING REQUIREMENTS

ARKANSAS SELF-FUNDED CYBER RESPONSE PROGRAM

CYBER RESPONSE CONTACT

JEFF MELTON | DIRECTOR, INFORMATION TECHNOLOGY | ARKANSAS MUNICIPAL LEAGUE
CELL: 501.353.4048 | OFFICE: 501.978.6106 | EMAIL: JMELTON@ARML.ORG

Rev. 11.25

ARKANSAS SELF-FUNDED
CYBER RESPONSE PROGRAM

Arkansas Act 846 of 2023, A.C.A. § 19-5-1159, created the mandatory Arkansas Self-Funded Cyber Response Program. Arkansas municipalities are required to participate in the program, which provides coverage for damages/losses caused by a cyberattack committed against a participating government entity. The Arkansas Cyber Response Board (ACRB) will determine coverage for actual losses to an amount not to exceed $100,000. There is a $1,000 deductible.

- The following pages contain information about the ACRB, initial, required steps to take in the event of a cyberattack and minimum cybersecurity standards.
- As required by Act 846, the ACRB developed an initial set of minimum cybersecurity standards for covered entities. Details of these standards will be emailed directly to mayors, city managers and IT directors.
- Additional benefits are available for member cities and towns that participate in the Arkansas Municipal League's Municipal Property Program.
- To learn more about the Arkansas Self-Funded Cyber Response Program, please contact Jeff Melton at jmelton@arml.org.

POLICY LIMIT

The policy limit is $100,000 per occurrence for entities that comply with published standards and *$50,000 for entities that do not comply for claims reported on or after July 1, 2024. A $1,000 per occurrence deductible will apply.

** The Arkansas Cyber Response Board will determine on a claim by claim basis whether or not the reduced limit will apply to the affected Participating Governmental Entity.*

CLAIMS

All claims must be called in to the Arkansas Division of Emergency Management State Watch office at: 501-683-6705 or 501-683-6709 or **aswo@adem.arkansas.gov.**

No coverage is provided for compensatory damages, punitive damages, exemplary damages, ransom demands or any interest or penalty amounts that accrue on a claim.

CYBER RESPONSE CONTACT

JEFF MELTON | DIRECTOR, INFORMATION TECHNOLOGY | ARKANSAS MUNICIPAL LEAGUE
CELL: 501.353.4048 | OFFICE: 501.978.6106 | EMAIL: JMELTON@ARML.ORG

ACRB MINIMUM CYBERSECURITY STANDARDS

The Arkansas Cyber Response Board (ACRB), established under Act 846 of 2023, has established minimum cybersecurity standards for entities in the Arkansas Self-Funded Cyber Response Program. As the cybersecurity landscape evolves, the ACRB's standards will adapt to address new challenges and threats.

Effective July 1, 2025, all participating entities must comply with these standards. It's important to note that these standards, while not exhaustive, are not intended to replace existing security policies and procedures. Organizations should continue to rely on their internally developed controls to ensure comprehensive security, while these standards provide additional safeguards.

1. Enforce multifactor authentication (MFA) across all employees with access to vital systems and services, including:

- Access to web-based platforms includes services provided by financial institutions, such as online banking and investment management, and third-party applications like cloud-based software solutions. This category also encompasses webmail services, such as Gmail and Outlook.com, or any other web-based platform that allows users to perform various transactions, including initiating financial transfers, authorizing payments, updating account information, and submitting confidential data.
- Multi-factor authentication (MFA) is required for all accounts with elevated access rights, including administrative, cloud service, and vendor system accounts (on-premise and cloud). This requirement also applies to accounts used to manage application user security. Service accounts are exempt from this requirement.

2. Maintain and test offline data backups (at least once yearly) for critical systems and data storage.

3. Implement a cybersecurity awareness training program for all employees.

4. Adhere to the ACRB password standard:

- Minimum of 8 characters (Strongly recommend 12 characters).
- Changed every 90 days (Passwords with at least 12 characters changed every 185 days).
- Not stored in plaintext.
- Enforce password complexity.
- Prevent the reuse of at least the last 24 passwords/phrases.
- The user account is locked after five unsuccessful attempts.
- Default passwords for new users must require a forced reset.

5. Adhere to the ACRB patch management standard:

- Ensure critical updates and patches to systems and hardware are applied within 14 days
- Ensure all other updates and patches to systems and hardware not designated as essential are applied within 30 days
- Patches, system upgrades, or other vendor releases must be obtained from trusted sources
- Periodic auditing and remediation of systems and appliances missing updates

Exceptions to Cybersecurity Standards

The ACRB may grant exceptions to these standards on a case-by-case basis, subject to thorough review and justification provided by the participating entities. Such exceptions must be based on compelling reasons such as technological limitations, resource constraints, or specific operational requirements. All exceptions granted shall be documented and periodically reassessed for compliance with evolving cybersecurity best practices and regulatory mandates.

CYBER INCIDENT CHECKLIST

Upon detection, please follow the required steps outlined below to report all cyber incidents and events. Prompt reporting serves to reduce cost and extent of loss.

REQUIRED STEPS

Immediately Notify:
- Jeff Melton, Arkansas Municipal League
  jmelton@arml.org or 501-353-4048

Within 48 Hours of Incident, Notify:
- ADEM Watch Office
  aswo@adem.arkansas.gov
  501-683- 6705 or 501-683-6709

Within 5 Business Days of Incident, Notify:
- Arkansas Legislative Audit
  https://incident.arklegaudit.gov/

Incidents that are not reported to the cyber response contact and ADEM within 48 hours of detection may result in increased mitigation cost to the participating governmental entity.

Additionally:
- Cooperation, assistance, submission, execution, consent, etc., with the cyber response contact is mandatory.
- Failure to submit requested information to the cyber response contact may result in increased mitigation cost to the participating governmental entity.
- Claim checks must be cashed within 90 days.

RECOMMENDED STEPS

Notify Internet Crime Complaint Center (IC3)
- https://www.ic3.gov/

Notify Cybersecurity Infrastructure Security Agency
- Helen “Gayle” Combs
  helen.combs@mail.cisa.dhs.gov
  479-866-8691

Notify FBI Little Rock Office
- SA Christopher Carter or SSA Tonja Sablatura
  LR_CTF@ic.fbi.gov
  501-221-9100

CYBER RESPONSE CONTACT

JEFF MELTON | DIRECTOR, INFORMATION TECHNOLOGY | ARKANSAS MUNICIPAL LEAGUE
CELL: 501.353.4048 | OFFICE: 501.978.6106 | EMAIL: JMELTON@ARML.ORG

GOOD (MINIMUM) PROTECTION RECOMMENDATIONS

- Incident Response Plan and Disaster Recovery Plan – Arkansas Act 260
- Develop formal policies and specify controls to ensure compliance
- Quarterly Security Awareness Training
- Business class email: .gov preferred or .org, .com, .net
- Managed Detection and Response (MDR): Leverage AI and SOC
- Least Privilege Access Model
- Multi-Factor Authentication (MFA) for all web-based applications
- Patch Management: workstations, servers, network devices
- Remote Access Policy: RDP and VPN connections with the addition of MFA
- Backup Policy: offline backup with Ransomware prevention
- Firewall: network and host-based firewalls

BETTER PROTECTION RECOMMENDATIONS

- Annual Incidence Response Plan and Disaster Recovery Plan – walk through
- Address vetting and oversight of external solutions and providers
- Establish a secure baseline configuration – implement CIS controls
- Email Tagging: alert end user email is from external sender
- Email content and delivery: filter all inbound messages for malicious content (Domain-Based Message Authentication, Routing and Conformance (DMARC))
- Web Browser Filtering
- Monthly email phishing campaigns / tests

BEST PROTECTION RECOMMENDATIONS

- Protective DNS (Malicious Domain Blocking and Reporting: MS-ISAC - https://mdbr.cisecurity.org/)
- Centralized Log Monitor: Security Information and Event Monitoring (SIEM)
- Network Segmentation and Segregation: control access and/or traffic flow within network environment
- Implement Zero Trust Model
- Multi-Factor Authentication MFA for all administrative tasks
- Vulnerability Scanning and Threat Hunting
- Develop Vendor Contracts

CYBER RESPONSE CONTACT

JEFF MELTON | DIRECTOR, INFORMATION TECHNOLOGY | ARKANSAS MUNICIPAL LEAGUE
CELL: 501.353.4048 | OFFICE: 501.978.6106 | EMAIL: JMELTON@ARML.ORG