Year 1 Minimum Cybersecurity Standards Recommendations
Cyber Response Board

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.