Act 504 Policy Summary (DRAFT)

Disclaimer: This document is an incomplete, condensed view of the Act 504 Cybersecurity Policy. Refer to the original policy documents and Arkansas Act 504 for full details and requirements.

The National Institute of Standards and Technology (NIST) published 20 controls (SP800-53/53B). As required by the SCSO, the Cybersecurity Policy is written to the moderate level of these NIST SP800-53 control families.

NIST Reference Tool

AC	- Access Control
AT	- Awareness and Training
AU	- Audit and Accountability
CA	- Assessment, Authorization, and Monitoring
CM	- Configuration Management
CP	- Contingency Planning
IA	- Identification and Authentication
IR	- Incident Response
MA	- Maintenance
MP	- Media Protection
PE	- Physical and Environmental Protection
PL	- Planning
PM	- Program Management
PS	- Personnel Security
PT	- Personally Identifiable Information Processing and Transparency
RA	- Risk Assessment
SA	- System and Services Acquisition
SC	- System and Communications Protection
SI	- System and Information Integrity
SR	- Supply Chain Risk Management

Common to All 20 Policies

- Controls shall be documented in accordance with NIST 800-53 Moderate and any applicable federal regulations and state laws.
- Reviews and updates to the current policies will occur according to the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet.

Access Control

- Access to information systems will only be provided to users based on business requirements, job function, responsibilities, need-to-know and least privilege.
- Requests for access will be formally documented and appropriately approved.
- Application and service accounts must only be used by the components requiring authentication.

Awareness and Training

- Establish, document and maintain a security awareness training program that:
  - incorporates all applicable regulations, State and Federal laws;
  - provides role-based training;
  - is performed prior to the authorization of system access;
  - is monitored and tracked.
- For regulated data areas (e.g., Centers for Medicare & Medicaid Services, Criminal Justice Information Services, Federal Tax Information), the State Cybersecurity Office (SCSO) considers all employees as requiring the same level of security awareness training.

Audit and Accountability

- Access to information systems and data, as well as significant system events, must be logged by the information system.
- Information system audit logs must be protected from unauthorized access or modification.
- Information system audit logs must adhere to a documented retention process. Audit logs must be in compliance with the regulatory requirements found in the State Cybersecurity Office (SCSO) Regulatory Settings spreadsheet. Audit logs that have exceeded this retention period should be destroyed.

Assessment, Authorization, and Monitoring

- Develop a security assessment and authorization plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- Document and maintain the authorization of system interconnections with Interconnection Security Agreements (ISA).
- Establish and implement a continuous monitoring program.

- Internal system connections must be authorized and documented.

Configuration Management

- A baseline for system configurations must be documented.
- Systems must only be configured with least functionality.

Contingency Planning

- Contingency plans must be documented for information systems that are mission critical to public and state entities.
- The plans must provide preventive measures, recovery strategies, and technical considerations in the event of a disruption.
- Contingency plans must include the following:
    - Procedures for restoring the information system, including the acquisition and maintenance of resources needed to facilitate the recovery and/or continuity of essential system functions;
    - Processes for acquiring and maintaining the resources necessary to ensure viability of the restoration procedures;
    - Training for personnel to execute contingency procedures;
    - Assignment of responsibilities to designated staff or positions involved in the execution of the plan; and
    - Readiness and preparedness procedures for the annual review and testing of the plan.

Identification and Authentication

- Access to information systems will only be provided to users and devices when successfully identified and authenticated.
- Requests for identification will be formally documented and appropriately approved.
- Devices must only be used by the components requiring authentication.

Incident Response

- All public and state entities must report to the CISO or designee any information security incident or event that has the potential to negatively impact the confidentiality, integrity, or availability of any information system that stores, processes, or transmits public and state entity information.
    - Information security incident reporting and its timeliness must be determined by risk and regulatory requirements.
    - Unsuccessful security incidents are foreseeable and expected, are not required to be reported, but may be reported if any uncertainty exists. Unsuccessful security incidents include, but are not limited to, pings on a

firewall, unsuccessful attempts to log onto a system with an invalid password or username, unsuccessful attempts to load malware, denial-of-service attacks that do not result in a server being taken off-line, and other events that do not result in actual impermissible use, disclosure, access or acquisition of public and state entity information resources or a substantial risk thereof.

- The CISO or designee must direct information security incident responses and investigations in coordination and collaboration with the affected system owners.
- The CISO or designee must be responsible for coordinating with any required external entities the reporting of information security incidents, such as regulators, Arkansas Attorney General, Arkansas Legislative Audit, contractual counterparties, affected data owners, or others as determined by the State Cybersecurity Office.

Maintenance

- Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or requirements conducted by the State Cybersecurity Office, local IT, and/or outsourced IT entities.
- Approve and monitor all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.
- Ensure that system owners and IT approve, control, and monitor information system maintenance tools.
- Approve and monitor non-local maintenance and diagnostic activities.
- Document in the security plan for the information system, the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.
- Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

Media Protection

- Organizational media must be labeled indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.
- Media must be protected until it is destroyed or sanitized using approved equipment, techniques, and procedures.
- Limit the transport of information system media to authorized personnel.

Physical and Environmental Protection

- The data center information assets of public and state entities shall be protected from tampering, damage, theft, or unauthorized physical access.
- Environmental controls shall be established, monitored, and maintained to prevent damage or failure.
- Data center utilities services of public and state entities shall be secured, monitored, and maintained to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.

Planning

- System Security Plans shall be developed for all systems.
- Establish rules of behavior that include responsibilities and expected behavior regarding system usage.
- Develop information security architecture that facilitates a defense-in-depth approach for organizational protection.

Program Management

- Establish, document, and maintain the requirements for the security program.

Personnel Security

- Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, guidance, and specific criteria established for the risk designations of assigned positions.
- Develop and document access agreements for information systems.
- Ensure that individuals requiring access to information and information systems sign appropriate access agreements prior to being granted access.
- Require third-party providers to comply with personnel security policies and procedures established by the entity.

Personally Identifiable Information Processing and Transparency

- Establish, document, and maintain requirements for personally identifiable information processing and transparency that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with data center policies and standards.

Risk Assessment

- Organizational risk must be identified, continuously monitored, and controlled.
- Risk assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to public and state entities.

- Applicable security requirements will be monitored for updates and risk reassessed within public and state entities when published.

System and Services Acquisition

- Determine, document, and allocate the resources required to protect the information systems as part of the capital planning and investment control process.
- The system development life cycle must include information security risk management processes.
- Public and state entities shall manage information systems using the system development life cycle to ensure incorporation of information security considerations.
- The acquisition process must include security requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service.
- Require that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with data center policies, standards, and procedures.

System and Communications Protection

- Organizational communications must be monitored, controlled, and protected (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Secure architectural designs, software development techniques, and systems engineering must be used within organizational information systems.
- Subnetworks for publicly accessible system components must be physically or logically separated from internal networks.
- Cryptographic mechanisms must be utilized to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical safeguards.

System and Information Integrity

- Identify, report, and correct information system flaws.
- Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
- Monitor the information system to detect attacks, indicators of potential attacks, unauthorized local, network, and remote connections.
- Generate internal security alerts, advisories, and directives as deemed necessary.

- Ensure the integrity of software, firmware, and information.

Supply Chain Risk Management

- Identify information security requirements for the information system or information system service in mission/business process planning.
- Protect the information system or information system service as part of the capital planning process.

NIST Glossary

Glossary | CSRC (nist.gov)