

ARKANSAS REGISTER

Proposed Rule Cover Sheet



Secretary of State
John Thurston
500 Woodlane Street, Suite 026
Little Rock, Arkansas 72201-1094
(501) 682-5070
www.sos.arkansas.gov



Name of Department _____

Agency or Division Name _____

Other Subdivision or Department, If Applicable _____

Previous Agency Name, If Applicable _____

Contact Person _____

Contact E-mail _____

Contact Phone _____

Name of Rule _____

Newspaper Name _____

Date of Publishing _____

Final Date for Public Comment _____

Location and Time of Public Meeting _____

Notice of Rulemaking

Pursuant to Arkansas Code Annotated § 25-15-201 et seq., notice is hereby given that the Arkansas Department of Transformation and Shared Services is considering a repeal of the following Rules: Rule 2014-1 State Employee Dispute Resolution Appeal Rules and Procedures; Standard Statement – Data and System Security; Standard Statement – Domain Name Service (DNS) Resolution; Standard Statement – Machine Readable Privacy Policy; Standard Statement – Physical and Logical Security; Standard Statement – Spyware Scanning; and Standard Statement – Subdomains of Arkansas.gov and AR.gov. The Department is also considering amendments to the Rule Governing Time Period of Submission for Resolution of Protested Solicitation and Awards. A public hearing will be held on October 26, 2021, at 1:30pm in the Timberlands Conference Room, 501 Woodlane Avenue, Suite 500, Little Rock, AR 72201. Written comments should be mailed to TSS, Attn: Public Comments at P.O. Box 3522, Little Rock, AR 72203. Comments may also be e-mailed to TSS.RulesComments@arkansas.gov. Copies of the proposed rule may also be obtained from the Department of Transformation and Shared Services, 501 Woodlane Avenue, Suite 101-N, Little Rock, AR 72201, or by accessing the Department's website at <https://www.transform.ar.gov/secretarys-office/legal/rules-hearings/>.

FINANCIAL IMPACT STATEMENT

PLEASE ANSWER ALL QUESTIONS COMPLETELY

DEPARTMENT _____
DIVISION _____
PERSON COMPLETING THIS STATEMENT _____
TELEPHONE NO. _____ FAX NO. _____ EMAIL: _____

To comply with Ark. Code Ann. § 25-15-204(e), please complete the following Financial Impact Statement and file two (2) copies with the Questionnaire and proposed rules.

SHORT TITLE OF THIS RULE

1. Does this proposed, amended, or repealed rule have a financial impact? Yes No
2. Is the rule based on the best reasonably obtainable scientific, technical, economic, or other evidence and information available concerning the need for, consequences of, and alternatives to the rule?
Yes No
3. In consideration of the alternatives to this rule, was this rule determined by the agency to be the least costly rule considered? Yes No

If an agency is proposing a more costly rule, please state the following:

- a) How the additional benefits of the more costly rule justify its additional cost;
- b) The reason for adoption of the more costly rule;
- c) Whether the more costly rule is based on the interests of public health, safety, or welfare, and if so, please explain; and
- d) Whether the reason is within the scope of the agency's statutory authority, and if so, please explain.

4. If the purpose of this rule is to implement a federal rule or regulation, please state the following:

a) What is the cost to implement the federal rule or regulation?

Current Fiscal Year

Next Fiscal Year

General Revenue _____
Federal Funds _____
Cash Funds _____
Special Revenue _____
Other (Identify) _____

General Revenue _____
Federal Funds _____
Cash Funds _____
Special Revenue _____
Other (Identify) _____

Total _____

Total _____

b) What is the additional cost of the state rule?

Current Fiscal Year

Next Fiscal Year

General Revenue _____
Federal Funds _____
Cash Funds _____
Special Revenue _____
Other (Identify) _____

General Revenue _____
Federal Funds _____
Cash Funds _____
Special Revenue _____
Other (Identify) _____

Total _____

Total _____

5. What is the total estimated cost by fiscal year to any private individual, entity and business subject to the proposed, amended, or repealed rule? Identify the entity(ies) subject to the proposed rule and explain how they are affected.

Current Fiscal Year

Next Fiscal Year

\$ _____

\$ _____

6. What is the total estimated cost by fiscal year to state, county, and municipal government to implement this rule? Is this the cost of the program or grant? Please explain how the government is affected.

Current Fiscal Year

Next Fiscal Year

\$ _____

\$ _____

7. With respect to the agency's answers to Questions #5 and #6 above, is there a new or increased cost or obligation of at least one hundred thousand dollars (\$100,000) per year to a private individual, private entity, private business, state government, county government, municipal government, or to two (2) or more of those entities combined?
- Yes No See attached for supplemental response to the following questions

If YES, the agency is required by Ark. Code Ann. § 25-15-204(e)(4) to file written findings at the time of filing the financial impact statement. The written findings shall be filed simultaneously with the financial impact statement and shall include, without limitation, the following:

- (1) a statement of the rule's basis and purpose;
- (2) the problem the agency seeks to address with the proposed rule, including a statement of whether a rule is required by statute;
- (3) a description of the factual evidence that:
 - (a) justifies the agency's need for the proposed rule; and
 - (b) describes how the benefits of the rule meet the relevant statutory objectives and justify the rule's costs;
- (4) a list of less costly alternatives to the proposed rule and the reasons why the alternatives do not adequately address the problem to be solved by the proposed rule;
- (5) a list of alternatives to the proposed rule that were suggested as a result of public comment and the reasons why the alternatives do not adequately address the problem to be solved by the proposed rule;
- (6) a statement of whether existing rules have created or contributed to the problem the agency seeks to address with the proposed rule and, if existing rules have created or contributed to the problem, an explanation of why amendment or repeal of the rule creating or contributing to the problem is not a sufficient response; and
- (7) an agency plan for review of the rule no less than every ten (10) years to determine whether, based upon the evidence, there remains a need for the rule including, without limitation, whether:
 - (a) the rule is achieving the statutory objectives;
 - (b) the benefits of the rule continue to justify its costs; and
 - (c) the rule can be amended or repealed to reduce costs while continuing to achieve the statutory objectives.

Standard Statement – Data and System Security

Title: Data and System Security Classification

Document Number: SS-70-001

Effective Date: 5/15/2005

Published by: Office of the State ECIO

1.0 Purpose

This document presents a framework through which Arkansas' agencies, boards, commissions, and institutions of higher education can classify data and systems across the two spectrums of (1) data sensitivity and (2) data and system criticality. Once data is classified by the agency or institution of higher education, then appropriate security measures can be applied.

2.0 Scope

This standard statement applies to all state agencies, boards, commissions and institutions of higher education.

3.0 Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.

In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies. The State Security Office, under the state's Executive Chief Information Officer, defines an environment for strategic security architecture and sets security standards and policies for information technology in state government. In order to apply appropriate security measures, data must first be classified to determine its sensitivity and required availability.

4.0 References

4.1 Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.

4.2 Act 1042 of 2001: Authorized the Executive CIO to develop security policy.

5.0 Standard

5.1 Data owned and maintained by agencies shall be put into appropriate classification levels according to its sensitivity and criticality. Data security levels are as follows:

Data Sensitivity Levels

LEVEL A -- UNRESTRICTED

Unrestricted data is characterized as being open public data with no distribution limitations and to which anonymous access is allowed.

These data elements form information that is actively made publicly available by state government. It is published and distributed freely, without restriction. It is available in the form of physical documents such as brochures, formal statements, press releases, reports that are made freely available, and in electronic form such as internet web pages and bulletin boards accessible with anonymous access.

The greatest security threat to this data is from unauthorized or unintentional alteration, distortion, or destruction of this data. Security efforts appropriate to the criticality of the system containing this data must be taken to maintain its integrity.

Examples of data at this sensitivity level include many agency public websites.

LEVEL B -- SENSITIVE

These data elements are the information that is made available through open records requests or other formal or legal processes. This category includes the majority of the data contained within the state government electronic databases. Direct access to this data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties.

Security threats to this data include unauthorized access, alteration and destruction concerns.

Examples:

- Most data elements in state personnel records
- Building code violations data
- Driver history records
- Collective bargaining data
- Employment & training program data
- Federal contracts data
- Firearm permits data
- Historical records repository data
- Real estate appraisal data
- Occupational licensing data
- Personnel data

LEVEL C -- VERY SENSITIVE

Data classified as being very sensitive is only available to internal authorized users and may be protected by federal and state regulations. Very sensitive data is intended for use only by individuals who require the information in the course of performing job functions.

These data elements include those protected by federal and state statute or regulation.

Access to these data elements is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties. These are the data elements removed from responses to information requests for reasons of privacy.

Security threats to this data include violation of privacy statutes and regulations in addition to unauthorized alteration or destruction. If this data were accessed by unauthorized persons, it could cause financial loss or allow identity theft. Unauthorized disclosure could provide significant gain to a vendor's competitors.

Examples:

Social Security numbers	Credit card numbers
Most home addresses	Competitive bids
Attorneys' files	Civil investigative data
Comprehensive law enforcement data	Criminal history data
Domestic abuse data	Economic development assistance data
Educational records	Food assistance programs data
Foster care data	Head Start data
Health and medical data	Juvenile delinquent data
Library borrower's records	Counselors' data
Signature imaging data	Trade secrets data
Welfare records/data	

LEVEL D – EXTREMELY SENSITIVE

Data classified as being extremely sensitive is data whose disclosure or corruption could be hazardous to life or health.

These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health or safety repercussions. Very strict rules must be adhered to in the usage of this data.

Examples of this data include the contents of state law enforcement investigative records and communications systems.

5.2 Data and systems should be put into appropriate classification levels according to their criticality. The levels of criticality and their descriptions are as follows:

Criticality Levels

LEVEL 1 – NOT CRITICAL

These data and systems are necessary to state government but short-term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of Arkansas' citizens.

LEVEL 2 – CRITICAL

These data and systems are required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the data and systems can be restored.

LEVEL 3 – EXTREMELY CRITICAL

These data and systems are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe. These data and systems also require restoration of the original facilities to be able to resume business.

6.0 Procedures

Agencies and institutions of higher education should classify their data and systems according to the data and system classification standard and be able to demonstrate compliance.

7.0 Revision History

Date	Description of Change
------	-----------------------

5/15/2005	Original Standard Statement Published
-----------	---------------------------------------

8.0 Definitions

8.1 Data

Data is information maintained in any form within state agencies or institutions of higher education. Any grouping of data is classified at the level of its most sensitive or critical data element.

8.2 System

In this context, the term system is defined as a combination of hardware, software, and procedures necessary to support particular data. A server may have multiple systems and a system may require multiple servers.

9.0 Related Resources

9.1 COBIT Standards: <http://www.isaca.org/cobit.htm>

10.0 Inquiries

Direct inquiries about this standard to:

Office of Information Technology

Shared Technical Architecture

124 West Capitol Avenue Suite 200, Little Rock, Arkansas 72201

Phone: 501-682-4300

FAX: 501-682-2040

Email: ITarch@mail.state.ar.us

OIT policies can be found on the Internet at: <http://www.cio.arkansas.gov/techarch>

11.0 Attachment

Data Sensitivity and System Criticality Grid

The following grid allows agencies to classify data and systems at the same time for criticality and sensitivity.

Rows Represent Data Sensitivity

Columns Represent System Criticality

	LEVEL 1 - NOT CRITICAL Necessary to state government but short-term interruption of service acceptable. These systems do not play any role in the scheme of health, security, safety of the citizens, etc. They could be easily offset with manual procedures.	LEVEL 2 - CRITICAL Required to perform a critical service of state government: These systems will be required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the system can be restored.	LEVEL 3 - EXTREMELY CRITICAL Critical to health or safety: These systems must be protected by a vital plan that would allow resumption of operations within a very short timeframe. It also requires the ability to be able to resume business.
LEVEL A - UNRESTRICTED Open public data with no distribution limitations, anonymous access. May be anonymous access via electronic sources. (See Appendix A for expanded definition.) Examples: Arkansas.gov website, ADEQ website, and other state agency public websites	1A	2A	3A
LEVEL B - SENSITIVE Public data with limited availability, but which requires a special application to be completed or special processing to be done prior to access (for example, to redact sensitive data elements). Examples: Most data elements in the state personnel records, data elements in motor vehicle records not restricted by privacy regulations, and driver history records	1B	2B	3B
LEVEL C - VERY SENSITIVE Data only available to internal authorized users. May be protected by federal and state regulations. Intended for use only by individuals who require the information in the course of performing job functions. Examples: Social security numbers, credit card numbers, home addresses, and competitive bids	1C	2C	3C
LEVEL D - EXTREMELY SENSITIVE Data whose disclosure or corruption could be hazardous to life or health. Examples: Contents of state law enforcement investigative records and communications systems	1D	2D	3D

