

A.C.A. § 25-1-128

Current through all legislation of the 2023 Regular Session and the 2023 First Extraordinary Session.

AR - Arkansas Code Annotated > Title 25 State Government > Chapter 1 General Provisions > Subchapter 1 — General Provisions

25-1-128. Policy regarding use of technology resources and cyber security — Definitions.

(a) As used in this section:

- (1) “Employee” means a person employed by a public entity;
- (2) “Public entity” means an instrumentality funded in whole or in part by taxpayer funds, including without limitation:
 - (A) The Department of Agriculture;
 - (B) The Department of Commerce;
 - (C) The Department of Corrections;
 - (D) The Department of Education;
 - (E) The Department of Energy and Environment;
 - (F) The Department of Finance and Administration;
 - (G) The Department of Health;
 - (H) The Department of Human Services;
 - (I) The Department of Inspector General;
 - (J) The Department of Labor and Licensing;
 - (K) The Department of the Military;
 - (L) The Department of Parks, Heritage, and Tourism;
 - (M) The Department of Public Safety;
 - (N) The Department of Transformation and Shared Services;
 - (O) The Department of Veterans Affairs;
 - (P) The office of a constitutional officer;
 - (Q) A political subdivision of the state;
 - (R) A public school district;
 - (S) A public school district board of directors;
 - (T) An open-enrollment public charter school;

- (U) An institution of higher education;
 - (V) The State Highway Commission;
 - (W) The Arkansas Department of Transportation; or
 - (X) The Arkansas State Game and Fish Commission;
- (3) “State educational entity” means an entity with an educational purpose that is funded in whole or in part by taxpayer funds that is, including without limitation:
- (A) A public school district;
 - (B) A public school district board of directors; and
 - (C) An open-enrollment charter school;
- (4) “State entity” means:
- (A) The Department of Agriculture;
 - (B) The Department of Commerce;
 - (C) The Department of Corrections;
 - (D) The Department of Education;
 - (E) The Department of Energy and Environment;
 - (F) The Department of Finance and Administration;
 - (G) The Department of Health;
 - (H) The Department of Human Services;
 - (I) The Department of Inspector General;
 - (J) The Department of Labor and Licensing;
 - (K) The Department of the Military;
 - (L) The Department of Parks, Heritage, and Tourism;
 - (M) The Department of Public Safety;
 - (N) The Department of Transformation and Shared Services;
 - (O) The Department of Veterans Affairs;
 - (P) The State Highway Commission;
 - (Q) The Arkansas Department of Transportation;
 - (R) The Arkansas State Game and Fish Commission; and
 - (S) An institution of higher education; and
- (5) “Technology resources” means:
- (A) The machines, devices, and transmission facilities used in information processing, including computers, word processors, terminals, telephones, cables, software, and related products;
 - (B) The devices used to process information through electronic capture, collection, storage, manipulation, transmission, retrieval, and presentation of information in the form of data, text, voice, or image and includes telecommunications and office automation functions;

(C) Any component related to information processing and wired and wireless telecommunications, including data processing and telecommunications hardware, software, services, planning, personnel, facilities, and training;

(D) The procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and the associated personnel, including consultants and contractors; and

(E) All electronic mail accounts issued by a public entity.

(b) A public entity shall:

(1) Create a technology resources policy that defines the authorized use of technology resources for the public entity;

(2)

(A) Develop a cyber security policy for all technology resources of the public entity based on the standards and guidelines set by the State Cyber Security Office.

(B) Subdivision (b)(2)(A) of this section shall not apply to political subdivisions of the state; and

(3)

(A) Develop a training program for all employees of the public entity concerning the technology resources policy and cyber security policy.

(B) A political subdivision of the state is not required to develop a training program under this section for a cyber security policy.

(c)

(1) The technology resources policy for each state entity shall be available to the public upon request.

(2) The Department of Education, in coordination with the State Cyber Security Office, shall:

(A) Develop technology resources policies that shall be used by each type of state educational institution; and

(B) Make the policies developed under subdivision (c)(2)(A) of this section available to the public upon request.

(d) Each technology resources policy shall include prohibitions on the use of a public entity's technology resources, including without limitation that a public entity's technology resources shall not be used to:

(1) Express a personal political opinion to an elected official unless the opinion is:

(A) Within the scope of the employee's regular job duties; or

(B) Requested by an elected official or public entity;

(2) Engage in lobbying an elected official on a personal opinion if the employee is not a registered lobbyist for the public entity;

(3) Engage in illegal activities or activities otherwise prohibited by federal law or state law; or

(4) Intentionally override or avoid the security and system integrity procedures of the public entity.

(e) A public entity shall create a disciplinary procedure for a violation of the public entity's technology resources policy concerning authorized use of technology resources.

(f)

(1) Each state entity shall submit a cyber security policy for the state entity for approval to the State Cyber Security Office by October 1 of each even-numbered year.

(2) The State Cyber Security Office shall establish a procedure to review and approve state entity cyber security policies.

(3) The Department of Education shall:

(A) Develop a cyber security policy that shall be used by each type of state educational institution;

(B) Submit the policies developed under subdivision (f)(3)(A) of this section for approval to the State Cyber Security Office by October 1 of each even-numbered year; and

(C) Coordinate with each state educational institution to implement the cyber security policy.

(g) A public entity, except for a political subdivision of the state, shall create a disciplinary procedure for a violation of the public entity's cyber security policy in consultation with the State Cyber Security Office that establishes:

(1) A disciplinary procedure for a violation of a state entity's cyber security policy; and

(2) The reporting procedure for suspected violations of the cyber security policy.

(h) All cyber security policies developed under this section shall not be deemed open public records under the Freedom of Information Act of 1967, § 25-19-101 et seq.

(i) The disciplinary procedures under subsection (e) of this section shall not apply to employee communications made in compliance with the:

(1) Public Employees' Political Freedom Act of 1999, § 21-1-501 et seq.; or

(2) Arkansas Whistle-Blower Act, § 21-1-601 et seq.

History

Acts 2023, No. 504, § 1.

Arkansas Code of 1987 Annotated Official Edition

Copyright © 2024 by the State of Arkansas All rights reserved