State of Arkansas *As Engrossed: H2/27/23*
94th General Assembly **A Bill**
Regular Session, 2023 HOUSE BILL 1369

By: Representative S. Meeks
By: Senator J. English

For An Act To Be Entitled

AN ACT TO REQUIRE PUBLIC ENTITIES TO CREATE A POLICY CONCERNING THE AUTHORIZED USE OF TECHNOLOGY RESOURCES AND A CYBER SECURITY POLICY; TO AMEND THE DUTIES OF THE STATE CYBER SECURITY OFFICE; AND FOR OTHER PURPOSES.

Subtitle

TO REQUIRE PUBLIC ENTITIES TO CREATE A POLICY CONCERNING THE AUTHORIZED USE OF TECHNOLOGY RESOURCES AND A CYBER SECURITY POLICY; AND TO AMEND THE DUTIES OF THE STATE CYBER SECURITY OFFICE.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

SECTION 1. Arkansas Code Title 25, Chapter 1, Subchapter 1, is amended to add an additional section to read as follows:

25-1-126. Policy regarding use of technology resources and cyber security.

(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 entity" means the:

(A) Department of Agriculture;

(B) Department of Commerce;

(C) Department of Corrections;

(D) Department of Education;

(E) Department of Energy and Environment;

(F) Department of Finance and Administration;

(G) Department of Health;

(H) Department of Human Services;

(I) Department of Inspector General;

(J) Department of Labor and Licensing;

(K) Department of the Military;

(L) Department of Parks, Heritage, and Tourism;

(M) Department of Public Safety;

(N) Department of Transformation and Shared Services;

(O) Department of Veterans Affairs;

(P) State Highway Commission;

(Q) Arkansas Department of Transportation; and

(R) Arkansas State Game and Fish Commission;

(4) "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;

(C) An open-enrollment charter school; and

(D) 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) 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 filed with the Joint Committee on Advanced Communications and Information Technology by October 1 of each even numbered year.

(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) File the policies developed under subdivision (c)(2)(A) of this section with the Joint Committee on Advanced Communications and Information Technology by October 1 of each even numbered year.

(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 to include without limitation:

(1) A written warning for the first reported violation;

(2) An administrative penalty for the second reported violation;

(3) Disciplinary action for the third violation and any

subsequent violations; and

(4) The reporting procedure for suspected violations of the technology resources policy.

(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 § 25-19-105(b)(11).

/s/S. Meeks