First Regular Session of the 124th General Assembly (2025)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type.~~

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.

Conflict reconciliation: Text in a statute in *this style type* or ~~*this style type*~~ reconciles conflicts between statutes enacted by the 2024 Regular Session of the General Assembly.

SENATE ENROLLED ACT No. 472

AN ACT to amend the Indiana Code concerning state offices and administration and to make an appropriation.

Be it enacted by the General Assembly of the State of Indiana:

SECTION 1. IC 4-13.1-2-9, AS AMENDED BY P.L.137-2021, SECTION 18, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]: Sec. 9. **(a)** A state agency (as defined in IC 4-1-10-2) other than **a** state educational ~~institutions,~~ **institution,** and a political subdivision (as defined in IC 36-1-2-13), **other than a political subdivision established under IC 8-1-11.1,** shall:

(1) report any cybersecurity incident using their best professional judgment to the office without unreasonable delay and not later than two (2) business days after discovery of the cybersecurity incident in a format prescribed by the chief information officer; and

(2) provide the office with the name and contact information of any individual who will act as the primary reporter of a cybersecurity incident described in subdivision (1) before September 1, 2021, and before September 1 of every year thereafter.

Nothing in this section shall be construed to require reporting that conflicts with federal privacy laws or is prohibited due to an ongoing law enforcement investigation.

SECTION 2. IC 4-13.1-4-2, AS ADDED BY P.L.108-2024, SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE

JULY 1, 2025]: Sec. 2. **(a) Except as provided in subsection (b),** as used in this chapter, "public entity" means a:

(1) political subdivision;

(2) state agency;

(3) school corporation; or

(4) state educational institution.

(b) The term does not include an acute care hospital licensed under IC 16-21 that is established and operated under IC 16-22-2, IC 16-22-8, or IC 16-23, or a political subdivision established under IC 8-1-11.1.

SECTION 3. IC 4-13.1-4-5, AS ADDED BY P.L.108-2024, SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]: Sec. 5. **(a) The office shall:**

(1) develop:

(A) standards and guidelines regarding cybersecurity for use by political subdivisions and state educational institutions; and

(B) a uniform cybersecurity policy for use by state agencies; and

(2) develop, in collaboration with the department of education:

(A) a uniform technology resources policy governing use of technology resources by the employees of a school corporation; and

(B) a uniform cybersecurity policy for use by school corporations.

(b) Not later than December 31, 2027, each public entity ~~may~~ **shall** adopt the following:

(1) A policy governing use of technology resources by the public entity's employees. ~~The policy may:~~ **If the public entity is a school corporation, the public entity shall adopt the uniform technology resources policy developed under subsection (a)(2)(A).**

~~(A) prohibit an employee of the public entity from using the public entity's technology resources to:~~

~~(i) engage in lobbying (as defined in IC 2-7-1-9) that is outside the scope of the employee's duties;~~

~~(ii) engage in illegal activity; or~~

~~(iii) violate the public entity's cybersecurity policy; and~~

~~(B) include disciplinary procedures for violation of the technology resources policy.~~

(2) A cybersecurity policy ~~If the public entity is:~~ **as follows:**

(A) **If the public entity is** a political subdivision or state educational institution, the **public entity shall adopt a cybersecurity** policy ~~may be~~ based on standards and guidelines developed ~~by the office~~ **under subsection (a)(1)(A).**

(B) **If the public entity is** a school corporation, the ~~policy may be based on~~ **public entity shall adopt the uniform** cybersecurity policy ~~standards and guidelines~~ developed ~~by the office, in collaboration with the department of education; and~~ **under subsection (a)(2)(B).**

(C) **If the public entity is** a state agency, the **public entity shall adopt the uniform cybersecurity** policy ~~is~~ developed ~~by the office.~~ **under subsection (a)(1)(B).**

(3) A training program regarding the public entity's technology resources policy adopted under subdivision (1) and cybersecurity policy adopted under subdivision (2), completion of which is mandatory for the public entity's employees.

(c) The uniform technology resources policy developed under subsection (a)(2)(A) and a technology resources policy adopted by a public entity other than a school corporation under subsection (b)(1) must:

(1) prohibit an employee of the public entity from using the public entity's technology resources to:

(A) engage in lobbying (as defined in IC 2-7-1-9) that is outside the scope of the employee's duties;

(B) engage in illegal activity; or

(C) violate the public entity's cybersecurity policy; and

(2) include disciplinary procedures for violation of the technology resources policy.

SECTION 4. IC 4-13.1-4-6, AS ADDED BY P.L.108-2024, SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]: Sec. 6. (a) Not later than December 31 of each odd-numbered year, a public entity ~~may~~ **shall** submit to the office the public entity's cybersecurity policy adopted by the public entity under section 5 of this chapter.

(b) The office ~~may~~ **shall** establish a procedure for collecting and maintaining a record of cybersecurity policies submitted to the office under subsection (a).

(c) If a public entity engages a third party to conduct an assessment of the public entity's cybersecurity policy, the public entity shall provide the results of the assessment to the office.

President of the Senate

President Pro Tempore

Speaker of the House of Representatives

Governor of the State of Indiana

Date: _____ Time: _____

SEA 472 — Concur