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. 459

AN ACT to amend the Indiana Code concerning environmental law.

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) This section does not apply to an entity subject to IC 13-18-16.5.**

(b) A state agency (as defined in IC 4-1-10-2), other than state educational institutions, and a political subdivision (as defined in IC 36-1-2-13) 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 13-18-3-1.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY

1, 2025]: **Sec. 1.5. (a) The board may adopt rules under IC 4-22-2 and IC 13-14-9 establishing standards for the reclamation and reuse of treated wastewater.**

(b) The rules adopted under subsection (a):

(1) must protect state waters and public health;

(2) may concern multiple categories of reuse; and

(3) may create a permitting process.

SECTION 3. IC 13-18-16.5 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]:

Chapter 16.5. Public Water and Wastewater Cybersecurity

Sec. 1. (a) This chapter applies to an entity that:

(1) is:

(A) a community water system (as defined in IC 13-11-2-35.5(b)) with a population of five hundred (500) or more;

(B) a publicly owned treatment works (as defined in IC 13-11-2-177.5); or

(C) a semipublic facility (as defined in 327 IAC 5-1.5-59) with a classification of Class III or Class IV (as described in 327 IAC 5-23-3(4) and 327 IAC 5-23-3(5)); and

(2) utilizes:

(A) a computerized system to monitor and control the processes of the entity's operation from a central location; or

(B) another vulnerable monitoring or management system identified by the department.

(b) An entity shall do the following:

(1) Conduct a cybersecurity vulnerability assessment at least once per calendar year.

(2) Before September 1 of each year, provide the office of technology established by IC 4-13.1-2-1 with the name and contact information of any individual who will act as the primary reporter of a cybersecurity incident.

(3) Beginning in 2026, not later than December 31 of each even-numbered year, submit a certification to the department via a secured portal verifying that the entity:

(A) completed the assessment described in subdivision (1);

(B) mitigated or has documented plans to mitigate identified vulnerabilities; and

(C) updated emergency response plans to account for vulnerabilities and mitigating procedures.

(4) When an actual or reasonably suspected cybersecurity breach occurs, report the cybersecurity incident to the office of technology established by IC 4-13.1-2-1:

(A) either:

(i) not later than twenty-four (24) hours after discovery of the cybersecurity incident, if the cybersecurity incident impacts the operations of the entity; or

(ii) not later than two (2) business days after discovery of the cybersecurity incident, if the cybersecurity incident does not impact the operations of the entity; and

(B) in a format prescribed by the chief information officer of the office of technology.

(c) In conducting an assessment under subsection (b)(1), the entity shall utilize an assessment tool or framework approved by the department and the office of technology established by IC 4-13.1-2-1.

(d) An assessment conducted under subsection (b)(1) is confidential under IC 5-14-3-4(b)(19).

President of the Senate

President Pro Tempore

Speaker of the House of Representatives

Governor of the State of Indiana

Date: _____ Time: _____