House Bill 4055

Introduced and printed pursuant to House Rule 12.00. Presession filed (at the request of Joint Legislative Committee on Information Management and Technology for Representative Nancy Nathanson)

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure **as introduced.** The statement includes a measure digest written in compliance with applicable readability standards.

Digest: Tells a local public body to give a report to the state when there is an information security incident. Prescribes what must be in the report. (Flesch Readability Score: 63.4).

Requires a local government, local service district or special government body to notify and submit a report to the State Chief Information Officer within 48 hours of an information security incident or ransomware incident. Prescribes the information that a public body is required to report.

Directs the State Chief Information Officer to establish a reporting system that allows a public body to submit a notification or report in a timely, secure and confidential manner. Directs the State Chief Information Officer to create a webpage to provide instructions on how to provide notification and submit a report.

Requires the State Chief Information Officer to provide an annual report to the Governor and the Joint Legislative Committee on Information Management and Technology on the information security incidents and ransomware incidents reported for the preceding year.

Exempts information security incident or ransomware incident reports from disclosure under public records laws and allows for the sharing of information under certain circumstances.

Becomes operative July 1, 2026.

Declares an emergency, effective on passage.

A BILL FOR AN ACT

Relating to information security; and declaring an emergency.

Be It Enacted by the People of the State of Oregon:

SECTION 1. (1) As used in this section:

(a) "Information security incident" means a substantial incident that leads to one or more of the following impacts:

(A) Substantial loss of confidentiality, integrity or availability of a public body's information system.

(B) Compromise in the safety and resilience of a public body's operational systems and processes.

(C) Disruption of a public body's ability to engage in business, carry on operations or deliver services.

(D) Unauthorized access to a public body's information system or nonpublic information, when the impact is caused by a compromise of a third-party information service or data hosting provider.

(b) "Information system" means a system of computers and related hardware, software, storage media and networks and any other means by which a public body collects, uses or manages the public body's information resources.

(c) "Public body" means:

(A) A local government, as defined in ORS 174.116.

(B) A local service district, as defined in ORS 174.116.

(C) A special government body, as defined in ORS 174.117.

NOTE: Matter in **boldfaced** type in an amended section is new; matter [*italic and bracketed*] is existing law to be omitted. New sections are in **boldfaced** type.

(d) "Ransomware incident" means an information security incident in which a person introduces software to gain unauthorized access to or encrypt, modify or render unavailable a public body's data for the purposes of demanding or compelling the public body to pay a ransom.

(2)(a) A public body shall, within 48 hours of discovering an information security incident or ransomware incident:

(A) Notify the State Chief Information Officer of the information security incident or ransomware incident; and

(B) Submit a report to the State Chief Information Officer that describes the actions the public body has taken or must reasonably take to prevent, mitigate or recover from damage to, unauthorized access to, unauthorized modifications or deletions of or other impairments of the integrity of the public body's information system.

(b) The State Chief Information Officer shall prescribe the format in which a report must be submitted under this section.

(3) The State Chief Information Officer shall establish an information security incident notification and reporting system that a public body shall use to provide notification or submit a report, as required under this section, in a timely, secure and confidential manner. The system must allow the State Chief Information Officer to:

(a) Securely accept from public bodies information security incident or ransomware incident notifications and reports;

(b) Track and identify trends in information security incidents and ransomware incidents that are reported through the system; and

(c) Provide reports on the types of incidents, threat indicators, defensive measures and entities that are reported through the system.

(4)(a) An information security incident or ransomware incident report that is submitted under this section is exempt from public disclosure under ORS 192.311 to 192.478 and must be treated as confidential.

(b) The State Chief Information Officer may share information concerning an information security incident or ransomware incident report with:

(A) The Oregon Cybersecurity Center of Excellence established under ORS 276A.555, if the information helps the center carry out the center's purpose as described under ORS 276A.555;

(B) Federal, state or local law enforcement authorities; and

(C) Any other entity as the State Chief Information Officer determines is appropriate.

(c) The State Chief Information Officer may anonymize and share information related to threat indicators and defensive measures to assist in preventing information security incidents or ransomware incidents.

(5) The State Chief Information Officer shall maintain a webpage that provides instructions on how a public body may provide notification and submit a report as described under subsection (2) of this section. The instructions must describe, at a minimum:

(a) The types of information security incidents and ransomware incidents that a public body is required to report; and

(b) Any information a public body should provide when notifying the State Chief Information Officer of an information security incident or ransomware incident.

(6)(a) The State Chief Information Officer shall submit to the Governor and submit to,

and present in an appropriate hearing or other proceeding before, the Joint Legislative Committee on Information Management and Technology an annual report concerning any notifications and reports the State Chief Information Officer receives from public bodies under this section. The annual report must include, at a minimum, for the preceding year:

(A) Information on the number of notifications the State Chief Information Officer received;

(B) A description of the types of information security incidents or ransomware incidents that were reported; and

(C) The type of public bodies that submitted notifications.

(b) The annual report described in paragraph (a) of this subsection may not include information security information or other materials that are exempt from disclosure under ORS 192.311 to 192.478.

SECTION 2. (1) Section 1 of this 2026 Act becomes operative on July 1, 2026.

(2) The State Chief Information Officer may adopt rules and take any other action before the operative date specified in subsection (1) of this section that is necessary to enable the State Chief Information Officer to undertake and exercise, on and after the operative date specified in subsection (1) of this section, all of the duties, functions and powers conferred on the State Chief Information Officer by section 1 of this 2026 Act.

(3) No later than 90 days after the effective date of this 2026 Act, the State Chief Information Officer shall:

(a) Establish the information security incident notification and reporting system described under section 1 (3) of this 2026 Act; and

(b) Create and maintain the webpage described under section 1 (5) of this 2026 Act.

SECTION 3. This 2026 Act being necessary for the immediate preservation of the public peace, health and safety, an emergency is declared to exist, and this 2026 Act takes effect on its passage.