Dexter A. Johnson
LEGISLATIVE COUNSEL

900 COURT ST NE S101
SALEM, OREGON 97301-4065
(503) 986-1243
FAX: (503) 373-1043
www.oregonlegislature.gov/lc

Open Government Impact Statement

83rd Oregon Legislative Assembly
2026 Regular Session

Measure: HB 4055

Only impacts on Original or Engrossed Versions are Considered Official

Prepared by:	Dexter A. Johnson
Date:	2/2/2026

SUMMARY

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.

OPEN GOVERNMENT IMPACT

Legislative Counsel has not adopted standards for drafting measures that establish exemptions from disclosure of public records.

This measure exempts from public disclosure an information security incident report or ransomware incident report submitted by a public body to the State Chief Information Officer, within 48 hours of discovering an information security incident or ransomware incident, describing 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.

If those public records that could be subject to public disclosure were instead subject to mandatory disclosure under public records law, the public could gain sensitive information about a public body's information system and the public body's response to an information security incident or ransomware incident.