

Washington AI Guardrails Act™: Plain-English Summary

MODEL BILL DRAFT, not legal advice, for discussion with a legislative sponsor. From the AI Guardrails Pledge.

What it does

It puts the Pledge's four AI levels into state law:

- **Low risk:** no new rules. Spam filters, maps, autocorrect.
- **Use with care:** tell people when they're talking to AI, offer a way to reach a human, and no impersonating real people without written consent.
- **High risk** (jobs, housing, loans, insurance, health care, school, public benefits): a human makes the final call, yearly bias testing, notice, plain-language reasons, a way to fix data and appeal within 30 days, data care, records, and a named person in charge.
- **Banned:** hidden social scores, mass facial tracking without legal authority, manipulating vulnerable people, AI deciding to use lethal force, and bulk sale of personal data without consent.

How it's enforced

The Attorney General enforces it under the Consumer Protection Act. Small businesses can rely on the vendor's bias testing, use free state templates, and get 60 days to fix a first mistake. Following a recognized framework (NIST, ISO 42001) is a defense. Takes effect January 1, 2028.

What it builds on (it doesn't repeat these)

Facial recognition law (RCW 43.386), My Health My Data Act (RCW 19.373), Law Against Discrimination (RCW 49.60), the 2026 companion chatbot law (ESHB 2225) and AI content labeling law (E2SHB 1170), and the WA AI Task Force's 2026 final report.

Roadmap

1. Washington (now to spring 2027)

- Find your district at app.leg.wa.gov/districtfinder and contact your one senator and two representatives. Also contact chairs of the House Technology, Economic Development & Veterans Committee and the Senate Environment, Energy & Technology Committee.
- A sponsor asks the Code Reviser to draft it. Prefiling opens in early December 2026, and the 105-day session starts January 11, 2027. Ask for a bill request by mid-December so it can be introduced in week one.
- Gather support: testimony, the Pledge signers, and business and consumer groups.

2. Federal (2027 on)

- Use the Washington bill as a model for a congressional bill, and share it with your members of Congress.
- Pitch it as a national floor of protections, which also answers the "50 different state laws" complaint.

3. International

- Line it up with the OECD AI Principles, the EU AI Act's risk tiers, and UN AI efforts (the UN Global Dialogue on AI Governance and its Scientific Panel), and offer it as a simple, common-sense standard.

Full Model Bill Text

MODEL BILL DRAFT, not legal advice, for discussion with a legislative sponsor. Proposed by the AI Guardrails Pledge. Based on the Pledge's Proposed AI Safety Protocols & Standards. This draft has not been reviewed by the Washington Code Reviser's Office and is not in final drafting form. Section numbers and RCW placement are placeholders.

____ **BILL** ____

State of Washington, 70th Legislature, 2027 Regular Session

By Representatives/Senators _____ (sponsor to be determined)

AN ACT Relating to establishing risk-based guardrails for artificial intelligence systems that affect Washington residents; adding a new chapter to Title 19 RCW; prescribing penalties; and providing an effective date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. Sec. 1. Findings and intent.

(1) The legislature finds that artificial intelligence offers real benefits to Washington residents, businesses, and public agencies, and that most uses of artificial intelligence pose little risk to people.

(2) The legislature also finds that some uses of artificial intelligence can decide or shape whether a person gets a job, a home, a loan, insurance, health care, education, or public benefits, and that these decisions can be wrong, unfair, or impossible to challenge when no human is responsible for them.

(3) The legislature further finds that a small number of uses, such as hidden social scoring, manipulation of vulnerable people, and the bulk sale of personal data without consent, are incompatible with the rights of Washington residents.

(4) It is the intent of the legislature to adopt a simple, risk-based approach: light rules for low-risk uses, honesty rules for AI that talks with people or creates realistic content, real safeguards for high-risk decisions, and a short list of prohibited practices. The legislature intends that a human remains in charge of decisions that matter, and that people's privacy and safety come first.

(5) The legislature intends this chapter to build on, and not duplicate, existing Washington law, including chapter 43.386 RCW (facial recognition by state and local agencies), chapter 19.373 RCW (My Health My Data Act), chapter 49.60 RCW (Washington Law Against Discrimination), chapter 19.86 RCW (Consumer Protection Act), and 2026 laws on AI companion chatbots and AI content provenance.

NEW SECTION. Sec. 2. Definitions.

The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Artificial intelligence system" means a machine-based system that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

(2) "Consequential decision" means a decision that has a material legal or similarly significant effect on a consumer's access to, eligibility for, or cost or terms of: (a) employment; (b) housing; (c) credit or financial services; (d) insurance; (e) health care services; (f) education or educational opportunity; or (g) essential government services or public benefits.

(3) "High-risk artificial intelligence system" means an artificial intelligence system that makes, or is a substantial factor in making, a consequential decision.

(4) "Substantial factor" means an output of an artificial intelligence system that is used to make, or that materially influences, a consequential decision.

(5) "Interactive or synthetic AI" means an artificial intelligence system that (a) communicates with a person in natural language, or (b) generates or materially alters images, audio, or video that a reasonable person could believe is authentic.

(6) "Deployer" means a person doing business in Washington, or a state or local agency, that uses an artificial intelligence system.

(7) "Developer" means a person that develops or intentionally and substantially modifies an artificial intelligence system offered to deployers in Washington.

(8) "Consumer" means a natural person who is a Washington resident.

(9) "Personal data" has the same meaning as in RCW 19.373.010, extended to all personal data and not only consumer health data.

(10) "Algorithmic discrimination" means an unlawful differential treatment or impact that disfavors a person on the basis of a characteristic protected under chapter 49.60 RCW or federal law.

(11) "Human reviewer" means a named, trained natural person with the authority and competence to review, approve, and override an output of a high-risk artificial intelligence system.

(12) "Small business" means a deployer with fewer than 50 full-time equivalent employees that does not use its own data to train a high-risk artificial intelligence system.

NEW SECTION. Sec. 3. Risk levels.

(1) This chapter recognizes four risk levels:

(a) **Level 1, low risk:** an artificial intelligence system that is not interactive or synthetic AI, is not a high-risk system, and is not used for a prohibited practice. Examples include spam filters, autocorrect, navigation, and entertainment recommendations.

(b) **Level 2, use with care:** interactive or synthetic AI that is not a high-risk system.

(c) **Level 3, high risk:** a high-risk artificial intelligence system.

(d) **Level 4, prohibited:** any use described in section 7 of this act.

(2) A system that meets more than one level is subject to the duties of each level that applies. When a deployer is uncertain which level applies, the deployer must treat the system as the higher level.

NEW SECTION. Sec. 4. Level 1 duties: low-risk systems.

Level 1 systems are subject to no duties under this chapter beyond sections 7 and 11. Nothing in this section limits existing privacy or consumer protection law.

NEW SECTION. Sec. 5. Level 2 duties: use with care.

(1) A deployer of interactive AI must clearly and conspicuously disclose to a person, at the start of an interaction, that the person is communicating with artificial intelligence and not a human, unless that is obvious to a reasonable person.

(2) A deployer of interactive AI used to provide customer service must offer a reasonably accessible way to reach a human.

(3) No person may use synthetic AI to impersonate a real, identifiable person without that person's prior written consent, except for lawful satire, parody, news reporting, or commentary that is clearly identified as such.

(4) Synthetic content must carry disclosure or provenance information as required by E2SHB 1170 (chapter 167, Laws of 2026). This section does not impose additional labeling duties on content governed by that law.

(5) Companion chatbots remain governed by ESHB 2225 (chapter 168, Laws of 2026). Where that law applies, it controls over this section.

NEW SECTION. Sec. 6. Level 3 duties: high-risk systems.

(1) **Human makes the final call.** A deployer may not make a consequential decision based on a high-risk system unless a human reviewer has reviewed the output and approved the decision. The human reviewer must be able to override the system.

(2) **Bias testing.** Before first use, and at least once every 12 months, a deployer must test or obtain testing of each high-risk system for algorithmic discrimination, take reasonable steps to correct problems found, and keep the results for at least three years.

(3) **Notice.** Before or at the time a high-risk system is used to make a consequential decision, the deployer must tell the consumer in plain language that artificial intelligence is being used, what it is used for, and how to contact the deployer.

(4) **Explanation.** If a consequential decision is adverse to the consumer, the deployer must, on request, give the consumer a plain-language statement of the principal reasons for the decision, including the role the system played and the main types of data it used.

(5) **Correction and appeal.** A deployer must give the consumer an opportunity to correct inaccurate personal data used in the decision and to appeal an adverse decision. An appeal must be reviewed by a human reviewer who did not make the original decision, where practical, and answered within 30 days, extendable once by 15 days with notice.

(6) **Data care.** A deployer must limit personal data used by a high-risk system to what is reasonably necessary for the decision, protect it with reasonable security, and may not sell it without the consumer's clear, affirmative consent.

(7) **Records.** A deployer must keep a log of consequential decisions made with a high-risk system, including the human review, for at least three years.

(8) **Accountability.** A deployer must designate a named individual responsible for each high-risk system and its compliance with this chapter.

(9) **Developer duties.** A developer of a high-risk system must give deployers documentation describing intended uses, known limits and risks, the general types of training data, results of the developer's bias testing, and instructions for meaningful human review.

NEW SECTION. Sec. 7. Level 4: prohibited practices.

No person may develop, deploy, or use an artificial intelligence system to:

- (1) Assign consumers a general score or ranking of trustworthiness or social behavior that leads to unjustified or disproportionate detrimental treatment in unrelated contexts, or that is hidden from the consumer;
- (2) Conduct real-time or mass facial recognition or biometric tracking of people in publicly accessible places without legal authority. For state and local agencies, chapter 43.386 RCW continues to govern and nothing in this act authorizes any use that chapter restricts;
- (3) Use deceptive or manipulative techniques that exploit the age, disability, or acute emotional or financial crisis of a person to materially distort the person's behavior in a way likely to cause harm;
- (4) Select and engage a human target with lethal force without meaningful human control. This subsection does not apply to the armed forces of the United States or to matters reserved to federal law; or
- (5) Buy, sell, or license the personal data of consumers in bulk to train or operate an artificial intelligence system without the consumers' knowledge and clear, affirmative consent.

NEW SECTION. Sec. 8. Small business accommodations.

- (1) A small business that uses a high-risk system as provided by a developer, for its intended purpose, may rely on the developer's bias testing under section 6(9) instead of conducting its own under section 6(2).
- (2) The attorney general shall publish free model notices, explanation forms, appeal procedures, and a one-page AI policy template that a deployer may use to satisfy this chapter.
- (3) For a first violation by a small business, the attorney general shall issue a notice and allow 60 days to cure before seeking penalties, except for violations of section 7.

NEW SECTION. Sec. 9. Enforcement.

- (1) A violation of this chapter is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying chapter 19.86 RCW. The attorney general may enforce this chapter.
- (2) [Option for sponsor] This chapter (a) does not create a private right of action, or (b) allows a consumer injured by a violation of section 6 or 7 to bring an action under RCW 19.86.090.

(3) It is an affirmative defense that the deployer or developer complies with a nationally or internationally recognized AI risk management framework, such as the NIST AI Risk Management Framework or ISO/IEC 42001, and discovered and cured the violation through its own testing or review.

(4) The attorney general may adopt rules under chapter 34.05 RCW to implement this chapter.

NEW SECTION. Sec. 10. Exemptions and relationship to other laws.

(1) This chapter does not apply to activities governed by federal law to the extent this chapter conflicts with that law, including uses that federal law expressly preempts.

(2) A deployer that complies with a substantially similar federal requirement for a specific duty is deemed to comply with the matching duty in this chapter.

(3) This chapter supplements and does not limit chapters 19.86, 19.373, 43.386, and 49.60 RCW, or any other remedy under law.

(4) This chapter does not require disclosure of trade secrets, but a trade secret claim does not excuse the notice, explanation, and appeal duties in section 6.

NEW SECTION. Sec. 11. Responsible AI policy (voluntary safe harbor).

A deployer that keeps a written AI policy listing the systems it uses and the risk level of each, trains staff on it annually, maintains a simple way to report AI errors and complaints, and reviews the policy annually, is presumed to have acted in good faith for purposes of penalties under section 9.

NEW SECTION. Sec. 12. Codification.

Sections 1 through 11 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. Sec. 13. Effective date.

Sections 1 through 12 of this act take effect January 1, 2028, except that section 8(2) and the attorney general's rule-making authority under section 9(4) take effect 90 days after adjournment of the session in which this act is passed.

NEW SECTION. Sec. 14. Severability.

If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

--- END ---

Washington AI Guardrails Act™ and AI Guardrails Pledge™ model language. MODEL BILL DRAFT, not legal advice, for discussion with a legislative sponsor.