RIGHT TO RUN

Minnesota Right to Compute and Access Advanced Intelligence Act

State bill · Version 1 · September 2026 · Two articles, 38 sections

Proposed for the 2027 session. Not introduced.

DISCUSSION DRAFT — V1

MINNESOTA LEGISLATURE — PROPOSED 2027 SESSION

H.F. No. _______ · S.F. No. _______

A bill for an act relating to technology and civil rights; establishing rights concerning computational resources and advanced artificial intelligence; protecting lawful access, possession, operation, development, sharing, and distribution; prohibiting direct and indirect capability-based restrictions by government; requiring capability parity between government and the public; protecting access to lawful information; requiring risk management policies for critical infrastructure controlled by artificial intelligence; limiting emergency restrictions; prohibiting retaliation; providing for the expiration and repeal of restrictions; protecting the publication and distribution of model weights; providing for portability of user data; providing civil remedies, damages, and attorney fees; preempting inconsistent local regulation; establishing a public access to advanced intelligence program; appropriating money; proposing coding for new law in Minnesota Statutes.

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

ARTICLE 1 — RIGHTS AND REMEDIES

SECTION 1. SHORT TITLE.

This act may be cited as the "Minnesota Right to Compute and Access Advanced Intelligence Act."

SEC. 2. FINDINGS AND POLICY.

Subdivision 1. Findings. The legislature finds that:

1. Computational resources and artificial intelligence function as tools for communication, education, emergency preparedness, cybersecurity, research, personal safety, technical problem-solving, and protection of persons and property. The rights of free expression and due process guaranteed by the Minnesota Constitution, article I, sections 3 and 7, may be burdened by restrictions on the technological tools through which those rights are exercised, and the legislature may protect those tools by statute.
2. The proper subject of governmental regulation is conduct. A person who commits fraud, intrusion, theft, or violence may be prosecuted for that conduct whether or not an artificial intelligence system assisted it. The capability of a lawfully possessed tool is not itself a harm, and the possibility that a capability could be misused by someone is not a lawful basis for denying it to everyone.
3. A standard permitting government to restrict capability whenever it can articulate a sufficiently weighty interest concedes the question this act is meant to settle. Accordingly, this act does not subject capability-based restrictions to balancing. It withholds the authority to impose them.

4. Governments in the United States have proposed or adopted restrictions on artificial intelligence that turn on the capability of a system rather than on any unlawful conduct. Examples include the training-compute reporting threshold of 10^{26} operations in Executive Order 14110 (October 30, 2023, revoked January 20, 2025); the controls on artificial-intelligence model weights in the January 2025 federal Framework for Artificial Intelligence Diffusion, which the Department of Commerce announced on May 13, 2025, it would not enforce and intended to rescind, but which had not been formally rescinded and remained in the Code of Federal Regulations as of May 2026, the Comptroller General having determined on May 12, 2026, in decision B-337935, that the non-enforcement announcement was itself a rule that had not been submitted to Congress as chapter 8 of title 5, United States Code, requires; the frontier-developer obligations keyed to a 10^{26}-operation training threshold in California's Transparency in Frontier Artificial Intelligence Act (SB 53, 2025); and the compute- and revenue-based thresholds in New York's Responsible AI Safety and Education Act (2025), as amended in 2026 and effective January 1, 2027.
5. Restrictions keyed to capability, compute, parameter count, or benchmark performance do not distinguish lawful from unlawful use. They tend to reserve the most capable tools to government and to large institutions while denying substantially comparable tools to residents, small businesses, researchers, and local governments.
6. Government can restrict access indirectly, by pressuring cloud providers, hardware suppliers, payment processors, or other intermediaries, as readily as it can restrict access directly. The United States Supreme Court held in *National Rifle Association of America v. Vullo*, 602 U.S. 175 (2024), that a government official may not coerce a private party to punish or suppress protected speech on the government's behalf.
7. A resident who is denied access as a result of governmental pressure on an intermediary is ordinarily never told that government was involved, and therefore cannot seek a remedy. Disclosure is what makes the prohibition in section 9 enforceable by the people it protects.
8. Advanced artificial intelligence is increasingly a principal means of access to medical, legal, financial, scientific, and technical information. A requirement that a system withhold from an adult information the adult could obtain from a public library or a licensed professional restricts the resident, not the technology.
9. Montana enacted the first Right to Compute Act in 2025 (Chapter 150, Laws of Montana 2025), pairing a general protection for the ownership and use of computational resources with a risk-management requirement for critical infrastructure controlled by artificial intelligence. That act passed the Montana Senate unanimously and the House of Representatives 61 to 38. This act builds on that approach and departs from it in one respect: Montana subjects a restriction on computational resources to a compelling-interest and narrow-tailoring test, while this act withholds the authority to impose a capability-based restriction rather than subjecting it to that test.
10. Executive Order 14365 (December 11, 2025) directed the United States Attorney General to establish a litigation task force to challenge state artificial intelligence laws, directed federal

agencies to develop preemption standards, and directed the preparation of proposed federal legislation preempting state artificial intelligence laws. This act protects residents against capability-based restrictions imposed by this state, preserves state authority to regulate conduct, and does not depend for its operation on the resolution of that federal question.

11. This act does not alter data center siting, energy use, water use, or generally applicable taxation, which are governed by other law. A tax or fee imposed by reference to the capability of an artificial intelligence system, or to training or inference compute, is a capability-based restriction governed by this act rather than a generally applicable facility tax.

Subd. 2. Policy. It is the policy of this state that a person remains free, for lawful purposes, to acquire and use computational resources; to access advanced artificial intelligence through lawful local, remote, commercial, public, open, or future technological channels; and, where lawfully available, to possess, develop, share, and independently operate artificial intelligence without a government-created capability-based restriction.

Subd. 3. Limits. This act does not immunize independently unlawful conduct and does not compel a private person to disclose trade secrets or provide a service.

SEC. 3. DEFINITIONS.

Subdivision 1. Scope. For purposes of this act, the terms in this section have the meanings given.

Subd. 2. Access. “Access” means the practical ability to obtain and lawfully use an artificial intelligence system or its capabilities through local execution, remote inference, an application programming interface, a commercial or public service, cloud computing, open-weight distribution, distributed computing, or another technological means.

Subd. 3. Adult. “Adult” means a person 18 years of age or older.

Subd. 4. Advanced artificial intelligence. “Advanced artificial intelligence” means an artificial intelligence system exhibiting capabilities at or near the leading edge of demonstrated, nonclassified civilian artificial intelligence capabilities deployed, used, or made available to government, commercial, academic, nonprofit, or other institutional users, regardless of whether equivalent access is then available to residents generally.

Subd. 5. Artificial intelligence system. “Artificial intelligence system” means a machine-based system that, for explicit or implicit objectives, infers from inputs how to generate outputs, including predictions, content, recommendations, decisions, plans, code, analyses, or actions, that can influence physical or virtual environments.

Subd. 6. Capability-based restriction. “Capability-based restriction” means a governmental restriction, whether legal or practical, that limits a person’s ability to acquire, possess, develop, train, publish, share, operate, or access an artificial intelligence system or computational resource because of, or by reference to, the capability of that system or resource, including its intelligence, scale, autonomy, reasoning ability, knowledge, cybersecurity ability, scientific or technical ability, context capacity, tool use, sustained-operation capacity, training or inference compute, parameter count, benchmark performance, architecture, openness or modifiability, or potential for misuse. The term includes such a restriction whether or not it is expressed as a threshold, and whether imposed directly or through a technical proxy or other indirect means described in section 8, subdivision 4.

Subd. 7. Computational resource. “Computational resource” means hardware, software, processors, accelerators, storage, networks, data-center capacity, algorithms, artificial intelligence systems, model weights, and other resources used to perform computation.

Subd. 8. Covered intermediary. “Covered intermediary” means a cloud or hosting provider, hardware supplier, model distributor, application store, payment processor, financial institution, internet or telecommunications provider, data-center operator, state or local contractor, or other person positioned to enable, deny, condition, or materially burden access to computational resources or artificial intelligence.

Subd. 9. Critical infrastructure facility. “Critical infrastructure facility” means a physical or virtual system or asset so vital to this state that its incapacity or destruction would have a debilitating effect on public health, safety, security, or economic well-being, including an electric generation, transmission, or distribution facility; a natural gas, petroleum, or hazardous-liquid pipeline or storage facility; a public water supply or wastewater treatment system; a telecommunications or broadband network; a hospital; a transportation control system; and a dam or flood-control structure.

Subd. 10. Government entity. “Government entity” means the state; an agency, department, board, commission, authority, or office of the state; and a political subdivision or other governmental instrumentality of the state, including an officer, employee, or agent acting in an official capacity.

Subd. 11. Model weights. “Model weights” means numerical or computational parameters learned, generated, or otherwise established during development or training of an artificial intelligence system and used by the system to produce outputs.

Subd. 12. Person. “Person” means a natural person, or a corporation, partnership, limited liability company, association, trust, or other legal entity. Except where this act expressly provides otherwise, a government entity is not a person for purposes of a right protected by sections 5 to 10, 13, or 14.

Subd. 13. Resident. “Resident” means a natural person domiciled in Minnesota, or a business, nonprofit, school, or unit of local government located in Minnesota.

Subd. 14. Specially privileged institution. “Specially privileged institution” means a private person that is permitted by a government entity to possess, operate, or access a capability under a license, exemption, contract, grant, registration, or other governmental authorization that is not made available on neutral terms to residents generally.

Subd. 15. Substantial burden. “Substantial burden”, with respect to a right protected by this act, means a governmental measure that prohibits, or that in practical operation materially impairs, the exercise of that right. The term includes a prohibition, a capability-based license, an excessive or discriminatory fee or tax, an unnecessary registration requirement, an unreasonable delay or waiting period, an institutional-eligibility or credentialing requirement, an excessive identity-verification requirement, and the provision of access that is materially degraded by artificial scarcity, unusable rate limits, materially inadequate context capacity or tool access, insufficient sustained-operation capacity, or restriction to an obsolete or materially less capable version. Nominal availability that ordinary residents cannot practically use is a substantial burden.

Subd. 16. Substantially comparable. "Substantially comparable", with respect to two artificial intelligence capabilities, means that the capabilities perform at materially similar levels across useful task performance, reasoning, planning, coding, scientific and technical work, cybersecurity, multimodal capability, context capacity, tool use, sustained operation, reliability, latency, availability, rate limits, and cost, considered together and without treating any single benchmark, parameter count, compute threshold, or architecture as dispositive. Where article 2 is in effect, the measures listed in section 5, subdivision 2, of that article shall be used. This subdivision applies whether or not article 2 is in effect. A difference in price, interface, branding, rate limit, or terms of service does not by itself make a capability not substantially comparable. The government entity bears the burden of proving that a capability it possesses is not substantially comparable to one it restricts.

Subd. 17. Technical proxy. "Technical proxy" means a measure, including parameter count, training or inference compute, hardware quantity, memory, training cost, benchmark score, context length, autonomy, agentic operation, tool use, multimodality, architecture, openness, modifiability, code-generation ability, cybersecurity capability, scientific capability, or any substantially equivalent criterion, that is used to identify or restrict a system because of its capability rather than because of a specific unlawful use. The term includes any measure, however labeled, the purpose or practical effect of which is to impose a capability-based restriction.

Subd. 18. Willing provider. "Willing provider" means a private or public person that voluntarily offers lawful access to an artificial intelligence system or computational resource, subject to lawful contract terms.

SEC. 4. APPLICABILITY; RULE OF CONSTRUCTION.

Subdivision 1. State and local law. This act applies to state and local law and to the implementation of state and local law, whether adopted before or after the effective date of this act.

Subd. 2. Later statutes. A state law enacted after the effective date of this act is subject to this act unless the later law explicitly excludes application of this act by specific reference to this section.

Subd. 3. Federal supremacy. Nothing in this act authorizes conduct prohibited by controlling federal law. To the fullest extent not preempted, a state or local restriction remains subject to this act.

Subd. 4. Capability alone. Possession of, access to, development of, or use of an otherwise lawful computational or artificial-intelligence capability does not become unlawful under state or local law solely because the capability is advanced, dual-use, capable of cybersecurity research, capable of generating code, or capable of tasks that could also be misused.

Subd. 5. Relationship to federal protection. This act is a floor. A federal statute protecting the rights described in this act, including one that preempts state and local capability-based restrictions, is consistent with this act and does not displace the protections in sections 5 to 14, which continue to bind government entities to the fullest extent permitted. A federal preemption of state artificial-intelligence regulation does not itself create state authority to restrict a right protected by this act.

SEC. 5. RIGHT TO COMPUTE, DEVELOP, SHARE, AND DISTRIBUTE.

Subdivision 1. Computational resources. A person has a statutory right, for lawful purposes, to acquire, own, lease, possess, configure, use, and operate computational resources.

Subd. 2. Development. Protected conduct includes lawful development, training, fine-tuning, testing, evaluation, modification, and creation of artificial intelligence systems and software.

Subd. 3. Sharing. Protected conduct includes lawful publication, distribution, transfer, sharing, collaborative development, and provision of artificial intelligence software, model weights, research, and tools that the person is legally entitled to distribute.

SEC. 6. RIGHT TO ACCESS ADVANCED ARTIFICIAL INTELLIGENCE.

Subdivision 1. Access. A person has a statutory right, for lawful purposes, to seek, obtain, purchase, subscribe to, connect to, and use advanced artificial intelligence made available by a willing provider through any technological means.

Subd. 2. Channel neutrality. Protection under subdivision 1 does not depend on whether access occurs through local execution, remote inference, cloud service, application programming interface, commercial service, public infrastructure, open-weight model, distributed system, or another technological method.

Subd. 3. Substantial burden. A substantial burden includes a prohibition, capability-based license, excessive or discriminatory fee, unnecessary registration requirement, unreasonable delay, institutional-eligibility requirement, or other measure that in practical operation materially impairs protected access.

Subd. 4. No institutional gatekeeping. A government entity may not establish, authorize, or require a system of tiered access under which advanced artificial intelligence is available to institutions, credentialed persons, or approved classes of users on terms materially better than those available to residents generally.

SEC. 7. RIGHT TO POSSESS AND INDEPENDENTLY OPERATE ARTIFICIAL INTELLIGENCE.

Subdivision 1. Possession. A person has a statutory right, for lawful purposes, to acquire, possess, store, copy, and operate artificial intelligence software and model weights that the person is legally entitled to obtain or possess.

Subd. 2. Local and offline operation. A government entity may not require that an otherwise lawful artificial intelligence system be accessible only through a remote provider, continuous network connection, government-controlled service, or revocable provider authorization merely because the system is advanced or highly capable.

Subd. 3. Private inference. A government entity may not require routine disclosure of private prompts, outputs, locally stored model weights, or locally processed information solely as a condition of lawful private operation, except pursuant to lawful compulsory process directed to a particular investigation or proceeding and consistent with constitutional requirements.

SEC. 8. PROHIBITION ON CAPABILITY-BASED RESTRICTIONS.

Subdivision 1. Categorical prohibition. A government entity may not prohibit, license, permit, ration, meter, register, condition, delay, suppress, or otherwise materially burden the lawful acquisition, possession, development, training, fine-tuning, evaluation, publication, distribution, sharing, operation, or access by a person of an artificial intelligence system or computational resource because of, or by reference to, the capability of that system or resource, including its intelligence, scale, autonomy, reasoning ability, knowledge, cybersecurity ability, scientific or technical ability, context capacity, tool use, sustained-operation capacity, training or inference compute, parameter count, benchmark performance, architecture, openness or modifiability, or potential for misuse. Capability-based restriction has the meaning given in section 3.

Subd. 2. Not subject to balancing. A capability-based restriction is void. Section 11 does not apply to, and supplies no authority for, such a restriction. No governmental interest, however weighty, and no degree of tailoring, however narrow, validates a capability-based restriction, and a court shall not weigh the asserted benefits of such a restriction against the rights protected by this act.

Subd. 3. Asserted interests insufficient. An asserted governmental interest in public safety, homeland security, catastrophic risk, systemic risk, technological risk, economic competitiveness, potential misuse, or the capabilities of artificial intelligence generally does not, standing alone or in combination, constitute authority to impose a capability-based restriction.

Subd. 4. No proxy evasion. A capability-based restriction may not be imposed through a technical proxy, a procurement or funding condition, a reporting or registration requirement, a liability rule keyed to capability, an insurance or bonding requirement, a standards or accreditation body, a condition on an unrelated license, a remote attestation or device integrity requirement, a mandatory telemetry or use-reporting requirement, escrow or deposit of model weights with a government entity or its designee, a government-controlled or government-mandated remote disablement capability, a tax or fee imposed by reference to capability or to training or inference compute, a restriction on the sale or transfer of general-purpose computational hardware to a person, or any other indirect means. A restriction imposed through such means is prohibited by subdivision 1 to the same extent as a direct restriction.

Subd. 5. Hardware. A government entity may not require registration, licensing, or reporting of general-purpose computational hardware because the hardware exceeds a computing-capacity threshold.

Subd. 6. Conduct unaffected. Nothing in this section limits the authority of a government entity to prohibit, investigate, prosecute, or punish conduct that is independently unlawful, including such conduct committed with the assistance of an artificial intelligence system and including conduct furthering a harm described in section 12. Liability attaches to the conduct and not to the capability employed.

Subd. 7. Infrastructure regulation not affected. This act does not limit a state or local law of general application governing the siting, zoning, construction, permitting, energy use, energy rates, water use, water discharge, noise, emissions, or taxation of a data center, power plant, or other physical facility, or a law regulating a separately regulated facility or activity, when that law regulates the facility or activity rather than computation itself. Such a law is not a capability-based restriction.

SEC. 9. PROHIBITION ON INDIRECT GOVERNMENT RESTRICTIONS.

Subdivision 1. Anti-circumvention. A government entity may not coerce, threaten, materially pressure, direct, induce, or condition a license, grant, contract, procurement opportunity, regulatory benefit, or other governmental advantage on a covered intermediary taking an action that the government entity could not lawfully require directly under this act.

Subd. 2. Practical effect. A court shall examine the substance and practical effect of governmental conduct, including threatened adverse action, repeated or coordinated requests, conditioning of governmental benefits, and whether a reasonable intermediary would understand the communication as carrying governmental consequences.

Subd. 3. Standing of affected persons. A person whose access to a computational resource or artificial intelligence system is denied, conditioned, or materially degraded by a covered intermediary as a result of conduct prohibited by subdivision 1 has suffered an injury for purposes of section 19, whether or not the intermediary itself objects.

Subd. 4. Public data. A written or recorded communication from a government entity to a covered intermediary requesting, directing, or encouraging the intermediary to deny, condition, or restrict access to a computational resource or artificial intelligence system is public data under Minnesota Statutes, chapter 13, except to the extent another provision of that chapter classifies the specific data as not public, including active criminal investigative data under section 13.82 and security information under section 13.37. A government entity shall retain each such communication for not less than three years.

Subd. 5. Notice to affected persons. A government entity that requests, directs, or encourages a covered intermediary to deny, terminate, or materially degrade an identified person's access shall notify that person in writing not later than 30 days after making the communication, and shall state the capability or access restricted and the reason. Notice may be delayed while, and only while, a court of competent jurisdiction finds that notice would compromise an active criminal investigation, and must be provided not later than 30 days after the delay ends.

Subd. 6. Private choice preserved. Nothing in this section restricts an intermediary from independently setting lawful terms, declining service, managing capacity, or taking action for bona fide commercial, security, fraud-prevention, or safety reasons not materially induced by conduct prohibited by subdivision 1.

Subd. 7. Lawful government communication. This section does not prohibit lawful compulsory process, a court order, communication concerning specific independently unlawful conduct, or a content-neutral procurement requirement, provided it is not used to accomplish indirectly a restriction that would violate this act if imposed directly.

SEC. 10. LAWFUL SAFETY, SELF-PRESERVATION, AND RESILIENCE.

Subdivision 1. Protected purposes. Protected use includes lawful use of artificial intelligence for personal safety; emergency preparedness and response; navigation; communications continuity; cybersecurity of systems the person owns or is authorized to protect; disaster recovery; infrastructure diagnostics; technical repair; environmental hazards; scientific, medical, or engineering information; protection of property; and other lawful activities relating to safety, autonomy, self-preservation, or resilience.

Subd. 2. Parity in defensive capability. A government entity may not restrict a person's protected use under subdivision 1 on the ground that the capability is equal to or greater than a capability the government entity or a specially privileged institution uses for the same protected purpose. Such a restriction is a capability-based restriction and is void under section 8.

Subd. 3. Offline and degraded conditions. Because protected use under subdivision 1 is most needed when networks, providers, or public services are unavailable, a government entity may not condition that use on continuous connectivity, remote authorization, or provider approval.

Subd. 4. No expansion of authority. This section does not authorize unauthorized computer access, unlawful physical force, unlicensed professional practice where licensure is otherwise validly required, interference with critical infrastructure, or another independently unlawful act.

SEC. 11. STANDARD FOR GOVERNMENT RESTRICTIONS.

Subdivision 1. Burden. A government entity bears the burden of proving by clear and convincing evidence that a substantial burden on a right protected by sections 5 to 10, 13, or 14, other than a capability-based restriction prohibited by section 8, furthers a compelling governmental interest and is narrowly tailored using the least restrictive reasonably available means.

Subd. 2. Particularized findings. The government entity must identify the specific capability, use, person, system, or circumstance creating the alleged risk; the reasonably anticipated harm; the supporting evidence; the persons affected; the duration; and why regulation of independently harmful conduct or a narrower technical or user-specific restriction would not adequately address the risk.

Subd. 3. Generalized fear insufficient. A generalized assertion that advanced artificial intelligence, autonomy, cybersecurity capability, code generation, scientific capability, or another broad class of capability could be misused is insufficient by itself to satisfy subdivision 1.

Subd. 4. Harms of denial. A court shall consider the reasonably foreseeable harms caused by denial or degradation of access, including effects on defensive capability, personal safety, emergency preparedness, research, competition, accessibility, continuity, and infrastructure resilience.

Subd. 5. No deference. In an action under section 19, a court shall determine all questions of law de novo and shall not defer to a government entity's interpretation of this act or of the scope of its own authority under this act.

Subd. 6. No application to capability-based restrictions. This section supplies no authority for a capability-based restriction prohibited by section 8. Such a restriction is void under that section without regard to any showing that could be made under this section, and a government entity may not defend such a restriction by satisfying this section.

SEC. 12. RECOGNIZED COMPELLING INTERESTS.

Subdivision 1. In general. Each interest described in subdivisions 2 to 4 is a compelling governmental interest for purposes of section 11, subdivision 1, and may be furthered by the prohibition, investigation, and punishment of independently unlawful conduct. No interest described in this section constitutes authority for a capability-based restriction prohibited by section 8.

Subd. 2. Weapons of mass destruction. Preventing the development, acquisition, or use of a chemical, biological, radiological, or nuclear weapon.

Subd. 3. Critical infrastructure and unauthorized access. Preventing unauthorized access to, intrusion into, disruption of, or damage to a critical infrastructure facility or a computer system that the actor does not own and is not authorized to access.

Subd. 4. Protection of minors. Preventing the sexual exploitation of minors, the production or distribution of material described in Minnesota Statutes, section 617.246, and the distribution to minors of material that is obscene as to minors.

Subd. 5. Tailoring still required. Subdivision 1 does not relieve a government entity of the burden under section 11 to demonstrate, with particularized evidence, that:

1. the restricted capability provides material uplift toward the harm identified, beyond the uplift available through published literature, generally available tools, and other lawful means; and
2. a restriction limited to the specific uplifting capability, or to independently unlawful conduct, would not adequately address the risk.

Subd. 6. No general ceiling. A restriction under this section may not take the form of a general capability-based restriction or technical proxy applied to advanced artificial intelligence as a class.

Subd. 7. Protected use unaffected. Nothing in this section authorizes a restriction on protected use under section 10. That a capability usable to secure a system is also usable to attack one is not, by itself, sufficient to satisfy subdivision 5.

Subd. 8. Age verification neutrality. A measure taken under subdivision 4 may not require a person to submit government-issued identification, biometric data, or a persistent identifier as a condition of access to an artificial intelligence system, where a less intrusive means of age assurance is reasonably available.

Subd. 9. No capability exception. Neither this section nor any other provision of law may be construed to permit a capability-based restriction prohibited by section 8 on the ground that a restricted capability could be used to bring about a harm described in this section. Where such a harm is threatened, the authority of the state is to prohibit, investigate, and punish the conduct that would produce it, without regard to the capability of any tool employed.

SEC. 13. CAPABILITY PARITY.

Subdivision 1. General rule. A government entity may not possess, procure, operate, or use a nonclassified civilian artificial intelligence capability while any state or local law, rule, order, or other governmental action restricts residents generally from acquiring, possessing, accessing, or operating a substantially comparable capability from a willing provider.

Subd. 2. Specially privileged institutions. Subdivision 1 applies with equal force where the capability is possessed, operated, or accessed by a specially privileged institution under a governmental license, exemption, contract, grant, registration, or other authorization not available to residents on neutral terms.

Subd. 3. Effect of violation. Where subdivision 1 or 2 is violated, the restriction on residents, and not the governmental possession, procurement, operation, or use, is the governmental action that is void as applied to residents. The remedy provided by this subdivision is the exclusive consequence of a violation of subdivision 1 or 2, and nothing in this section requires a government entity to cease possessing, procuring, operating, or using a capability, or authorizes a court to enjoin it from doing so. Where the restriction is a capability-based restriction, it is void under section 8 without regard to section 11. In any other case, the fact of governmental or privileged-institution possession is conclusive evidence that the restriction is not the least restrictive reasonably available means under section 11, subdivision 1.

Subd. 4. No tiered eligibility. A government entity may not condition a person’s acquisition of, access to, or operation of an artificial intelligence system on the person’s institutional affiliation, accreditation, professional licensure, employment, security clearance, contractual relationship with a government entity, corporate size, research credential, or membership in any class of approved users.

Subd. 5. Disclosure of state capability. By October 1 of each year, the commissioner of information technology services shall publish a description, at a level of generality consistent with operational security, of the nonclassified civilian artificial intelligence capabilities in use across state agencies, including capabilities not then meaningfully available to residents. The commissioner shall transmit the description to the chairs and ranking minority members of the legislative committees with jurisdiction over state government finance and policy.

Subd. 6. Exclusions. This section does not apply to a capability the possession of which is restricted by federal law, to a system used solely for a law-enforcement operational purpose and not offered for civilian use, or to information classified under federal law.

Subd. 7. Rule of construction. This section imposes no obligation on a private person and does not require any developer to offer, sell, license, or disclose any system or capability.

SEC. 14. ACCESS TO LAWFUL INFORMATION.

Subdivision 1. General rule. A government entity may not require, request under circumstances described in section 9, subdivision 1, or condition any benefit upon, the design or configuration of an artificial intelligence system to withhold from an adult information that the person could lawfully obtain from a public library, a published work, a generally available search engine, a government publication, or a licensed professional.

Subd. 2. No mandated refusal lists. A government entity may not maintain, distribute, or require adherence to a list of subjects, viewpoints, questions, or categories of lawful information that an artificial intelligence system must decline to address.

Subd. 3. Scientific, medical, legal, and technical information. Subdivision 1 applies with particular force to information concerning medicine, health, law, personal finance, engineering, cybersecurity of systems the person owns or is authorized to protect, agriculture, emergency preparedness, and scientific research.

Subd. 4. Private editorial discretion preserved. Nothing in this section limits a private provider's own decisions about the content, configuration, or behavior of a system it develops or operates, and nothing in this section requires a provider to produce any particular output.

Subd. 5. Exceptions. This section does not apply to a restriction that is not prohibited by section 8 and that both satisfies section 11 and falls within an interest recognized under section 12, or to information the disclosure of which is prohibited by state or federal law.

Subd. 6. Minors. This section governs access by adults. Nothing in this section limits a measure taken under section 12, subdivision 4, subject to section 12, subdivision 8.

SEC. 15. CRITICAL INFRASTRUCTURE CONTROLLED BY ARTIFICIAL INTELLIGENCE.

Subdivision 1. Risk management policy. A person that deploys an artificial intelligence system to control, in whole or in part, the operation of a critical infrastructure facility shall adopt and maintain a written risk management policy that is reasonable in light of the facility's function and that considers the current version of the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework, ISO/IEC 42001, or another nationally or internationally recognized artificial-intelligence risk-management standard.

Subd. 2. Human shutdown. The policy must ensure that an authorized person can, at all times, halt or override the artificial intelligence system's control of the facility.

Subd. 3. Enforcement. The attorney general or the commissioner of public safety may bring an action in district court for injunctive relief to compel compliance with this section. This section does not create a private right of action.

Subd. 4. Not a capability-based restriction. A requirement under this section regulates the operation of a critical infrastructure facility and is not a capability-based restriction or a substantial burden under this act.

Subd. 5. Small entities. This section does not apply to a person that, together with its affiliates, employs fewer than 50 individuals, unless the person operates a critical infrastructure facility serving more than 10,000 customers.

SEC. 16. EMERGENCY RESTRICTIONS.

Subdivision 1. Findings and duration. An executive emergency action, including an order issued under Minnesota Statutes, chapter 12, that substantially burdens a right protected by this act, other than a capability-based restriction prohibited by section 8, must state particularized findings satisfying section 11 and expires not later than 30 days after taking effect, notwithstanding an extension of the underlying peacetime emergency approved by the Executive Council under Minnesota Statutes, section 12.31, subdivision 2.

Subd. 2. Continuation. A restriction under subdivision 1 may continue beyond 30 days only by a law enacted by the legislature that specifically identifies the restricted capability or class, states an expiration date, and preserves judicial review under section 19.

Subd. 3. No reset. The executive branch may not evade subdivision 2 by rescinding and reissuing, renaming, or materially reproducing a substantially identical restriction based on the same emergency facts.

Subd. 4. Expedited review. A court hearing a challenge to an emergency restriction shall expedite consideration to the greatest extent practicable.

Subd. 5. No capability-based restrictions. No emergency, declaration, finding of exigency, or action under this section, under Minnesota Statutes, chapter 12, or under any other authority permits a capability-based restriction prohibited by section 8. The existence of an emergency does not enlarge the authority of a government entity under this act.

SEC. 17. RULEMAKING; REQUIRED STATEMENT.

Subdivision 1. Statement of need and reasonableness. An agency proposing a rule under Minnesota Statutes, chapter 14, that would impose a capability-based restriction, use a technical proxy, or otherwise substantially burden a right protected by sections 5 to 14 shall include in the statement of need and reasonableness required by section 14.131 the particularized findings described in section 11, subdivision 2.

Subd. 2. Effect of omission. A rule adopted without the statement required by subdivision 1 is invalid to the extent it burdens a right protected by this act, and the omission may be raised in a proceeding under section 19 or under section 14.44.

Subd. 3. No independent authority. Nothing in this act authorizes a government entity to adopt a rule restricting a right protected by this act.

SEC. 18. PRIVATE PROVIDERS; PROPERTY; TRADE SECRETS.

Subdivision 1. No compelled service. Nothing in this act requires a private provider to offer a product or service, continue a contractual relationship, provide unlimited or uncompensated inference, or serve a particular person.

Subd. 2. No compelled disclosure. Nothing in this act requires a private person to disclose proprietary model weights, source code, trade secrets, copyrighted material, confidential information, or privately owned computational resources absent separate lawful authority.

Subd. 3. Voluntary transactions. A government entity may not prohibit or materially burden a lawful transaction between a person and a willing provider merely because the transaction provides access to advanced artificial intelligence, except under a restriction that is not prohibited by section 8 and satisfies section 11.

SEC. 19. ENFORCEMENT AND REMEDIES.

Subdivision 1. Cause of action. A person suffering an actual legal injury or a credible and imminent threat of legal injury from conduct alleged to violate this act, including an injury described in section 9, subdivision 3, may bring a civil action for declaratory, injunctive, or monetary relief in district court against the responsible government entity or official in an official capacity.

Subd. 2. Consent to suit. The state and its agencies consent to suit for the relief provided by this section. This consent extends to an award under subdivision 8 and does not otherwise waive immunity for money damages.

Subd. 3. Defense. A person may assert this act as a claim, defense, or ground for equitable relief in a state civil, administrative, licensing, forfeiture, or enforcement proceeding in which government action would burden a protected right.

Subd. 4. Attorney fees. The court shall award reasonable attorney fees and litigation costs to a prevailing plaintiff, or to a person who prevails on a defense under subdivision 3, unless the court finds special circumstances that would make an award unjust. No award of attorney fees or costs may be made against a plaintiff under this act.

Subd. 5. No exhaustion. Exhaustion of an administrative remedy is not required before an action under this section unless a Minnesota statute enacted after this act expressly requires exhaustion by specific reference to this section.

Subd. 6. Preliminary relief. In determining whether to grant temporary or preliminary relief, a court shall treat the threatened loss of a right protected by this act as an injury capable of supporting equitable relief when the other requirements for such relief are satisfied. A showing that a government entity has substantially burdened a protected right without making the findings required by section 11, subdivision 2, establishes a rebuttable presumption of irreparable harm.

Subd. 7. No dismissal for ripeness. A court may not dismiss an action under this section on the ground that the plaintiff has not been subjected to enforcement, where the plaintiff alleges that the plaintiff has refrained or will refrain from protected conduct because of the challenged governmental action.

Subd. 8. Damages. In an action under this section, a court may award:

1. statutory damages of not less than $1,000 for each violation, without proof of actual injury. For purposes of this clause, each discrete governmental action that burdens a protected right of a plaintiff is one violation, and continuation of a single action over time is not a separate violation for each day it remains in effect. The total statutory damages awarded to a single plaintiff under this clause for violations arising from the same governmental action may not exceed $50,000, and this limit does not apply to an award under clause (2);
2. compensatory damages for financial loss, lost business or research opportunity, and out-of-pocket costs proximately caused by the violation.

Subd. 9. Immunities. Statutory immunity, official immunity, and vicarious official immunity are not defenses to an action under this section. This section does not create personal liability for an officer or employee sued in an individual capacity, and an award under subdivision 8 is payable by the responsible government entity.

Subd. 10. Expedited schedule. The government entity shall file the particularized findings required by section 11, subdivision 2, or a statement that none were made, not later than 30 days after service of the complaint.

Subd. 11. Venue. An action may be brought in the county in which the plaintiff resides or maintains a principal place of business, in which a substantial part of the events occurred, or in Ramsey County.

SEC. 20. ANTI-RETALIATION; UNCONSTITUTIONAL CONDITIONS.

Subdivision 1. Retaliation prohibited. A government entity may not deny, revoke, delay, condition, or take any adverse action with respect to a grant, contract, license, permit, certification, accreditation, employment, benefit, procurement opportunity, tax treatment, or regulatory approval because a person has:

1. exercised a right protected by this act;
2. acquired, possessed, developed, shared, accessed, or operated a computational resource or artificial intelligence system of any level of capability;
3. brought or participated in an action under section 19; or
4. petitioned under section 21 or testified, assisted, or provided information concerning a violation of this act.

Subd. 2. No waiver. A government entity may not require, as a condition of any benefit described in subdivision 1, that a person waive, limit, or agree not to assert a right protected by this act. A purported waiver obtained in violation of this subdivision is void and unenforceable.

Subd. 3. Contract terms. A term in a state or local contract, grant, or cooperative agreement that restricts a person's exercise of a right protected by this act beyond what is necessary to perform the instrument is void.

Subd. 4. Remedy. A violation of this section is enforceable under section 19, including under subdivisions 8 and 9 of that section.

SEC. 21. EXPIRATION AND REPEAL OF RESTRICTIONS.

Subdivision 1. Expiration. A rule, order, or other governmental action, other than a law enacted by the legislature, that substantially burdens a right protected by this act expires:

1. in the case of an action that first takes effect on or after the effective date of this act, three years after the date it takes effect; and
2. in the case of an action in effect on the effective date of this act, three years after that date.

Subd. 2. Republication. An action that is not a capability-based restriction prohibited by section 8 does not expire under subdivision 1 if, before the applicable date, the government entity republishes the particularized findings required by section 11, subdivision 2, updated to reflect then-current facts, and affords not less than 60 days for public comment. A capability-based restriction prohibited by section 8 is void under that section, may not be preserved by republication, and is not made lawful by any finding, comment period, or period of non-enforcement.

Subd. 3. No perpetual restriction. An action republished under subdivision 2 is subject to the same three-year limit on each occasion.

Subd. 4. Petition for repeal. A person may petition a government entity to repeal or narrow a governmental action alleged to violate this act. The government entity shall issue a reasoned written decision not later than 120 days after receipt.

Subd. 5. Failure to act. A government entity's failure to issue a timely decision under subdivision 4 is reviewable under section 19, and the challenged action is suspended as to the petitioner pending decision.

Subd. 6. Annual inventory. By January 15 of each year, the attorney general shall publish an inventory of every state governmental action then in effect that substantially burdens a right protected by this act, the compelling interest asserted for each, and the date each expires under subdivision 1. An action omitted from the inventory is unenforceable until published.

SEC. 22. GENERALLY APPLICABLE LAW; FEDERAL LAW.

Subdivision 1. Unlawful conduct. Nothing in this act creates immunity from laws governing fraud, theft, extortion, stalking, threats, violence, child exploitation, privacy, intellectual property, unauthorized computer access, destruction of property, critical infrastructure, weapons, controlled substances, consumer protection, unfair or deceptive trade practices, professional conduct, or professional licensure, when those laws regulate independently unlawful conduct rather than capability as such.

Subd. 2. Product liability and negligence. A generally applicable product liability, negligence, warranty, or duty-of-care standard is not a capability-based restriction or a technical proxy solely because the standard of care or the scope of a duty takes account of the foreseeable risk presented by a system, including risk that varies with what the system is able to do. This subdivision does not permit a rule that conditions the lawfulness of acquiring, possessing, developing, publishing, or operating a system on its capability.

Subd. 3. Purpose-built unlawful tools. A law that prohibits or conditions the development, marketing, offering, or distribution of a product or service that is designed, marketed, or primarily used to produce a result that is independently unlawful, including a nonconsensual intimate image, material described in Minnesota Statutes, section 617.246, or a forged identification document, regulates that conduct and is not a capability-based restriction. This subdivision does not permit a restriction on a general-purpose artificial intelligence system or computational resource by reason of the capability of that system or resource, and the existence of an unlawful use to which a general-purpose system could be put is not within this subdivision.

Subd. 4. Safety regulation of regulated products and activities. A law governing the safety, operation, certification, or licensing of a motor vehicle, aircraft, vessel, unmanned aircraft system, medical device, or other separately regulated product or activity is not a capability-based restriction or a technical proxy solely because it classifies, conditions, or restricts by reference to the degree of automation or autonomous operation of the product, or to the demonstrated performance of a function the product performs, where the law regulates that product or activity rather than the acquisition, possession, development, publication, or general operation of an artificial intelligence system or computational resource.

Subd. 5. No relabeling. A government entity may not avoid this act by relabeling a restriction on computation, possession, sharing, or access as a regulation of conduct when its practical operation is to prohibit a protected capability as such.

Subd. 6. Federal law. Nothing in this act authorizes conduct prohibited by controlling federal law. State and local restrictions remain subject to this act to the fullest extent not preempted by federal law.

SEC. 23. LOCAL PREEMPTION.

The regulation of rights protected by this act is a matter of statewide concern. A political subdivision may not enact or enforce an ordinance, rule, licensing condition, procurement condition, or other requirement that conflicts with this act or provides less protection for a right established by this act. This section does not limit a political subdivision’s authority described in section 8, subdivision 7.

SEC. 24. PUBLICATION AND DISTRIBUTION OF MODEL WEIGHTS.

Subdivision 1. Protected conduct. The creation, publication, distribution, transfer, receipt, retention, modification, fine-tuning, evaluation, and redistribution of model weights, source code, training methods, and technical documentation for an artificial intelligence system are protected conduct under section 5 and are expressive activity for purposes of this act.

Subd. 2. No prior restraint. A government entity may not require prior approval, licensure, registration, notification, or review as a condition of publishing or distributing model weights that a person is otherwise lawfully entitled to possess.

Subd. 3. Capability not a basis. A government entity may not prohibit, condition, or burden the publication or distribution of model weights on the ground that the system is advanced, open-weight, modifiable, capable of being fine-tuned, or capable of being operated without the supervision of its developer.

Subd. 4. No duty to supervise downstream use. A person who lawfully publishes model weights is not, by reason of that publication alone, required to monitor, restrict, authenticate, or retain records of persons who obtain them, and is not liable under state law for the independently unlawful conduct of another person who obtains them.

Subd. 5. Construction of section 5, subdivision 3. For purposes of section 5, subdivision 3, a governmental restriction that does not satisfy this section does not render a person not legally entitled to distribute model weights.

Subd. 6. Exceptions. This section does not apply to a restriction that is not prohibited by section 8 and that both satisfies section 11 and falls within an interest recognized under section 12, to the intellectual property laws or the terms of a license under which the person obtained the weights, to information classified under federal law, or to conduct prohibited by controlling federal law, including export control and sanctions law.

Subd. 7. No compelled publication. Nothing in this section requires any developer to publish model weights, to adopt an open-weight release strategy, or to disclose any system, capability, or documentation.

SEC. 25. PORTABILITY OF USER DATA AND CUSTOMIZATIONS.

Subdivision 1. In general. A covered intermediary that, in the preceding calendar year, provided artificial intelligence systems or computational resources to more than 25,000 residents shall, upon the request of a resident, provide that person with a copy of:

1. the person's prompts, inputs, outputs, conversation history, and uploaded files;
2. stored context, instructions, memory, and configuration the person supplied; and
3. to the extent technically separable from the developer's base model and from the data of other persons, the parameters of any customization or fine-tuning the person created using the person's own data.

Subd. 2. Form and timing. The copy must be provided in a structured, commonly used, machine-readable format not later than 30 days after the request, at no charge for the first two requests in a calendar year, and without requiring the person to waive any right or to continue the service.

Subd. 3. No government interference. A government entity may not prohibit, condition, or materially burden the export, retention, or transfer by a person of material described in subdivision 1.

Subd. 4. Exceptions. Subdivision 1 does not require disclosure of the developer's base model weights, trade secrets, safety or abuse-prevention systems, or the data of another person, and does not apply where disclosure is prohibited by law.

Subd. 5. Relationship to chapter 325M. The right under this section is in addition to, and does not limit, replace, or condition, the right to obtain personal data under Minnesota Statutes, section 325M.14, subdivision 1, or any other right under Minnesota Statutes, chapter 325M. This section reaches material that section 325M.14 does not, including outputs generated by an artificial intelligence system and the parameters of a customization the person created, and applies at a lower threshold and to persons who are not consumers within the meaning of chapter 325M. Where a single request falls within both this section and section 325M.14, one response that satisfies the requirements of both discharges both, and a covered intermediary is not required to respond twice. Nothing in this section excuses compliance with chapter 325M, and compliance with chapter 325M does not by itself discharge a duty under this section.

Subd. 6. Enforcement. The attorney general may enforce subdivisions 1 and 2 under Minnesota Statutes, section 8.31. This section does not create a private right of action.

SEC. 26. SEVERABILITY.

If any provision of this act or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application. This paragraph applies to each section, subdivision, and clause separately.

Sections 13, 14, 15, 20, 21, 24, and 25 are each independently severable from one another and from the remainder of this act. If any of them is held invalid, the remaining provisions have full force and effect, and no inference may be drawn that the legislature would not have enacted them absent the invalid provision.

If section 19, subdivision 9, is held invalid, the remainder of section 19 has full force and effect, and the immunities otherwise available under Minnesota Statutes, chapter 3 or 466, apply to an action under that section.

Article 2 is severable from this article, and the rights and remedies in this article do not depend on the enactment, funding, or operation of article 2.

SEC. 27. EFFECTIVE DATE.

This article is effective the day following final enactment, except that section 13, subdivision 5, section 15, and section 25, subdivisions 1 and 2, are effective July 1, 2027.

ARTICLE 2 — PUBLIC ACCESS TO ADVANCED ARTIFICIAL INTELLIGENCE

SECTION 1. PURPOSE.

The rights in article 1 protect access to advanced artificial intelligence that a willing provider offers. This article ensures that some advanced capability remains available to Minnesota residents on neutral terms even if commercial, academic, and open channels fail to provide it, and that the state corrects any access gap it causes.

SEC. 2. DEFINITIONS.

Subdivision 1. Scope. The definitions in article 1, section 3, apply to this article. In addition, the terms in this section have the meanings given.

Subd. 2. Board. “Board” means the Board of Regents of the University of Minnesota.

Subd. 3. Institute. “Institute” means the Minnesota Supercomputing Institute of the University of Minnesota, or a successor unit designated by the board.

Subd. 4. Program. “Program” means the Minnesota advanced intelligence access program established under section 3.

Subd. 5. Resident. “Resident” means a natural person domiciled in Minnesota, or a business, nonprofit, school, or unit of local government located in Minnesota.

SEC. 3. MINNESOTA ADVANCED INTELLIGENCE ACCESS PROGRAM.

Subdivision 1. Request. The board is requested to establish and operate, through the institute, a Minnesota advanced intelligence access program that provides meaningful resident access to advanced artificial intelligence.

Subd. 2. Methods. The program may use any combination of: (1) hosted inference of open-weight models at or near the leading edge of publicly available open-weight capability; (2) purchase or subsidy of commercial access to advanced artificial intelligence for residents on neutral eligibility terms; (3) shared compute and reserved inference capacity on institute infrastructure; (4) participation in and matching of the federal National Artificial Intelligence Research Resource or a successor program; (5) grants to Minnesota public libraries, schools, and local governments for access; and (6) negotiated public-use rights in systems the state substantially funds. The program should avoid a single point of failure where reasonably practicable.

Subd. 3. Eligibility. Eligibility may not be limited to state contractors, large corporations, accredited institutions, or another institutionally preferred class. Reasonable neutral rules may be used for residency verification, age, capacity management, fraud prevention, sanctions compliance, and acceptable-use enforcement.

Subd. 4. Baseline allotment. The program is requested to provide to each adult resident who requests it, at no charge, a baseline allotment of access to advanced artificial intelligence sufficient for ordinary personal, educational, civic, and small-business use, as measured against the standards published under section 4. The institute may set neutral periodic limits on the allotment based on available capacity, and is requested to publish those limits. The baseline allotment may not be conditioned on income, employment, institutional affiliation, or credential.

Subd. 5. Priority populations. In allocating capacity beyond the baseline allotment, the program is requested to give priority to residents in rural areas, residents with low incomes, residents with disabilities, public schools, public libraries, Tribal governments and Tribal colleges, and units of local government, and to ensure that the program's interfaces are accessible and support languages other than English in proportion to demonstrated need.

Subd. 6. No restrictive authority. Nothing in this article authorizes the board, the institute, or any government entity to prohibit, license, register, restrict, or create a presumption against private possession, development, sharing, or access.

SEC. 4. ACCESS STANDARDS.

Subdivision 1. Standards. The board is requested to publish measurable minimum standards for the program covering affordability, availability, useful capacity, context capacity, tool access, sustained operation, reliability, rate limits, and wait time.

Subd. 2. Nominal availability insufficient. Compliance with this article may not be based solely on the nominal availability of an interface or model that ordinary residents cannot practically use.

Subd. 3. Parity benchmark. The standards published under subdivision 1 are requested to be set by reference to the capabilities described in the most recent assessment under section 5 as deployed, used, or made available to state agencies, and to state, for each measure, the percentage of that capability the program delivers to residents. Where the program delivers less than full parity, the institute is requested to publish the reason and the date by which parity is expected.

Subd. 4. Capability floor. Not later than 180 days after a capability enters the comparison under section 5, the program is requested to make available to residents a substantially comparable capability. A determination under this subdivision is to be made on the measures listed in section 5, subdivision 2, considered together, and no single benchmark, parameter count, compute threshold, or architecture may be dispositive. Publication of a reason or an expected date under subdivision 3 does not satisfy this subdivision.

Subd. 5. Review of the floor. A failure to meet subdivision 4 is a reviewable determination for purposes of section 7 and triggers the corrective duty under section 6. The board bears the burden of showing that a capability in the comparison is not substantially comparable to one the program provides.

SEC. 5. CAPABILITY AND ACCESS ASSESSMENT.

Subdivision 1. Assessment. The board is requested to publish, through the institute, a quarterly public assessment comparing (1) demonstrated, nonclassified advanced artificial-intelligence capabilities used by or available to state agencies, commercial entities, academic institutions, and other institutional users, with (2) capabilities meaningfully available to residents through market, open, academic, nonprofit, and public channels, including the program.

Subd. 2. Measures. The assessment shall consider useful task performance, reasoning, planning, coding, scientific and technical work, cybersecurity, multimodal capability, context capacity, tool use, sustained operation, reliability, latency, availability, rate limits, and cost. No single benchmark, parameter count, compute threshold, or architecture may be dispositive.

Subd. 3. Material advance. The board is requested to publish a supplemental assessment within 30 days after identifying a material advance in demonstrated nonclassified capability.

Subd. 4. Reporting. The institute is requested to transmit each assessment to the chairs and ranking minority members of the legislative committees with jurisdiction over higher education, commerce, and state government finance.

SEC. 6. CORRECTIVE DUTY.

Subdivision 1. Trigger. A corrective duty arises when an assessment under section 5 finds a material gap between institutional capability and meaningful resident access that is attributable in whole or substantial part to (1) a restriction imposed by a government entity; (2) routine possession or use by state agencies of materially more capable nonclassified systems than are meaningfully available to residents; or (3) loss of a previously relied-upon public access pathway.

Subd. 2. Plan. Within 60 days after a triggering assessment, the board is requested to publish a corrective access plan and the commissioner of management and budget shall include in the next budget submission any appropriation the plan identifies as necessary. If the gap arises under subdivision 1, clause (1), and the restriction is a capability-based restriction prohibited by article 1, section 8, the responsible government entity shall withdraw the restriction within the same 60 days, and publication of findings does not satisfy this subdivision. If the gap arises under subdivision 1, clause (1), and the restriction is not prohibited by article 1, section 8, the entity shall, within the same 60 days, either withdraw the restriction or publish the findings required by article 1, section 11.

Subd. 3. Restoration. Where the gap arises from a state-operated pathway, the plan must provide for restoration of compliant access within 90 days after the assessment unless the legislature provides otherwise by law.

Subd. 4. Rights not contingent. Failure to fund or implement a plan under this section does not suspend or diminish the rights, prohibitions, or remedies in article 1.

SEC. 7. PETITIONS.

Subdivision 1. Petition. A resident may petition the institute alleging that the program does not meet the standards under section 4 or that state action has created a gap described in section 6.

Subd. 2. Determination. The institute is requested to issue a reasoned written determination within 60 days, or within 30 days if the petition credibly alleges imminent loss of the only meaningful public access pathway.

Subd. 3. Review. Where a petition alleges a gap attributable to a restriction imposed by a government entity under section 6, subdivision 1, clause (1), the restriction is reviewable under article 1, section 19. Nothing in this section creates a cause of action against the board or the institute.

SEC. 8. PRIVACY AND CONTINUITY.

Subdivision 1. Data minimization. The program shall collect and retain only information reasonably necessary for account administration, billing if any, abuse prevention, security, legal compliance, and service operation.

Subd. 2. Content use. User prompts, files, outputs, and conversation content may not be used for advertising, commercial profiling, or unrelated model training without affirmative opt-in consent.

Subd. 3. Retention. Absent user direction, a documented security incident, or a specific legal preservation duty, content must be deleted or de-identified as soon as reasonably practicable and not later than 30 days after the program no longer requires it for operational delivery.

Subd. 4. Disclosure. Disclosure of user content must be authorized by law and supported by legal process appropriate to the information sought. Aggregate or de-identified service metrics may be used for program administration and public reporting.

Subd. 5. Continuity. The program shall maintain a continuity plan and, where reasonably practicable, at least two technically independent access pathways or reserve capacity sufficient to restore compliant service within 30 days after a material pathway fails or is discontinued.

SEC. 9. COST MODEL.

The board is requested to include in its first biennial budget request after enactment a cost model for the program at pilot, statewide-baseline, and high-capacity service levels, including inference or compute capacity, expected concurrent users, unit costs, privacy and security costs, continuity capacity, and expected appropriations for five fiscal years.

SEC. 10. APPROPRIATION.

$________ in fiscal year 2028 and $________ in fiscal year 2029 are appropriated from the general fund to the Board of Regents of the University of Minnesota for the program under this article. Money appropriated under this section is available until June 30, 2029.

SEC. 11. EFFECTIVE DATE.

This article is effective July 1, 2027.