

CHAPTER 57-A OF THE CONSOLIDATED LAWS
STATE TECHNOLOGY LAW

Article		Section
I	Office of Information Technology Services	(§§ 101-107)
II	Internet Security and Privacy Act	(§§ 201-210)
III	Electronic Signatures and Records Act	(§§ 301-309)
IV	Automated employment decision-making in state government	(§§ 401-402-a)

ARTICLE I

OFFICE OF INFORMATION TECHNOLOGY SERVICES

Section 101.	Definitions.
102.	Office of information technology services; director, organization and employees.
103.	Functions, powers and duties of the office.
103-a.	State information technology innovation center.
103-b.	Gender-neutral terminology; state agencies.
103-c.	State agency websites; mobile friendly websites.
103-c*2.	Cloud computing.
103-d.	Website accessibility; state agencies.
103-e.	Artificial intelligence (AI) inventory.
103-f.	Cybersecurity awareness training.
104.	Advisory council for technology.
105.	Functions, powers and duties of the council.
106.	Responsibility to respond to the freedom of information law for certain data.
106-a.	Health care proxy information.
106-b.	Use of biometric identifying technology in schools.
107.	Severability.

§ 101. Definitions. As used in this article the following terms shall mean:

1. "Council" means the advisory council for technology.

2. "Director" means the director of the office.

3. "Office" means the office of information technology services.

4. "State agency" means any department, board, bureau, commission, division, office, council, committee or officer of the state. Such term shall not include the legislature or judiciary.

5. "Technology" means either a good or a service or a combination thereof, used in the application of any computer or electronic information or interconnected system that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or voice including, but not limited to, hardware, software, information appliances, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically and electronically collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, coverage, interface, switch, or disseminate data of any kind or form, and shall include all associated consulting, management, facilities, maintenance, support and training. Goods may be either new or used.

6. "Cloud computing" shall have the same meaning as defined by the national institute of standards and technology's special publication 800-145, and any subsequent version of such publication.

§ 102. Office of information technology services; director, organization and employees. 1. The office of information technology services is hereby created within the executive department to have and exercise the functions, powers and duties provided by the provisions of this article and any other provision of law.

2. The head of the office shall be the director of the office, who shall serve as the chief technology officer for the state of New York and shall be designated as management confidential in the noncompetitive

class in accordance with the civil service law. The director shall be the chief executive officer of and in sole charge of the administration of the office. The director shall be entitled to receive reimbursement for expenses actually and necessarily incurred by him or her in the performance of his or her duties.

3. The director may, from time to time, create, abolish, transfer and consolidate bureaus and other units within the office not expressly established by law as he or she may determine necessary for the efficient operation of the office, subject to the approval of the director of the budget.

4. The director may appoint, in accordance with the civil service law, such deputies, assistants, and other officers and employees, committees and consultants as he or she may deem necessary, prescribe their powers and duties, fix their compensation, and provide for reimbursement of their expenses within the amounts appropriated therefor.

5. The director may request and receive from any department, division, board, bureau, commission or other agency of the state or any political subdivision thereof or any public authority, staff and other assistance, information, and resources as will enable the office to properly carry out its functions, powers and duties.

§ 103. Functions, powers and duties of the office. The office shall have the following functions, powers and duties:

1. To act as the official state planning and coordinating office for the advancement of technology to improve government efficiency and effectiveness, and perform all necessary and appropriate services required to fulfill these duties;

2. To advise and assist the state agencies in developing policies, plans and programs for improving the statewide coordination, administration, security, confidentiality, program effectiveness, acquisition and deployment of technology;

3. To perform technology reviews and make recommendations for improving management and program effectiveness pertaining to technology;

4. To review and coordinate the purchase of technology by state agencies. Where applicable, such review shall include but not be limited to: assessing consistency with the statewide strategic technology plan and agency technology plan; statewide technology standards; the safeguarding of information privacy; security of confidential records; and proper dissemination of public information;

5. To establish, oversee, manage, coordinate and facilitate the planning, design and implementation of the state's common technology networks;

6. To undertake research, studies and analyses, and act as a central repository, clearinghouse and disseminator of research studies, with respect to technology;

7. To facilitate and coordinate the improvement of program delivery services through technology with and among other departments, divisions and agencies of the state, its political subdivisions and municipalities;

7-a. To provide technology services via agreements with:

(a) municipal corporations, public benefit corporations and district corporations as defined in section sixty-six of the general construction law;

(b) political subdivisions as defined in section one hundred of the general municipal law;

(c) public authorities;

(d) soil and water conservation districts;

(e) any unit of the state university and city university of New York pursuant to and consistent with sections three hundred fifty-five and sixty-two hundred eighteen of the education law;

8. To encourage and foster the exchange of and increase access to

information within and among public and private entities and individuals in order to improve the delivery of state programs and services of the state;

8-a. (a) To advise and assist state agencies in the implementation of language translation technology on state agency websites containing information about the novel coronavirus ("COVID-19") or programs, benefits or services related to COVID-19 within sixty days of the effective date of this subdivision; and on all state agency websites within six months of the effective date of this subdivision.

(b) Such language translation technology shall, at a minimum, allow users to translate the text of state agency websites into at least the twelve most common non-English languages spoken by individuals with limited-English proficiency in the state of New York, based on United States census data.

(c) As used in this subdivision, the term "state agency website" shall mean an internet website operated by or for a state agency. Such term shall include those websites operated on behalf of state agencies by other public or private entities, but shall not include any portions of the internet outside the control of the state agency.

9. To undertake technology projects with a statewide or multi-agency impact and, where appropriate, designate agencies to act as lead agency for the project;

10. To establish statewide technology policies, including but not limited to preferred technology standards and security, including statewide policies, standards, programs, and services relating to the security of state government networks and geographic information systems, including the statewide coordination of geographically referenced critical infrastructure information;

11. To adopt, amend, or rescind rules and regulations necessary or convenient to the performance of the functions, powers and duties of the office pursuant to the state administrative procedure act;

12. To complete a comprehensive study of existing state information

resource technology infrastructure to the extent that the information is available.

Such study shall include, but not be limited to, inventories of:

- (a) state operations' computer hardware and software;
- (b) major physical infrastructures supporting existing operations, including power, air conditioning, space and other environmental needs;
- (c) the telecommunications and other networks supporting existing operations;
- (d) personnel associated with existing operations and management;
- (e) expected retirement schedule of existing computer hardware and software and replacement costs; and
- (f) data processing consulting and contracting services utilized.

Such study shall be completed and submitted to the governor, the temporary president of the senate and the speaker of the assembly on or before October first, two thousand two. The office shall provide interim reports on October first, two thousand and October first, two thousand one.

12-a. To develop:

- (a) a methodology to ascertain how much the state spends on technology goods and services;
- (b) a process to update the computer hardware and software inventory periodically;
- (c) a methodology to determine the expected life-cycle of state operations' computer hardware and software which shall include the total cost of ownership; and
- (d) formal disaster recovery plans for the state data center and statewide network, NY e-net; such plans shall be confidential.

Such developments shall be completed and submitted to the governor, the temporary president of the senate and the speaker of the assembly on or before October first, two thousand three.

12-b. To request and shall receive from any department, division, board, commission or other agency of the state any information and

resources necessary to carry out the responsibilities and provisions set forth in subdivisions twelve and twelve-a of this section.

13. To establish a multi-year statewide strategy plan covering a time period of not less than three years to promote and coordinate interagency technology efforts and initiatives that conform to the state's overarching programmatic policy under which state agencies shall develop their information resource management plans. Such plan shall be submitted to the governor, the temporary president of the senate and the speaker of the assembly upon completion on or before October first, two thousand. Such plan shall be updated as needed, but not less than once every three years;

14. To coordinate state budget submission to address known year two thousand conversion issues;

15. To conduct selective evaluations of technology activities in state agencies; and

16. To perform such acts, directly or by other means, as are necessary or convenient to carry out the office's functions, powers and duties.

17. To enter into contracts with any person, firm, corporation, not-for-profit corporation, political subdivision of the state, or governmental entity.

18. To provide for the protection of the state government's cyber security infrastructure, including, but not limited to, the identification and mitigation of vulnerabilities, deterring and responding to cyber events, and promoting cyber security awareness within the state.

19. To maintain, in electronic or paper formats, maps, geographic images, geographic data and metadata.

20. To issue guidance and training for state agencies in their compliance with the Web Content Accessibility Guidelines required

pursuant to section one hundred three-d of the state technology law.

21. To issue guidance for contractors, subcontractors, vendors, consultants, or other persons in their compliance with the Web Content Accessibility Guidelines required pursuant to section one hundred seventy-f of the executive law.

22. Notwithstanding the provisions of subparagraphs (i) and (ii) of paragraph (a) of subdivision eight of section seventy-three of the public officers law, former officers or employees of the office of cyber security employed by the not-for-profit corporation that operates the multi-state information sharing and analysis center may appear before and render services to any federal, state, local, territorial or tribal government relating to cyber security.

* 23. To issue guidance for state agencies in their compliance with the gender-neutral terminology requirements set forth in section one hundred three-b of this chapter.

* NB There are 2 sb 23's

* 23. Notwithstanding the provisions of section one hundred sixty-three of the state finance law, section one hundred three of the general municipal law, article four-C of the economic development law, or any other provision of law relating to the award of public contracts, any officer, body, or agency of New York state, public corporation, or other public entity subject to such provisions of law shall be authorized to enter individually or collectively into contracts with the not-for-profit corporation that operates the multi-state information sharing and analysis center for the provision of services through September thirtieth, two thousand fifteen related to cyber security including, but not limited to, monitoring, detecting, and responding to cyber incidents, and such contracts may be awarded without compliance with the procedures relating to the procurement of services set forth in such provisions of law. Such contracts shall, however, be subject to the comptroller's existing authority to approve contracts where such approval is required by section one hundred twelve of the state finance law or otherwise. Such officers, bodies, or agencies may pay the fees or other amounts specified in such contracts in consideration of the cyber security services to be rendered pursuant to such contracts.

* NB There are 2 sb 23's

24. To educate state agencies on the benefits of using cloud service providers in relation to data storage and management.

25. To provide technical specifications to state agencies regarding certain qualifications and specifications that cloud service providers should satisfy, in relation to such agencies' consideration of contracting with cloud service providers.

*** § 103-a. State information technology innovation center.** 1. The director may establish a state information technology innovation center or "iCenter" to develop, pilot, and consider technology solutions to assist the state, state agencies, authorities, municipalities and other governmental entities find potential solutions to their technology needs or requirements. The director shall ensure the iCenter complies with all state laws, rules, regulations, and policies. Vendor participation in the iCenter shall not be construed to:

(a) create preferred status for any vendor in any government procurement, or

(b) abrogate the requirement that technology procurements are awarded pursuant to all applicable laws, including such laws requiring a competitive process.

2. The director shall implement guidelines to carry out the provisions of this section which shall not contravene any provision of the state finance law. Such procedures shall include, but not be limited to:

(a) establishing the process for selecting vendors for participation in the iCenter, which shall be a public process;

(b) establishing a process to determine which technology needs or requirements shall be iCenter initiatives; and

(c) establishing safeguards to ensure the iCenter does not function in a manner that results in the circumvention of competitive bidding, including but not limited to through single and sole source exemptions.

3. The director shall conduct an outreach campaign informing the

public of the iCenter and shall conduct specific outreach to minority and women-owned business enterprises certified pursuant to article fifteen-A of the executive law, small businesses as such term is defined in section one hundred thirty-one of the economic development law, and service disabled veteran owned business enterprises certified pursuant to article three of the veterans' services law to inform such businesses of iCenter initiatives.

4. Every January first, beginning in two thousand nineteen, the director shall submit a report to the speaker of the assembly, the temporary president of the senate, and the governor detailing iCenter initiatives undertaken in the prior year. Such report shall include but not be limited to: an identification of any state resources used to support the iCenter in the prior year; the number and nature of iCenter initiatives undertaken in the prior year; the identity of vendors that participated in the iCenter in the prior year, any iCenter initiatives piloted in the prior year that were subsequently awarded a procurement contract with any state agency to the extent the office of information technology services may be aware of such contracts; and an evaluation of the effectiveness of the iCenter. Such report shall be publicly posted on the office's website.

* NB Repealed June 30, 2028

§ 103-b. Gender-neutral terminology; state agencies. Each state agency shall use gender-neutral terminology on their websites for website content, including but not limited to forms accessible through the website, that is created by or on behalf of such agency, or is within their control to modify, provided that such content is created or modified, including without limitation by the addition of content, after the effective date of this section; provided further, however, if such language is in reference to a specific person, or a specific group of people, the language referring to such person or group may be gendered in accordance with the gender identity of such person or group of people.

*** § 103-c. State agency websites; mobile friendly websites.** All state agency websites, as defined in section two hundred two of this chapter, shall offer a mobile friendly form and shall be made available for all mobile devices that support such technology, provided that such requirement shall only apply to websites created or modified with changes to form or function after the effective date of this section and prior to January first, two thousand twenty-seven, and to all state agency websites thereafter. For the purposes of this section, "mobile friendly" shall mean, with respect to a website, that such website is configured in such a way that such website may be navigated, viewed and accessed on a smartphone, tablet computer, or similar mobile device. For the purposes of this section, "changes to form or function" shall mean modifications to the visual presentation, informational organization, website infrastructure, or user utility of the website, including but not limited to:

1. redesigns of site layout, color schemes, graphics, branding elements, or other aesthetic components; or

2. integration of dynamic interfaces.

* NB There are 2 § 103-c's

*** § 103-c. Cloud computing.** 1. Each state agency shall, whenever possible and feasible, consider cloud computing solutions in such agency's technology sourcing strategy for future technology initiatives, data storage and management purposes, and upgrades.

2. All state agencies shall, in consultation with the office, adopt written procedures for the evaluation of cloud computing options for future technology initiatives, data storage and management, upgrades, and procurements.

* NB There are 2 § 103-c's

§ 103-d. Website accessibility; state agencies. Each state agency shall, to the extent practicable, conform any of their websites, created

or modified with changes to form or function after the effective date of this section, by January first, two thousand twenty-seven, to the most current version of the Web Content Accessibility Guidelines, specifically level AA, adopted by the World Wide Web Consortium for accessibility, or any successor standards. A state agency that cannot comply with the requirements of this section shall, by January first, two thousand twenty-seven, post publicly on its website a written progress report that describes with specificity the steps the agency has taken to comply with this section, the impediments that prevented compliance, the efforts undertaken by the agency to come into compliance, and an estimated time frame for compliance. The written report shall be updated annually from the date of the original posting. This section shall not require an agency to take any action that would result in a fundamental alteration in the nature of a service, program, or activity.

For purposes of this section, "changes to form or function" shall mean modifications to the visual presentation, informational organization, website infrastructure, or user utility of the website, including but not limited to: 1. redesigns of site layout, color schemes, graphics, branding elements, or other aesthetic components; and 2. integration of dynamic interfaces. Nothing in this section shall be construed to be inconsistent with any current or future applicable federal laws or regulations.

§ 103-e. Artificial intelligence (AI) inventory. 1. The office shall maintain an inventory of state agency artificial intelligence systems. The office shall issue guidance to state agencies identifying the data elements to be collected and submitted to the office for such inventory, including but not limited to the purpose and uses of the artificial intelligence systems. The inventory shall be posted on the New York state open data website on the thirtieth of December next succeeding the date this section takes effect, and annually thereafter. State agencies shall submit information required by the office at least sixty days in advance of the annual publication date. The office may withhold certain information if it determines disclosure of this information would

jeopardize the security of information technology assets, or as prescribed by article six of the public officers law.

2. For purposes of this section, "artificial intelligence system" shall mean a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments that, when used, may "directly impact the public". Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action. "Artificial intelligence system" includes but is not limited to systems that use machine learning, large language model, natural language processing, and computer vision technologies, including generative artificial intelligence. "Artificial intelligence system" shall not include basic calculations, basic automation, or pre-recorded rule-based conditional logic response systems with predefined triggers that automatically initiate predetermined actions, such as If This Then That (IFTT) systems.

3. For purposes of this section, "directly impact the public" shall mean when the use of an artificial intelligence system would control, have a material impact on, or meaningfully influence the outcome of activities that impact the safety, welfare, or rights of the public. Such activities include but are not limited to assessments or decisions about individuals including in law enforcement, housing, hiring and employment, financial, educational, or healthcare contexts, decisions regarding access to or eligibility for government benefits or about child welfare, or the functioning of emergency services or critical infrastructure.

4. The office may ask and shall receive from any state agency any information or assistance necessary to carry out its powers and duties under this section.

5. The office shall submit a copy of the artificial intelligence inventory to the governor, the temporary president of the senate, and

the speaker of the assembly.

§ 103-f. Cybersecurity awareness training. 1. (a) Employees of the state who use technology as a part of their official job duties shall take annual cybersecurity awareness training beginning January first, two thousand twenty-six. Employees of the state shall be required to complete the training provided by the office.

(b) For purposes of this section, "employees of the state" shall include employees of all state agencies and all public benefit corporations, the heads of which are appointed by the governor.

2. Employees of a county, a city, a town, a village, or a district as defined in section one hundred nineteen-n of the general municipal law, who use technology as a part of their official job duties shall take annual cybersecurity awareness training beginning January first, two thousand twenty-six. The office shall make a cybersecurity training available for use by a county, a city, a town, a village, or a district as defined in section one hundred nineteen-n of the general municipal law, at no charge, provided however, no employee of a county, a city, a town, a village, or a district as defined in section one hundred nineteen-n of the general municipal law shall be required to complete such training provided by the office and the cybersecurity awareness training requirements of this section may be satisfied by the completion of other cybersecurity awareness training.

3. All training mandated by this section shall be conducted during the employee's regular working hours and employees shall receive compensation at their regular rate of pay for any time spent participating in such training.

*** § 103-f. Automated decision-making tool inventory.** 1. The office shall maintain an inventory of state automated decision-making tools. The office shall issue guidance to state agencies identifying the data elements to be collected and submitted to the office for such inventory, including but not limited to the purpose and uses of such automated

decision-making tools. The inventory shall be posted on the New York state open data website on the thirtieth of December next succeeding the date on which this section takes effect, and annually thereafter. State agencies shall submit information required by the office at least sixty days in advance of the annual publication date. The office may withhold certain information if it determines disclosure of this information would jeopardize the security of information technology assets, or as prescribed by article six of the public officers law.

2. For purposes of this section, "automated decision-making tool" shall have the same meaning as the term is defined in section five hundred one of this chapter.

3. The office may ask and shall receive from any state agency any information or assistance necessary to carry out its powers and duties under this section.

4. The office shall submit a copy of the artificial intelligence inventory to the governor, the temporary president of the senate, and the speaker of the assembly.

* NB Repealed July 1, 2028

* NB There are 2 § 103-f's

§ 104. Advisory council for technology. 1. There shall be within the office, an advisory council for technology. The director of the office shall serve as chair of the council. The council shall be composed of a minimum of nine information resource management directors or their equivalent appointed by the governor. The governor's appointments shall be selected from state agencies. In addition, one shall be appointed upon recommendation of the temporary president of the senate and one shall be appointed upon the recommendation of the speaker of the assembly.

2. The members of the council shall receive no compensation for their services, but shall be allowed their actual and necessary expenses incurred in the performance of their duties.

§ 105. Functions, powers and duties of the council. The council shall have the following functions, powers and duties:

1. To review and comment on all rules and regulations of the office;
2. To provide guidance and support to the office in the development of any statewide plan for the further development and improvement of the state's technology acquisitions;
3. To recommend surveys and reports to be completed by the director to carry out all of the objectives and purposes of this article; and
4. To perform such other acts as may be assigned by the chairperson of the council which are necessary or appropriate to carry out the functions of the council.

§ 106. Responsibility to respond to the freedom of information law for certain data. Where the office receives a request for another agency's data which is in the possession of the office because it administers, operates or manages a statewide technology program, the office will transmit, within five days, in writing the request to the agency that owns the data with a copy of this law and send a copy of the transmittal to the requester. Upon receiving the forwarded request, the agency must comply with article six of the public officers law as if it had initially received the request. The time periods for responding to a request as required by article six of the public officers law commence when the agency receives the request from the office.

§ 106-a. Health care proxy information. Any state agency, board, bureau, authority, commission, division, or other governmental entity performing a governmental or proprietary function for the state that maintains a public website and has a significant public interaction in the field of public health shall, in consultation with the office of

information technology services and the department of health, create a link on their homepage to the health care proxy information on the department of health's website. A state agency, board, bureau, authority, commission, division, or other governmental entity performing a governmental or proprietary function for the state which determines that creating such link would create a financial hardship or which do not have a significant public interaction in the field of public health shall be exempted from the provisions of this section.

§ 106-b. Use of biometric identifying technology in schools. 1. As used in this section:

a. "biometric identifying technology" shall mean any tool using an automated or semi-automated process that assists in verifying a person's identity based on a person's biometric information.

b. "biometric information" shall mean any measurable physical, physiological or behavioral characteristics that are attributable to a person, including but not limited to facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other characteristics that can be used to identify a person including, but are not limited to: fingerprints; handprints; retina and iris patterns; DNA sequence; voice; gait; and facial geometry.

c. "facial recognition" shall mean any tool using an automated or semi-automated process that assists in uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's face.

2. a. Except as authorized in paragraph b of this subdivision, public and nonpublic elementary and secondary schools, including charter schools, shall be prohibited from purchasing or utilizing biometric identifying technology for any purpose, including school security, until July first, two thousand twenty-two or until the commissioner of education authorizes such purchase or utilization as provided in subdivision three of this section, whichever occurs later.

b. Schools may utilize biometric identifying technology for the following purposes: (i) fingerprint identification of prospective school employees where utilized for the purpose of compliance with a provision of the education law or the regulations of the commissioner of education or (ii) to exclusively identify employees that have consented in writing to the use of such technology or in the case of employees represented under article fourteen of the civil service law, where the employee organization representing such employee has consented in writing to the use of such technology.

3. a. The commissioner of education shall not authorize the purchase or utilization of biometric identifying technology, including but not limited to facial recognition technology, without the director first issuing a report prepared in consultation with the state education department, making recommendations as to the circumstances in which the utilization of such technology is appropriate in public and nonpublic elementary and secondary schools, including charter schools, and what restrictions and guidelines should be enacted to protect individual privacy, civil rights, and civil liberty interests. Such report shall be made public and presented to the governor, the temporary president of the senate, and the speaker of the assembly, and shall consider, evaluate and present recommendations concerning:

i. the privacy implications of collecting, storing, and/or sharing biometric information of students, teachers, school personnel and the general public entering a school or school grounds;

ii. the potential impact of the use of biometric identifying technology on student civil liberties and student civil rights, including the risks and implications of the technology resulting in false facial identifications, and whether the risks of false facial identifications differs for different subgroups of individuals based on race, national origin, gender, age and other factors, and any other reasonable accuracy concerns with respect to technology;

iii. whether, and under what circumstances, such technology may be

used for school security and the effectiveness of such technology to protect students and school personnel;

iv. whether, and under what circumstances and in what manner, information collected may be used by schools and shared with students, parents or guardians, outside agencies including law enforcement agencies, individuals, litigants, the courts, and any other third parties;

v. the length of time biometric information may be retained and whether, and in what manner, such information may be required to be permanently destroyed;

vi. the risk of an unauthorized breach of biometric information and appropriate consequences therefor;

vii. expected maintenance costs resulting from the storage and use of facial recognition images and other biometric information, including the cost of appropriately securing sensitive data, performing required updates to protect against an unauthorized breach of data, and potential costs associated with an unauthorized breach of data;

viii. analysis of other schools and organizations, if any, that have implemented facial recognition technology and other biometric identifying technology programs;

ix. the appropriateness and potential implications of using any existing databases, including but not limited to, local law enforcement databases, as part of biometric identifying technology;

x. whether, and in what manner such biometric identifying technology should be assessed and audited, including but not limited to, vendor datasets, adherence to appropriate standards of algorithmic fairness, accuracy, and other performance metrics, including with respect to subgroups of persons based on race, national origin, gender, and age;

xi. whether, and in what manner, the use of such technology should be

disclosed by signs and the like in such schools, as well as communicated to parents, guardians, students, and district residents; and

xii. existing legislation, including but not limited to section two-d of the education law, that may be implicated by or in conflict with biometric technology to ensure the maintenance of records related to the use of such technology, protect the privacy interests of data subjects, and avoid any breaches of data.

b. The director, in consultation with the commissioner of education, shall consult with stakeholders and other interested parties when preparing such report. The state education department, the division of criminal justice services, law enforcement authorities and the state university of New York and the city university of New York shall, to the extent practicable, identify and provide representatives to the office of information technology, at the request of the director, in order to participate in the development and drafting of such report.

4. The director shall, via scheduled public hearings and other outreach methods, seek feedback from teachers, school administrators, parents, individuals with expertise in school safety and security, and individuals with expertise in data privacy issues and student privacy issues, and individuals with expertise in civil rights and civil liberties prior to making such recommendations.

§ 107. Severability. The provisions of this article shall be severable and if any portion thereof or the applicability thereof to any person or circumstances shall be held to be invalid, the remainder of this article and the application thereof shall not be affected thereby.

ARTICLE II

INTERNET SECURITY AND PRIVACY ACT

Section 201. Short title.

202. Definitions.

203. Model internet privacy policy.

- 204. Collection and disclosure of personal information.
- 205. Access to personal information.
- 206. Exceptions.
- 207. Construction.
- 208. Notification; person without valid authorization has acquired private information.
- 209. Notification of a breach of the security of the system or a breach of network security; shared data.
- 210. Cybersecurity protection.

§ 201. Short title. This article shall be known and may be cited as the "internet security and privacy act".

§ 202. Definitions. As used in this article, the following terms shall have the following meanings:

1. "Collect" shall mean to store information, including via cookie technology, for purposes of retrieval at a later time to initiate communication with or make determinations about the person who is the subject of such information.
2. "Disclose" shall mean to reveal, release, transfer, disseminate or otherwise communicate information orally, in writing or by electronic or other means, other than to the person who is the subject of such information.
3. "Internet" shall mean a system of linked computer networks, international in scope, that facilitate data transmission and exchange.
4. "Office" shall mean the state office of information technology services.
5. "Personal information" shall mean any information concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person.

6. "State agency" shall have the same meaning as the meaning given to "agency" under subdivision one of section ninety-two of the public officers law.

7. "State agency website" shall mean an internet website operated by or for a state agency. Such term shall include those websites operated on behalf of state agencies by other public or private entities, but shall not include any portions of the internet outside the control of the state agency.

8. "User" shall mean any natural person who uses the internet to access a state agency website.

§ 203. Model internet privacy policy. 1. The office shall adopt rules and regulations in conformity with the provisions of this article, and specify a model internet privacy policy for state agencies that maintain state agency websites. Such model privacy policy shall include, but not be limited to, the following elements:

(a) a statement of any information, including personal information, the state agency website will collect with respect to the user and the use of the information;

(b) the circumstances under which information, including personal information, collected may be disclosed;

(c) whether any information collected will be retained by the state agency, and, if so, the period of time that such information will be retained;

(d) the procedures by which a user may gain access to the collected information pertaining to that user;

(e) the means by which information is collected and whether such collection occurs actively or passively;

(f) whether the collection of information is voluntary or required, and the consequences, if any, of a refusal to provide the required information; and

(g) the steps being taken by the state agency to protect the confidentiality and integrity of the information.

2. Each state agency that maintains a state agency website shall adopt an internet privacy policy which shall, at a minimum, include the information required by the model internet privacy policy. Each state agency shall post its internet privacy policy on its website. Such posting shall include a conspicuous and direct link to such privacy policy.

3. The model internet privacy policy specified by the office shall also be made available at no charge to other public and private entities.

§ 204. Collection and disclosure of personal information. No state agency shall collect personal information concerning a user through a state agency website, or disclose personal information concerning a user to any person, firm, partnership, corporation, limited liability company or other entity, including internal staff who do not need the information in the performance of their official duties pursuant to a state agency purpose meeting the requirements of subdivision one of section two hundred six of this article, unless such user has consented to the collection or disclosure of such personal information. For the purposes of this section, the voluntary disclosure of personal information to a state agency by a user through a state agency website, whether solicited or unsolicited, shall constitute consent to the collection or disclosure of the information by the state agency for the purposes for which the user disclosed it to the state agency, as reasonably ascertainable from the nature and terms of the disclosure.

§ 205. Access to personal information. Except as otherwise provided by law, a state agency shall provide users with access to all personal information pertaining to such user which has been collected through its state agency website. Access to such personal information and the opportunity to request correction or amendment of such personal information shall be provided to users in the manner provided for access to and correction or amendment of personal information under section

ninety-five of the public officers law. A state agency shall provide a user access to such personal information via the internet when such access is feasible and only if that access can be provided in a secure manner.

§ 206. Exceptions. Notwithstanding section two hundred four of this article, a state agency may collect or disclose personal information if the collection or disclosure is:

1. necessary to perform the statutory duties of the state agency that collected or is collecting the personal information, or necessary for that agency to operate a program authorized by law, or authorized by state or federal statute or regulation;
2. made pursuant to a court order or by law;
3. for the purpose of validating the identity of the user; or
4. if the information is used solely for statistical purposes and is in a form that cannot be used to identify any particular person.

§ 207. Construction. Nothing in this article shall abridge public access to information available or permitted by any other provision or rule of law, including without limitation article six of the public officers law. Nothing in this article shall authorize the collection or disclosure of information the collection or disclosure of which is prohibited or restricted by any other provision of law, including without limitation article six-A of the public officers law. Nothing in this article shall alter the obligations of state agencies and users pursuant to article six-A of the public officers law.

§ 208. Notification; person without valid authorization has acquired private information. 1. As used in this section, the following terms shall have the following meanings:

(a) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number;

(3) account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(b) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person

without valid authorization, such state entity may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(c) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

(1) the judiciary; and

(2) all cities, counties, municipalities, villages, towns, and other local agencies.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the integrity of the

data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the state entity shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to paragraph (a) of subdivision seven of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision seven of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules,

regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or

(d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;

- (2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and
- (3) notification to major statewide media.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.

9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (a) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance

Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

10. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

§ 209. Notification of a breach of the security of the system or a breach of network security; shared data. 1. The office shall, within twenty-four hours of either being notified of or receiving evidence of a breach of the security of the system, or a breach of network security, as defined in paragraphs (a) and (b) of subdivision three of this section, notify the chief information officer, the chief information security officer, and where appropriate, the cyber security coordinator of any state entity with which it shares data, provides networked services or shares a network connection whose data, services or connection is reasonably suspected to be affected by any such breach.

2. The office shall provide the chief information officer, the chief information security officer, and where appropriate, the cyber risk coordinator of any state entity, who has been notified pursuant to subdivision one of this section, with its plan for remediation of the breach and future protection of such data and network.

3. For purposes of this section:

(a) "Breach of the security of the system" shall have the same meaning as defined in paragraph (b) of subdivision one of section two hundred eight of this article.

(b) "Breach of network security" shall mean unauthorized access to or access without valid authorization of a computer network which compromises the security, confidentiality, or integrity of such network.

(c) "State entity" shall have the same meaning as provided by paragraph (c) of subdivision one of section two hundred eight of this article.

§ 210. Cybersecurity protection. 1. Definitions. For purposes of this section, the following terms shall have the following meanings:

(a) "Breach of the security of the system" shall have the same meaning as such term is defined in section two hundred eight of this article.

(b) "Data subject" means any natural person about whom personal information has been collected by a state agency.

(c) "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(d) "State agency-maintained personal information" means personal information stored by a state agency that was generated by a state agency or provided to the state agency by the data subject, a state agency, a federal governmental entity, or any other third-party source. Such term shall also include personal information provided by an adverse party in the course of litigation or other adversarial proceeding.

(e) "State agency" shall have the same meaning as such term is defined in section one hundred one of this chapter.

2. Data protection standards. The director shall issue policies and standards for:

(a) protection against breaches of the security of the information systems and for personal information used by such information systems;

(b) data backup;

(c) information system recovery;

(d) secure sanitization and deletion of data;

(e) vulnerability management and assessment; and

(f) annual workforce training regarding protection against breaches of the security of the system, as well as processes and procedures that should be followed in the event of a breach of the security of the system.

3. Information system inventory. (a) No later than two years after the

effective date of this section, each state agency shall create, then maintain, an inventory of its information systems.

(b) Upon written request from the office, a state agency shall provide the office with the state agency-maintained information systems inventories required to be created or updated pursuant to this subdivision.

(c) Notwithstanding paragraph (a) of this subdivision, the state agency-maintained information systems inventories required to be created or updated pursuant to this subdivision shall be kept confidential, as disclosure of such information would jeopardize the security of a state agency's information systems and information technology assets and, further, shall not be made available for disclosure or inspection under the state freedom of information law.

4. Incident management and recovery. (a) No later than eighteen months after the effective date of this section, each state agency shall have created an incident response plan for incidents involving a breach of the security of the system that render an information system or its data unavailable, and incidents involving a breach of the security of the system that result in the alteration or deletion of or unauthorized access to, personal information.

(b) Such incident response plan shall include, but not be limited to, a procedure for situations where information systems have been adversely affected by a breach of the security of the system, as well as a procedure for the recovery of personal information and information systems.

(c) Beginning January first, two thousand twenty-eight and on an annual basis thereafter, each state agency shall complete at least one exercise of its incident response plan. Upon completion of such exercise, the state agency shall document the incident response plan's successes and shortcomings in an incident response plan exercise report. The incident response plan and any incident response plan exercise reports shall be kept confidential, as disclosure of such information would jeopardize the security of a state agency's information systems and information technology assets, and, further, shall not be made available for disclosure or inspection under the state freedom of information law.

5. No private right of action. Nothing set forth in this section shall be construed as creating or establishing a private cause of action.

ARTICLE III

ELECTRONIC SIGNATURES AND RECORDS ACT

Section 301. Short title.

302. Definitions.

303. Electronic facilitator.

304. Use of electronic signatures.

305. Use of electronic records.

306. Admissibility into evidence.

307. Exceptions.

308. Personal privacy protection.

309. Use of electronic records and signatures to be voluntary.

§ 301. Short title. This article shall be known and may be cited as the "electronic signatures and records act".

§ 302. Definitions. For the purpose of this article:

1. "Electronic" shall mean of or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

2. "Electronic record" shall mean information, evidencing any act, transaction, occurrence, event, or other activity, produced or stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities.

3. "Electronic signature" shall mean an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record.

4. "Person" shall mean a natural person, corporation, trust, estate, partnership, incorporated or unincorporated association or any other legal entity, and also includes any department, agency, authority, or instrumentality of the state or its political subdivisions.

5. "Governmental entity" shall mean any state department, board, bureau, division, commission, committee, public authority, public benefit corporation, council, office, or other governmental entity or officer of the state having statewide authority, except the state legislature, and any political subdivision of the state.

§ 303. Electronic facilitator. 1. The office of information technology services shall be the electronic facilitator and administer this article. In addition to the authority, duties and responsibilities set forth in article one of this chapter, the electronic facilitator shall have the authority, duties and responsibilities granted in this article.

2. The electronic facilitator shall have the following functions, powers, and duties:

(a) To promulgate rules and regulations consistent with the provisions of this article. In developing rules and regulations, the electronic facilitator shall seek the advice of the attorney general, the state comptroller, the director of budget, government and private entities and individuals as the electronic facilitator deems appropriate.

(b) To cooperate with government and private entities and individuals in order to assist in the development and implementation of this article.

(c) To develop guidelines for the improvement of business and commerce by electronic means. Such guidelines shall identify preferred technology standards relating to security, confidentiality and privacy of electronic signatures and electronic records.

§ 304. Use of electronic signatures. 1. The electronic facilitator shall establish rules and regulations governing the use of electronic signatures and authentication. The electronic facilitator shall not

establish rules or regulations that seek to apportion fault or impose or limit liability relating to the use of electronic signatures.

2. In accordance with this section unless specifically provided otherwise by law, an electronic signature may be used by a person in lieu of a signature affixed by hand. The use of an electronic signature shall have the same validity and effect as the use of a signature affixed by hand.

§ 305. Use of electronic records. 1. In accordance with rules and regulations promulgated by the electronic facilitator, government entities are authorized and empowered to produce, receive, accept, acquire, record, file, transmit, forward, and store information by use of electronic means. If any such government entity uses electronic records, it must also ensure that anyone who uses the services of such government entity may obtain access to records as permitted by statute, and receive copies of such records in paper form in accordance with fees prescribed by statute. No person shall be required to submit or file any record electronically to any government entity except as otherwise provided by law. Government entities that obtain, store, or utilize electronic records shall not refuse to accept hard copy, non-electronic forms, reports, and other paper documents for submission or filing except as otherwise provided by law.

2. A government entity shall have the authority to dispose of or destroy a record in accordance with the arts and cultural affairs law, regardless of format or media.

3. An electronic record shall have the same force and effect as those records not produced by electronic means.

4. The director shall study how electronic documents and the mechanisms and processes for obtaining access to and reading electronic data can be created, maintained, exchanged, and preserved by the state in a manner that encourages appropriate government control, access, choice, interoperability, and vendor neutrality. The study shall

consider, but not be limited to, the policies of other states and nations, management guidelines for state archives as they pertain to electronic documents, public access, expected storage life of electronic documents, costs of implementation, and savings. The director shall solicit comments regarding the creation, maintenance, exchange, and preservation of electronic documents by the state from stakeholders, including but not limited to, the office of the state comptroller, the office of the attorney general, the state archives, and the state historian. The director shall also solicit comments from members of the public. The director shall report findings and recommendations to the governor, the speaker of the assembly, and the temporary president of the senate on or before January fifteenth, two thousand eight.

§ 306. Admissibility into evidence. In any legal proceeding where the provisions of the civil practice law and rules are applicable, an electronic record or electronic signature may be admitted into evidence pursuant to the provisions of article forty-five of the civil practice law and rules including, but not limited to section four thousand five hundred thirty-nine of such law and rules.

§ 307. Exceptions. This article shall not apply:

* 1. To any document providing for the disposition of an individual's person or property upon death or incompetence, or appointing a fiduciary of an individual's person or property, including, without limitation, wills, trusts, decisions consenting to orders not to resuscitate, and powers of attorney, with the exception of: (a) contractual beneficiary designations; (b) the registration of making, amending, or revoking an anatomical gift under section forty-three hundred ten of the public health law; (c) documents and forms authorizing or accepting funeral, cemetery and cremation services; and (d) the execution of a valid power of attorney for the purpose of transferring a salvage certificate of title and the execution of an odometer and damage disclosure statement in connection with such title whenever a loss in connection with a private automobile is determined by an insurer to be a total loss or constructive total loss under section three thousand four hundred twelve

of the insurance law.

* NB Effective until December 12, 2027

* 1. To any document providing for the disposition of an individual's person or property upon death or incompetence, or appointing a fiduciary of an individual's person or property, including, without limitation, wills, unless such will is executed pursuant to part six of article three of the estates, powers and trusts law, trusts, decisions consenting to orders not to resuscitate, and powers of attorney, with the exception of: (a) contractual beneficiary designations; (b) the registration of making, amending, or revoking an anatomical gift under section forty-three hundred ten of the public health law; (c) documents and forms authorizing or accepting funeral, cemetery and cremation services; and (d) the execution of a valid power of attorney for the purpose of transferring a salvage certificate of title and the execution of an odometer and damage disclosure statement in connection with such title whenever a loss in connection with a private automobile is determined by an insurer to be a total loss or constructive total loss under section three thousand four hundred twelve of the insurance law.

* NB Effective December 12, 2027

2. To any negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title, unless an electronic version of such record is created, stored or transferred pursuant to this article in a manner that allows for the existence of only one unique, identifiable and unalterable version which cannot be copied except in a form that is readily identifiable as a copy.

3. To any other document that the electronic facilitator has specifically excepted, pursuant to the rules and regulations of the electronic facilitator, from the application of this article.

§ 308. Personal privacy protection. 1. Any information reported to the electronic facilitator by a government entity in connection with the authorization of an electronic signature shall continue to be withheld from public disclosure if such information was withheld from public disclosure by such government entity. Electronic records shall be

considered and treated as any other records for the purposes of the freedom of information law as set forth in article six of the public officers law and the personal privacy protection law as set forth in article six-A of the public officers law.

2. A person or an entity that acts as an authenticator of electronic signatures shall not disclose to a third party any personal information reported to it by the electronic signatory other than the information necessary to authenticate the signature unless the disclosure is made pursuant to a court order or statute, or if the information or data is used solely for statistical purposes in aggregate form. For purposes of this section, "personal information" shall mean data that identifies a specific person, including but not limited to home and work addresses, telephone number, e-mail address, social security number, birthdate, gender, marital status, mother's maiden name, and health data.

§ 309. Use of electronic records and signatures to be voluntary.

Nothing in this article shall require any entity or person to use an electronic record or an electronic signature unless otherwise provided by law.

ARTICLE IV

AUTOMATED EMPLOYMENT DECISION-MAKING IN STATE GOVERNMENT

Section 401. Definitions.

402. Disclosure of automated employment decision-making tools used by state agencies.

402-a. Disclosure of automated employment decision-making tools used by covered entities.

§ 401. Definitions. For the purpose of this article:

1. "Automated employment decision-making tool" shall mean any software that uses algorithms, computational models, or artificial intelligence techniques, or a combination thereof, to materially automate or replace

human decision-making regarding employment, including but not limited to wages and other compensation, hiring, selection for recruitment, discipline, promotion, and termination. "Automated employment decision-making tool" shall not include any software used primarily for basic computerized processes, such as calculators, spellcheck tools, autocorrect functions, spreadsheets, electronic communications, or any tool that relates only to internal management affairs such as ordering office supplies or processing payments, and that do not materially affect the rights, liberties, benefits, safety or welfare of any individual within the state.

2. "State agency" shall mean any department, public authority, board, bureau, commission, division, office, council, committee or officer of the state. Such terms shall not include the legislature or judiciary.

* 3. "Covered entity" shall mean any county, city, town, village, school district, board of cooperative educational services, county vocational education and extension board, district corporation, the state university of New York, the city university of New York, or community college.

* NB Repealed July 1, 2028

§ 402. * Disclosure of automated employment decision-making tools used by state agencies.

* NB Effective until July 1, 2028

* Disclosure of automated employment decision-making tools.

* NB Effective July 1, 2028

Any state agency that utilizes an automated employment decision-making tool, as defined in section four hundred one of this article, shall publish a list of such automated employment decision-making tools on such state agency's website no later than the thirtieth of December next succeeding the date on which the amendments made to this section by a chapter of the laws of two thousand twenty-four take effect, and annually thereafter. Such disclosure shall include:

1. a description of the automated employment decision-making tool utilized by such state agency;

2. the date that the state agency use of such automated employment decision-making tool began;

3. a summary of the purpose and use of such automated employment decision-making tool; and

4. any other information deemed relevant by the agency.

*** § 402-a. Disclosure of automated employment decision-making tools used by covered entities.** To the extent feasible, any covered entity that utilizes an automated employment decision-making tool, shall publish a list of such automated employment decision-making tools on such covered entity's website no later than the thirtieth of December next succeeding the date on which this section shall have become a law, and annually thereafter. To the extent feasible, such disclosure shall include:

1. a description of the automated employment decision-making tool utilized by such covered entity;

2. the date that the covered entity use of such automated employment decision-making tool began;

3. a summary of the purpose and use of such automated employment decision-making tool; and

4. any other information deemed relevant by the covered entity.

* NB Repealed July 1, 2028

*** ARTICLE V**

AUTOMATED DECISION-MAKING IN GOVERNMENT AGENCIES

Section 501. Definitions.

502. Disclosure of automated decision-making tools by government agencies.

503. Impact assessments.

504. Submission to the governor and legislature.

* NB Repealed July 1, 2028

* **§ 501. Definitions.** For the purpose of this article:

1. "Automated decision-making tool" shall mean any software that uses algorithms, computational models, or artificial intelligence techniques, or a combination thereof, to automate, support, or replace human decision-making. "Automated decision-making tool" shall not include any software used primarily for basic computerized processes, such as calculators, spellcheck tools, autocorrect functions, spreadsheets, electronic communications, or any tool that relates only to internal management affairs such as ordering office supplies or processing payments, and that do not materially affect the rights, liberties, benefits, safety or welfare of any individual within the state.

"Automated decision-making tools" shall not include "automated employment decision-making tools" as defined in section four hundred one of this chapter.

2. "Meaningful human review" means review, oversight and control of the automated decision-making process by one or more individuals who understand the risks, limitations, and functionality of, and are trained to use, the automated decision-making tool and who have the authority to intervene or alter the decision under review, including but not limited to the ability to approve, deny, or modify any decision recommended or made by the automated tool.

3. "Government agency" shall mean: (a) the state or civil division thereof; (b) a county, city, town or village; (c) a school district, board of cooperative educational services, vocational education and extension board or a school district as enumerated in section one of chapter five hundred sixty-six of the laws of nineteen hundred sixty-seven, as amended; (d) the state university of New York; (e) the city university of New York; (f) a public improvement or special district including police or fire districts; (g) a public authority,

commission or public benefit corporation; or (h) any other public corporation, agency, instrumentality or unit of government which exercises governmental power under the laws of this state.

* NB Repealed July 1, 2028

*** § 502. Disclosure of automated decision-making tools by government agencies.** Any government agency that utilizes an automated decision-making tool, as defined in section five hundred one of this article, shall publish a list of such automated decision-making tools on such government agency's website no later than the thirtieth of December next succeeding the date on which this section takes effect, and annually thereafter. Such disclosure shall include:

1. a description of the automated decision-making tool utilized by such government agency;

2. the date that the government agency use of such automated decision-making tool began;

3. a summary of the purpose and use of such automated decision-making tool; and

4. any other information deemed relevant by the agency.

* NB Repealed July 1, 2028

*** § 503. Impact assessments.** 1. Government agencies seeking to utilize or apply an automated decision-making tool permitted under section five hundred two of this article with continued and operational meaningful human review shall conduct or have conducted an impact assessment substantially completed and bearing the signature of one or more individuals responsible for meaningful human review for the lawful application and use of such automated decision-making tool. Following the first impact assessment, an impact assessment shall be conducted in accordance with this section at least once every two years. An impact assessment shall be conducted prior to any material change to the

automated decision-making tool that may change the outcome or effect of such tool. Such impact assessments shall include:

- (a) a description of the objectives of the automated decision-making tool;

- (b) an evaluation of the ability of the automated decision-making tool to achieve its stated objectives;

- (c) a description and evaluation of the objectives and development of the automated decision-making including:

- (i) a summary of the underlying algorithms, computational modes, and artificial intelligence tools that are used within the automated decision-making tool; and

- (ii) the design and training data used to develop the automated decision-making tool process;

- (d) testing for:

- (i) accuracy, fairness, bias and discrimination, and an assessment of whether the use of the automated decision-making tool produces discriminatory results on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability and outlines mitigations for any identified performance differences in outcomes across relevant groups impacted by such use;

- (ii) any cybersecurity vulnerabilities and privacy risks resulting from the deployment and use of the automated decision-making tool, and the development or existence of safeguards to mitigate the risks;

- (iii) any public health or safety risks resulting from the deployment and use of the automated decision-making tool;

- (iv) any reasonably foreseeable misuse of the automated decision-making tool and the development or existence of safeguards against such misuse;

- (e) the extent to which the deployment and use of the automated decision-making tool requires input of sensitive and personal data, how that data is used and stored, and any control users may have over their data; and

- (f) the notification mechanism or procedure, if any, by which individuals impacted by the utilization of the automated decision-making tool may be notified of the use of such automated decision-making tool

and of the individual's personal data, and informed of their rights and options relating to such use.

2. Notwithstanding the provisions of this article or any other law, if an impact assessment finds that the automated decision-making tool produces discriminatory or biased outcomes, the government agency shall cease any utilization, application, or function of such automated decision-making tool, and of any information produced using such tool.

* NB Repealed July 1, 2028

*** § 504. Submission to the governor and legislature.** 1. Each impact assessment conducted pursuant to this article shall be submitted to the governor, the temporary president of the senate, and the speaker of the assembly at least thirty days prior to the implementation of the automated decision-making tool that is the subject of such assessment.

2. (a) The impact assessment of an automated decision-making tool shall be published on the website of the relevant government agency.

(b) If the government agency makes a determination that the disclosure of any information required in the impact assessment would result in a substantial negative impact on health or safety of the public, infringe upon the privacy rights of individuals, or significantly impair the government agency's ability to protect its information technology or operational assets, such government agency may redact such information, provided that an explanatory statement on the process by which the government agency made such determination is published along with the redacted impact assessment.

(c) If the impact assessment covers any automated decision-making tool that includes technology that is used to prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or other illegal activity, preserve the integrity or security of tools, or to investigate, report or prosecute those responsible for any such malicious or deceptive action, such government agency may redact such information for the purposes of this subdivision, provided that an explanatory statement on the process by which the government agency made such determination is

published along with the redacted impact assessment.

* NB Repealed July 1, 2028