NATIONAL CONFERENCE OF STATE LEGISLATURES

7700 EAST FIRST PLACE DENVER, COLORADO 80230
303-364-7700 FAX: 303-364-7800

Examples of State Statutes Requiring Cybersecurity Awareness Training for State Government Employees

April 6, 2022

Below are excerpts from statutes in four states—Colorado, Florida, Louisiana, Texas and Virginia—that require cybersecurity training for state employees.

STATE AND CITATION/LINK	STATUTORY EXCERPT
Colorado CRS § 24-37.5-403	(2) The chief information security officer shall: …. (g) Conduct information security awareness and training programs;
Florida Fla. Stat. § 282.318	The department, acting through the Florida Digital Service, shall also: …. (e) In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security incident response team members that contains training on cybersecurity, including cybersecurity threats, trends, and best practices. (f) Annually review the strategic and operational cybersecurity plans of state agencies. (g) Provide cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the state university system …. (i) Provide cybersecurity awareness training to all state agency employees in the first 30 days after commencing employment concerning cybersecurity risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the state university system.
Louisiana La. Rev. Stat. § 42:1267	Required training; cybersecurity A.(1) The Department of State Civil Service shall institute, develop, conduct, and otherwise provide for training programs designed to keep state agencies safe from cyberattack. The programs shall be designed to focus on forming information security habits and procedures that protect information resources and teach best practices for detecting, assessing, reporting, and addressing information security threats. The department may make the training available as an online course. The office of technology services shall provide assistance to the Department of State Civil Service in the development of the training program. The cost of instituting, developing, conducting, and otherwise providing cybersecurity awareness training shall be paid in the manner established by R.S. 42:1383.

	(2) The Department of State Civil Service shall make the education and training on cybersecurity developed pursuant to Paragraph (1) of this Subsection available to agencies within political subdivisions of the state at as minimal cost as possible to assist those agencies in compliance with the provisions of this Section. B.(1) Each state and local agency shall identify employees or elected officials who have access to the agency's information technology assets and require those employees and elected officials to complete cybersecurity training. Each new state and local agency official or employee with access to the agency's information technology assets shall complete this training within the first thirty days of initial service or employment with the agency. (2) The agency head shall verify and report to the Department of State Civil Service on the completion of cybersecurity training by agency employees. The agency head shall periodically require an internal review to ensure compliance. (3)(a) An agency shall require any contractor who has access to state or local government information technology assets to complete cybersecurity training during the term of the contract and during any renewal period. (b) Completion of cybersecurity shall be included in the terms of a contract awarded by a state or local government agency to a contractor who has access to its information technology assets. (c) The person who oversees contract management for the agency shall report each such contractor's completion to the agency head and periodically review agency contracts to ensure compliance. (d) The agency head shall verify and report to the Department of State Civil Service on the completion of cybersecurity training by each such contractor.
Texas Tex. Govt. Code § 2054.519, § 5191, § 5192	Sec. 2054.519. STATE CERTIFIED CYBERSECURITY TRAINING PROGRAMS. (a) The department, in consultation with the cybersecurity council established under Section 2054.512 and industry stakeholders, shall annually: (1) certify at least five cybersecurity training programs for state and local government employees; and (2) update standards for maintenance of certification by the cybersecurity training programs under this section. (b) To be certified under Subsection (a), a cybersecurity training program must: (1) focus on forming information security habits and procedures that protect information resources; and (2) teach best practices for detecting, assessing, reporting, and addressing information security threats. (c) The department may identify and certify under Subsection (a) training programs provided by state agencies and local governments that satisfy the training requirements described by Subsection (b). (d) The department may contract with an independent third party to certify cybersecurity training programs under this section. (e) The department shall annually publish on the department's Internet website the list of cybersecurity training programs certified under this section. (f) Repealed by Acts 2021, 87th Leg., R.S., Ch. 51 (H.B. 1118), Sec. 5, eff. May 18, 2021.

	Added by Acts 2019, 86th Leg., R.S., Ch. 1308 (H.B. 3834), Sec. 3, eff. June 14, 2019. Amended by: Acts 2021, 87th Leg., R.S., Ch. 51 (H.B. 1118), Sec. 5, eff. May 18, 2021. Sec. 2054.5191. CYBERSECURITY TRAINING REQUIRED: CERTAIN EMPLOYEES AND OFFICIALS. (a) Each state agency shall identify state employees who use a computer to complete at least 25 percent of the employee's required duties. At least once each year, an employee identified by the state agency and each elected or appointed officer of the agency shall complete a cybersecurity training program certified under Section 2054.519. (a-1) At least once each year, a local government shall: (1) identify local government employees and elected and appointed officials who have access to a local government computer system or database and use a computer to perform at least 25 percent of the employee's or official's required duties; and (2) require the employees and officials identified under Subdivision (1) to complete a cybersecurity training program certified under Section 2054.519. (a-2) The governing body of a local government or the governing body's designee may deny access to the local government's computer system or database to an individual described by Subsection (a-1)(1) who the governing body or the governing body's designee determines is noncompliant with the requirements of Subsection (a-1)(2). (b) The governing body of a local government may select the most appropriate cybersecurity training program certified under Section 2054.519 for employees and officials of the local government to complete. The governing body shall: (1) verify and report on the completion of a cybersecurity training program by employees and officials of the local government to the department; and (2) require periodic audits to ensure compliance with this section. (c) A state agency may select the most appropriate cybersecurity training program certified under Section 2054.519 for employees of the state agency. The executive head of each state agency shall verify completion of a cybersecurity training program by employees of the state agency in a manner specified by the department. (d) The executive head of each state agency shall periodically require an internal review of the agency to ensure compliance with this section. (e) The department shall develop a form for use by state agencies and local governments in verifying completion of cybersecurity training program requirements under this section. The form must allow the state agency and local government to indicate the percentage of employee completion. (f) The requirements of Subsections (a) and (a-1) do not apply to employees and officials who have been: (1) granted military leave; (2) granted leave under the federal Family and Medical Leave Act of 1993 (29 U.S.C. Section 2601 et seq.);

	(3) granted leave related to a sickness or disability covered by workers' compensation benefits, if that employee no longer has access to the state agency's or local government's database and systems; (4) granted any other type of extended leave or authorization to work from an alternative work site if that employee no longer has access to the state agency's or local government's database and systems; or (5) denied access to a local government's computer system or database by the governing body of the local government or the governing body's designee under Subsection (a-2) for noncompliance with the requirements of Subsection (a-1)(2). Added by Acts 2019, 86th Leg., R.S., Ch. 1308 (H.B. 3834), Sec. 3, eff. June 14, 2019. Amended by: Acts 2021, 87th Leg., R.S., Ch. 51 (H.B. 1118), Sec. 2, eff. May 18, 2021. Acts 2021, 87th Leg., R.S., Ch. 51 (H.B. 1118), Sec. 3, eff. May 18, 2021. Sec. 2054.5192. CYBERSECURITY TRAINING REQUIRED: CERTAIN STATE CONTRACTORS. (a) In this section, "contractor" includes a subcontractor, officer, or employee of the contractor. (b) A state agency shall require any contractor who has access to a state computer system or database to complete a cybersecurity training program certified under Section 2054.519 as selected by the agency. (c) The cybersecurity training program must be completed by a contractor during the term of the contract and during any renewal period. (d) Required completion of a cybersecurity training program must be included in the terms of a contract awarded by a state agency to a contractor. (e) A contractor required to complete a cybersecurity training program under this section shall verify completion of the program to the contracting state agency. The person who oversees contract management for the agency shall: (1) not later than August 31 of each year, report the contractor's completion to the department; and (2) periodically review agency contracts to ensure compliance with this section.
Virginia Va .Code § 2.2-2009	Additional duties of the CIO relating to security of government information. I. 1. This subsection applies to the Commonwealth's executive, legislative, and judicial branches and independent agencies. 2. In collaboration with the heads of executive branch and independent agencies and representatives of the Chief Justice of the Supreme Court and the Joint Rules Committee of the General Assembly, the CIO shall develop and annually update a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats. The curriculum shall include activities, case studies, hypothetical situations, and other methods of instruction (i) that focus on forming good information security habits and procedures among state employees and (ii) that teach best practices for detecting, assessing, reporting, and addressing information security threats.

	3. Every state agency shall provide annual information security training for each of its employees using the curriculum and materials developed by the CIO pursuant to subdivision 2. Employees shall complete such training within 30 days of initial employment and by January 31 each year thereafter. State agencies may develop additional training materials that address specific needs of such agency, provided that such materials do not contradict the training curriculum and materials developed by the CIO. The CIO shall coordinate with and assist state agencies in implementing the annual information security training requirement. 4. Each state agency shall (i) monitor and certify the training activity of its employees to ensure compliance with the annual information security training requirement, (ii) evaluate the efficacy of the information security training program, and (iii) forward to the CIO such certification and evaluation, together with any suggestions for improving the curriculum and materials, or any other aspects of the training program. The CIO shall consider such evaluations when it annually updates its curriculum and materials.

NCSL contact for additional information: Pam Greenberg, NCSL Denver Office, pam.greenberg@ncsl.org.