CodeCenters International
A PLATFORM FOR ENTERPRISE ANALYSIS

433 PLAZA REAL STE 275,
BOCA RATON, FL 33432
PHONE: 954-426-4248
SALES@CODECENTERS.COM

EXPERT DATA, INFRASTRUCTURE DESIGN AND SECURITY AUDITING

DATA SECURITY LAWS FOR STATE GOVERNMENT – HOW CAN WE HELP YOU

Overview

State governments hold a vast amount of data about citizens, including personally identifiable information such as Social Security numbers, driver's license information, and tax and financial information. State databases also have become attractive targets for cybercriminals, who sell the data for personal gain or use it to access government networks or services, to disrupt critical infrastructures or to expose or embarrass governments and officials.

Citizens are often required to provide certain types of data to state government agencies, so protecting that information and maintaining the public's trust is critically important. All states have security measures in place to protect data and systems. However, at least 19 states require, by statute which state government agencies have in place specific policies or measures to ensure the security of the data they hold.

Many of these state laws provide for a statewide, comprehensive approach to security and security oversight. Most state data security laws require agencies to implement and maintain reasonable security procedures and practices to protect sensitive information from unauthorized access, destruction, use, modification, or disclosure. Some laws also require training, periodic security audits or assessments, development of standards and guidelines, and other provisions.

CodeCenters understands what it takes to secure high profile government systems that are targeted for attack while meeting all regulatory requirements. Contact us at Sales@Codecenters.com – 954-426-4248

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
Arizona	Ariz. Rev. Stat. § 18-105	State budget units and state agencies	Establishes a statewide information security and privacy office. Provides that the office serve as the strategic planning, facilitation and coordination office for information technology security in the state. Individual budget units continue to maintain operational responsibility for information technology security. Provides for the appointment of a statewide chief information security officer to manage the statewide information security and privacy office. Requires the office to direct security and privacy compliance reviews, identify and mitigate security and privacy risks, monitor compliance with policies and standards, and coordinate training programs.
California	Calif. Govt. Code § 11549.3 et seq., Calif. Govt. Code § 8592.30-8592.45	State agencies.	Comply with information security program developed by the Chief of the Office of Information Security, as specified/detailed in statute, including conducting an annual independent security assessment. Requires each state agency to implement cybersecurity strategy incident response standards to secure its critical infrastructure controls and critical infrastructure information.
Colorado	C.R.S. §§ 24-37.5-401 et seq.	Public agencies, institutions of higher education	The chief information security officer shall: (a) Develop and update information security policies, standards, and guidelines for public agencies; (b) Promulgate rules pursuant to article 4 of this title containing information security policies, standards, and guidelines;

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
			(c) Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies pursuant to *section 24-37.5-404*; (d) Direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments. Establishes the Colorado Cybersecurity Council and provides for coordination of missions related to homeland security and cybersecurity.
Connecticut	C.G.S. § 4e-70	Any state agency with a department head and any state agency disclosing confidential information to a contractor pursuant to a written agreement with such contractor for the provision of goods or services for the state.	Implement and maintain a comprehensive data-security program for the protection of confidential information. The Secretary of the Office of Policy and Management, or the secretary's designee, may require additional protections or alternate measures of security assurance when warranted.
Florida	Fla. Stat. § 282.318, Fla. Stat. § 20.61	State agencies.	Comply with the statewide information technology security standards and processes developed by the Agency for State Technology **as specified/detailed in statute**, including conducting and updating a comprehensive risk assessment every three years, creating an incident response team and reporting process, and providing security and cybersecurity awareness training for all state agency employees.

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
Georgia	Georgia Code § 50-25-4	Agencies	The Georgia Technology Authority shall have the following powers (21) To establish technology security standards and services to be used by all agencies; (22) To conduct technology audits of all agencies;
Indiana	Ind. Code § 4-13.1-2-2	State agencies	The Office Of Technology shall (9) Review projects, architecture, security, staffing, and expenditures. (10) Develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government. (11) Advise the state personnel department on guidelines for information technology staff for state agencies. (12) Conduct periodic management reviews of information technology activities within state agencies upon request.
Kentucky	K.R.S. § 42-724 K.R.S. § 61.932(1)	Public agencies and nonaffiliated third parties.	An agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches. Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology.

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
Maryland	Md. State Govt. Code §§ 10-1301 to -1304	An executive agency, a department, a board, a commission, an authority, a public institution of higher education, a unit or an instrumentality of the State; or a county, municipality, bi–county, regional, or multicounty agency, county board of education, public corporation or authority, or any other political subdivision of the State.	Implement and maintain a written information security policy and reasonable security procedures and practices that are appropriate to the nature of the personal information collected and the nature of the unit and its operations. Require, by written contract or agreement, that third parties implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information disclosed to the nonaffiliated third party.
Massachusetts	Mass. Gen. Laws Ch. 93H § 2(c)	The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor.	Adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.
Minnesota	Minn. Stat. § 16E.03	State agencies in the executive branch of state government, including the Minnesota Office of Higher Education, but not the	Provides that the chief information officer (CIO) shall establish and enforce standards and ensure acquisition of hardware and software necessary to protect data and systems in state agency networks connected to the Internet.

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
		Minnesota State Colleges and Universities.	Further provides that the CIO shall establish cyber security policies, guidelines, and standards and install and administer state data security systems on the state's computer facilities consistent with policies, guidelines, standards, and state law to ensure the integrity of computer-based and other data and to ensure applicable limitations on access to data.
Montana	Mont. Code § 2-6-1502	Each state agency that maintains personal information.	Develop procedures, **as specified/detailed in statute**, to protect personal information while enabling the state agency to use personal information as necessary for the performance of its duties under federal or state law.
New York	New York State Tech. Law § 103	State agencies.	Provides for the office of information technology services to advise and assist state agencies in developing policies, plans and programs for improving the statewide coordination, administration, security, confidentiality, program effectiveness, acquisition and deployment of technology. Also authorizes the office to perform technology reviews and make recommendations for improving management and program effectiveness pertaining to technology; and to review and coordinate the purchase of technology by state agencies.
North Carolina	N.C. Gen. Stat. § 147-33.110 to -33.112	State agencies.	The state Chief Information Officer shall establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the state's distributed information

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
			technology assets, including communications and encryption technologies. The state CIO shall review and revise the security standards annually. As part of this function, the state Chief Information Officer shall review periodically existing security standards and practices in place among the various state agencies to determine whether those standards and practices meet statewide security and encryption requirements. The state Chief Information Officer may assume the direct responsibility of providing for the information technology security of any State agency that fails to adhere to security standards adopted under this Article.
Ohio	Ohio Rev. Code § 125.18	State agencies	Provides that the chief information officer shall establish policies and procedures for the security of personal information that is maintained and destroyed by state agencies. Provides for a chief information security officer (CISO) who is responsible for the implementation of such policies and procedures. Also provides for the CISO to assist agencies with IT security strategic plans and to review those plans.
Oklahoma	62 Okl. St. § 34.32	Each state agency that has an information technology system.	Conduct an annual information security risk assessment to identify vulnerabilities associated with the information system. The final information security risk assessment report shall identify, prioritize, and document information security vulnerabilities for each of the state agencies assessed. Failure to comply with the requirements of this

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
			subsection may result in funding being withheld from the agency. State agencies shall use either the standard security risk assessment created by the Information Services Division or a third-party risk assessment meeting the ISO/IEC 17799 standards and using the National Institute of Standards and Technology Special Publication 800-30 (NIST SP800-30) process and approved by the Information Services Division.
Oregon	ORS § 182.122, 2016 Ore. Laws Chap. 110	State agencies	Provides for the Oregon Department of Administrative Services, in its sole discretion, to (a) Review and verify the security of information systems operated by or on behalf of agencies; (b) Monitor state network traffic to identify and react to security threats; and (c) Conduct vulnerability assessments of agency information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems.
South Carolina	2015 H.B. 3701 (Budget bill)	All state agencies.	Adopt and implement cyber security policies, guidelines and standards developed by the Department of Administration. The department may conduct audits on state agencies as necessary to monitor compliance. Upon request, public institutions of higher learning, technical colleges, political subdivisions, and quasi-governmental bodies shall submit sufficient evidence that

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
			their cyber security policies, guidelines and standards meet or exceed those adopted and implemented by the department. Exempts judicial and legislative branches.
Texas	Tex. Govt. Code § 2054.0286	State agencies	Provides for employment of a statewide data coordinator to improve the control and security of information collected by state agencies; Requires the statewide data coordinator to develop and implement best practices among state agencies to improve information management and analysis to increase information security.
Utah	Utah Code § 63F-2-102		Creates a data security management council, which shall review existing state government data security policies, assess ongoing risks, notify state and local entities of new risks, coordinate breach simulation exercises, develop data security best practices recommendations for state government. Provides for hiring and training of a chief information security officer for each government entity.
Virginia	Va. Code § 2.2-603 Va. Code § 2.2-2009	Every agency and department in the executive branch of state government, including those appointed by their respective boards or the Board of Education	Every agency and department is responsible for securing the electronic data held by his agency or department and shall comply with the requirements of the commonwealth's information technology security and risk-management program as set forth in § 2.2-2009, and shall report all known incidents that threaten data security. The CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
			appropriate security measures and performing security audits of government electronic information. Such policies, procedures, and standards will apply to the commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. The CIO shall also develop policies, procedures, and standards that shall address the scope of security audits and the frequency of such security audits.
Washington	RCW 43.105.054 RCW 43.105.020, RCW § 43.105.215	State agencies (certain provisions also apply to institutions of higher education the legislature, and the judiciary)	Requires the Consolidated Technology Services Agency to establish security standards and policies to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure. Also provides for implementing a process for detecting, reporting, and responding to security incidents. The director shall appoint a state chief information security officer. Requires each state agency, institution of higher education, the legislature, and the judiciary to develop an information technology security program that adheres to the office's security standards and policies. Requires each state agency to review and update its program annually and certify to the office that its program is in compliance with the office's security standards and policies. Requires state agencies to obtain an independent compliance audit at least once every three years.
West Virginia	W.V. Code § 5A-6-4a	Every agency and department.	The Chief Technology Officer is authorized to develop policies, procedures, standards and legislative rules that

State	Statutory Citation / Link	Applies to Government:	Statutory Summary/Excerpt
			identify and require the adoption of practices to safeguard information systems, data and communications infrastructures. Provides for annual security audits of all executive branch agencies regarding the protection of government databases and data communications.
Wyoming	Wyo. Stat. § 9-21-101	Every agency, department, board, commission, council, institution, separate operating agency or any other operating unit of the executive branch of state government.	Requires every agency to adopt, enforce and maintain a policy regarding the collection, access, security and use of data. The policy shall, at a minimum, comply with applicable federal and state law, adhere to standards set by the state chief information officer and include the following: (i) An inventory and description of all data required of, collected or stored by an agency; (ii) Authorization and authentication mechanisms for accessing the data; (iii) Administrative, physical and logical security safeguards, including employee training and data encryption; (iv) Privacy and security compliance standards; (v) Processes for identification of and response to data security incidents, including breach notification and mitigation procedures; (vi) In accordance with existing law, processes for the destruction and communication of data.