§ 143B-1376. Statewide security and privacy standards.

(a) The State CIO shall be responsible for the security and privacy of all State information technology systems and associated data. The State CIO shall manage all executive branch information technology security and shall establish a statewide standard for information technology security and privacy to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. The State CIO shall review and revise the security standards annually. As part of this function, the State CIO shall review periodically existing security and privacy standards and practices in place among the various State agencies to determine whether those standards and practices meet statewide security, privacy, and encryption requirements. The State CIO shall ensure that State agencies are periodically testing and evaluating information security controls and techniques for effective implementation and that all agency and contracted personnel are held accountable for complying with the statewide information security program. The State CIO may assume the direct responsibility of providing for the information technology security of any State agency that fails to adhere to security and privacy standards adopted under this Article.

(b) The State CIO shall establish standards for the management and safeguarding of all State data held by State agencies and private entities and shall develop and implement a process to monitor and ensure adherence to the established standards. The State CIO shall establish and enforce standards for the protection of State data. The State CIO shall develop and maintain an inventory of where State data is stored. For data maintained by non-State entities, the State CIO shall document the reasons for the use of the non-State entity and certify, in writing, that the use of the non-State entity is the best course of action. The State CIO shall ensure that State data held by non-State entities is properly protected and is held in facilities that meet State security standards. By October 1 each year, the State CIO shall certify in writing that data held in non-State facilities is being maintained in accordance with State information technology security standards and shall provide a copy of this certification to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division.

(c) Before a State agency can contract for the storage, maintenance, or use of State data by a private vendor, the agency shall obtain the approval of the State CIO.

(d) With the approval of the State CIO, enterprise-level system owners may share data between their secure systems and other enterprise-level secure systems to maximize State government's effectiveness and productivity, unless sharing the data is expressly prohibited by State or federal law. Sharing of data under this subsection shall include the transfer of PII or other potentially sensitive data only when appropriate safeguards are in place for both the transfer of the data and storage of the data in the receiving system and when consistent with the Statewide Information Security Policy. For purposes of this subsection, the term "owner" means a State agency having both (i) possession or control of data with the ability to access, create, modify, transfer, or remove data and (ii) authority to assign access privileges to others. (2015-241, s. 7A.2(b); 2019-200, s. 6(f); 2021-180, s. 25.2(a).)