

VIRGINIA ACTS OF ASSEMBLY -- 2007 SESSION

CHAPTER 769

An Act to amend and reenact §§ 2.2-2006 and 2.2-2009 of the Code of Virginia, relating to security of confidential data maintained by a state agency.

[S 845]

Approved March 23, 2007

Be it enacted by the General Assembly of Virginia:

1. That §§ 2.2-2006 and 2.2-2009 of the Code of Virginia are amended and reenacted as follows:

§ 2.2-2006. Definitions.

As used in this chapter:

"Board" means the Information Technology Investment Board created in § 2.2-2457.

"Communications services" includes telecommunications services, automated data processing services, and management information systems that serve the needs of state agencies and institutions.

"Confidential data" means information made confidential by federal or state law that is maintained by a state agency in an electronic format.

"Information technology" means telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services. It is in the interest of the Commonwealth that its public institutions of higher education in Virginia be in the forefront of developments in technology. Therefore, the provisions of this chapter shall not be construed to hamper the pursuit of the missions of the institutions in instruction and research.

"Major information technology project" means any state agency information technology project that (i) is mission-critical, (ii) has statewide application, or (iii) has a total estimated cost of more than \$1 million.

"Noncommercial telecommunications entity" means any public broadcasting station as defined in § 2.2-2427.

"Public telecommunications entity" means any public broadcasting station as defined in § 2.2-2427.

"Public telecommunications facilities" means all apparatus, equipment and material necessary for or associated in any way with public broadcasting stations or public broadcasting services as those terms are defined in § 2.2-2427, including the buildings and structures necessary to house such apparatus, equipment and material, and the necessary land for the purpose of providing public broadcasting services, but not telecommunications services.

"Public telecommunications services" means public broadcasting services as defined in § 2.2-2427.

"Secretary" means the Secretary of Technology.

"State agency" or "agency" means any agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch listed in the appropriation act. However, the terms "state agency," "agency," "institution," "public body," and "public institution of higher education," shall not include the University of Virginia Medical Center.

"Technology asset" means hardware and communications equipment not classified as traditional mainframe-based items, including personal computers, mobile computers, and other devices capable of storing and manipulating electronic data.

"Telecommunications" means any origination, transmission, emission, or reception of signs, signals, writings, images, and sounds or intelligence of any nature, by wire, radio, television, optical, or other electromagnetic systems.

"Telecommunications facilities" means apparatus necessary or useful in the production, distribution, or interconnection of electronic communications for state agencies or institutions including the buildings and structures necessary to house such apparatus and the necessary land.

§ 2.2-2009. Additional duties of the CIO relating to security of government data and databases.

A. To ensure the security of state government databases and data communications from unauthorized uses, intrusions or other security threats, the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits. In developing and updating such policies, procedures and standards, the CIO shall consider, at a minimum, the advice and recommendations of the Council on Technology Services created pursuant to § 2.2-2651.

B. The CIO shall designate a government entity to oversee, plan and coordinate the conduct of periodic security audits of all executive branch agencies and institutions of higher education regarding the protection of government databases and data communications.

1. Security audits may include, but are not limited to, on-site audits as well as reviews of all written

security procedures.

2. The designated entity may contract with a private firm or firms that specialize in conducting such audits subject to approval of the CIO.

C. All public bodies subject to such audits as required by this section shall fully cooperate with the entity designated to perform such audits.

D. The provisions of this section shall not infringe upon responsibilities assigned to the Comptroller, the Auditor of Public Accounts, or the Joint Legislative Audit and Review Commission by other provisions of the Code of Virginia.

E. *To ensure the security and privacy of citizens of the Commonwealth in their interactions with state government, the CIO shall direct the development of policies, procedures, and standards for the protection of confidential data maintained by state agencies against unauthorized access and use. Such policies, procedures, and standards shall include, but not be limited to:*

1. Requirements that any state employee or other authorized user of a state technology asset provide passwords or other means of authentication to (i) use a technology asset and (ii) access a state-owned or operated computer network or database; and

2. Requirements that a digital rights management system or other means of authenticating and controlling an individual's ability to access electronic records be utilized to limit access to and use of electronic records that contain confidential data to authorized individuals.

F. The CIO shall promptly receive reports from directors of departments in the executive branch of state government made in accordance with § 2.2-603 and shall take such actions as are necessary, convenient or desirable to ensure the security of the Commonwealth's databases ~~and~~, data communications, *and confidential data.*

2. That the provisions of this act shall become effective on July 1, 2008.