Fla. Stat. § 282.0041

Current through Chapter 1 of the 2024 session and through the 2023 C special session.

LexisNexis® Florida Annotated Statutes > Title XIX. Public Business. (Chs. 279 — 290) > Chapter 282. Communications and Data Processing. (Pts. I — III) > Part I. Enterprise Information Technology Services Management. (§§ 282.003 — 282.34)

§ 282.0041. Definitions.

As used in this chapter, the term:

(1) "Agency assessment" means the amount each customer entity must pay annually for services from the Department of Management Services and includes administrative and data center services costs.

(2) "Agency data center" means agency space containing 10 or more physical or logical servers.

(3) "Breach" has the same meaning as provided in s. 501.171.

(4) "Business continuity plan" means a collection of procedures and information designed to keep an agency's critical operations running during a period of displacement or interruption of normal operations.

(5) "Cloud computing" has the same meaning as provided in Special Publication 800-145 issued by the National Institute of Standards and Technology.

(6) "Computing facility" or "agency computing facility" means agency space containing fewer than a total of 10 physical or logical servers, but excluding single, logical-server installations that exclusively perform a utility function such as file and print servers.

(7) "Customer entity" means an entity that obtains services from the Department of Management Services.

(8) "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources.

(9) "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted.

(10) "Data governance" means the practice of organizing, classifying, securing, and implementing policies, procedures, and standards for the effective use of an organization's data.

(11) "Department" means the Department of Management Services.

(12) "Disaster recovery" means the process, policies, procedures, and infrastructure related to preparing for and implementing recovery or continuation of an agency's vital technology infrastructure after a natural or human-induced disaster.

(13) "Electronic" means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(14) "Electronic credential" means an electronic representation of the identity of a person, an organization, an application, or a device.

(15) "Enterprise" means state agencies and the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services.

(16) "Enterprise architecture" means a comprehensive operational framework that contemplates the needs and assets of the enterprise to support interoperability.

(17) "Enterprise information technology service" means an information technology service that is used in all agencies or a subset of agencies and is established in law to be designed, delivered, and managed at the enterprise level.

(18) "Event" means an observable occurrence in a system or network.

(19) "Incident" means a violation or an imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur.

(20) "Information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form.

(21) "Information technology policy" means a definite course or method of action selected from among one or more alternatives that guide and determine present and future decisions.

(22) "Information technology resources" has the same meaning as provided in s. 119.011.

(23) "Interoperability" means the technical ability to share and use data across and throughout the enterprise.

(24) "Open data" means data collected or created by a state agency, the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services, and structured in a way that enables the data to be fully discoverable and usable by the public. The term does not include data that are restricted from public disclosure based on federal or state laws and regulations, including, but not limited to, those related to privacy, confidentiality, security, personal health, business or trade secret information, and exemptions from state public records laws; or data for which a state agency, the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services is statutorily authorized to assess a fee for its distribution.

(25) "Performance metrics" means the measures of an organization's activities and performance.

(26) "Project" means an endeavor that has a defined start and end point; is undertaken to create or modify a unique product, service, or result; and has specific objectives that, when attained, signify completion.

(27) "Project oversight" means an independent review and analysis of an information technology project that provides information on the project's scope, completion timeframes, and budget and that identifies and quantifies issues or risks affecting the successful and timely completion of the project.

(28) "Ransomware incident" means a malicious cybersecurity incident in which a person or an entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a state agency's, county's, or municipality's data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

(29) "Risk assessment" means the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

(30) "Service level" means the key performance indicators (KPI) of an organization or service which must be regularly performed, monitored, and achieved.

(31) "Service-level agreement" means a written contract between the Department of Management Services or a provider of data center services and a customer entity which specifies the scope of services provided, the service level, the duration of the agreement, the responsible parties, and the service costs. A service-level agreement is not a rule pursuant to chapter 120.

(32) "Stakeholder" means a person, group, organization, or state agency involved in or affected by a course of action.

(33) "Standards" means required practices, controls, components, or configurations established by an authority.

(34) "State agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission.

The term does not include university boards of trustees or state universities. As used in part I of this chapter, except as otherwise specifically provided, the term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services.

(35) "SUNCOM Network" means the state enterprise telecommunications system that provides all methods of electronic or optical telecommunications beyond a single building or contiguous building complex and used by entities authorized as network users under this part.

(36) "Telecommunications" means the science and technology of communication at a distance, including electronic systems used in the transmission or reception of information.

(37) "Threat" means any circumstance or event that has the potential to adversely impact a state agency's operations or assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

(38) "Variance" means a calculated value that illustrates how far positive or negative a projection has deviated when measured against documented estimates within a project plan.

History

SS. 3, 11, ch. 83-92; s. 17, ch. 87-137; ss. 10, 11, ch. 90-160; s. 4, ch. 91-171; s. 10, ch. 91-221; s. 5, ch. 91-429; s. 3, ch. 92-98; s. 95, ch. 92-142; s. 14, ch. 94-226; s. 11, ch. 94-340; s. 9, ch. 97-286; s. 16, ch. 2000-164; s. 51, ch. 2001-61; s. 10, ch. 2001-261; s. 4, ch. 2007-105, eff. July 1, 2007; s. 5, ch. 2008-116, eff. June 10, 2008; s. 6, ch. 2009-80, eff. May 27, 2009; s. 5, ch. 2010-78, eff. July 1, 2010; s. 9, ch. 2010-148, eff. May 28, 2010; s. 3, ch. 2011-50, eff. May 26, 2011; s. 4, ch. 2014-189, effective July 1, 2014; s. 9, ch. 2014-221, effective July 1, 2014; s. 58, ch. 2018-10, effective July 1, 2018; s. 78, ch. 2019-116, effective July 1, 2019; s. 8, ch. 2019-118, effective July 1, 2019; s. 3, ch. 2020-161, effective July 1, 2020; s. 2, ch. 2021-234, effective July 1, 2021; s. 2, ch. 2022-153, effective July 1, 2022; s. 1, ch. 2022-220, effective July 1, 2022.

End of Document