CHAPTER 60GG-4
CLOUD COMPUTING

60GG-4.001 Purpose and Applicability; Definitions

60GG-4.002 Cloud Procurement and Contractual Elements

60GG-4.003 Cloud Financials

60GG-4.004 Cloud Security and Risk Mitigation Strategy

60GG-4.005 State Agency Request for Variance or Waiver

60GG-4.001 Purpose and Applicability; Definitions

(1) These rules apply to state agencies as defined in section 282.0041, Florida Statutes.

(2) These rules are designed to further state agency implementation of the cloud-first policy as provided in section 282.206, Florida Statutes, that requires state agencies to show a preference for cloud computing services that minimize or do not require the purchasing, financing, or leasing of state data center infrastructure when cloud-computing solutions meet the needs of the agency, reduce costs, and meet or exceed the applicable state and federal laws, regulations, and standards for information technology security.

(3) These rules establish the requirements for state agencies to create formal processes to provide a preference for and to properly evaluate cloud computing services during procurement while ensuring that state agencies have adequately addressed and demonstrated protections to ensure that systems provisioned in the cloud are appropriately secure and performant, appropriate to the workload and data hosted, and ultimately ensure the availability, integrity and confidentiality of state data and resources.

(4) Definitions:

(a) Breach - has the same meaning as provided in section 501.171, Florida Statutes.

(b) Cloud Computing – a service, solution or option as defined in Special Publication 800-145 issued by the National Institute for Standards and Technology (NIST).

(c) Cloud Service Provider – Person, organization, or entity responsible for making a cloud computing service, solution or option available to a consumer.

(d) Data – has the same meaning as defined in section 282.0041, Florida Statutes.

(e) Data Classification – The act of categorizing information systems and the information processed, stored, and transmitted by those systems based on the security impact analysis found under the risk assessment process outlined in 60GG-2.002, Florida Administrative Code, Information Security Categorization.
(f) Department of Management Services (DMS) – State agency created pursuant to section 20.22, F.S., which includes the Division of State Technology (DST), responsible for operating the state data center and developing statewide information technology policy, among other functions.

(g) Information Technology – has the same meaning as defined in section 282.0041, Florida Statutes.

(h) Interoperability - The ability for two disparate information technology systems to exchange data in a coordinated manner and make use of the data exchanged.

(i) Managed Services – the delivery of information technology services, such as network, application, infrastructure and security, via continuous, regular management and support, to include active administration on the customer’s premises, in the service provider’s data center, or in a third-party data center.

(j) Open data – has the same meaning as defined in section 282.0041, Florida Statutes.

(k) Portability – The ease by which data or an information technology system can be extracted, transformed, and loaded from one computing environment to another.

(l) Service Level Agreement (SLA) – a component of an agreement between a cloud service provider and a customer. The SLA describes the IT service, documents service level requirements, and specifies the responsibilities of the cloud service provider and the customer.

Rulemaking Authority 282.0051(19) FS. Law Implemented 282.0051(6) FS. History-New______.

60GG-4.002 Cloud Procurement and Contractual Elements

(1) As part of their cloud-first policy, the state agency will develop formal procedures to be used when procuring information technology that establish a preference for cloud computing.

(2) Where products or services are required for cloud migration and integration with products or services hosted at the State Data Center (SDC), the state agency shall consult with the Division of State Technology (DST) prior to the procurement of cloud services to ensure compatibility and security. The state agency will document such consultation in writing.

(3) The state agency will maintain and provide to DST by October 15 of each year a comprehensive, documented record of applications, workload, data, and services procured or placed into a cloud service provider environment. The record will include the business system’s common name, purpose, operating requirements, and estimated annual cost of cloud computing.
(4) The state agency will ensure that security and interoperability with applications that interface outside the cloud service provider’s cloud are well documented and addressed, including data egress charge models.

(5) The state agency will ensure that technical security controls are commensurate with the data’s classification as defined in Rule Chapter 60GG-2, Information Security, F.A.C.

(6) The state agency will ensure that contracts reflect the restriction on the geographic location of data to the continental United States unless approved in writing by the agency head or designee. Remote access to data, other than open data, from outside the continental United States is prohibited unless approved in writing by the agency head or designee.

(7) Prior to execution of the contract and deployment of a cloud computing service, the state agency shall ensure that the cloud service provider delivers audit reports based on the classification of the data, for the agency assessment of the effectiveness and suitability of the cloud service provider. During the contract term, the state agency will ensure that security controls required under (5) above are well documented and addressed.

(8) The state agency will maintain data ownership and will include contractual provisions for portability for risk management purposes.

(9) The state agency will include contract provisions, associated with end of contract or breach of contract, that fully document the exit strategy for cloud computing services or applications, including data acquisition, migration strategy, high-level timeline, and costs.

(10) The state agency will ensure that Service Level Agreement (SLA) requirements for cloud computing availability, performance, and response are included in the contract.

(11) The contract will provide for performance and service level monitoring and reporting from the cloud service provider to the state agency.

(12) The state agency will ensure contractual financial consequences are included in the contract in the event of the cloud service provider’s failure to perform as agreed under the terms of the service level agreement, consistent with applicable law.

(13) The state agency will validate that the cloud service provider’s disaster recovery plan is developed commensurate with data classification and complies with Rule Chapter 60GG-2, Florida Administrative Code, Information Technology Security. If the disaster recovery plan is modified during the contract term, the cloud service provider will provide the modified plan to the state agency.
60GG-4.003 Cloud Financials

(1) The state agency will document the controls and processes that are in place to proactively control cloud spend and maintain acceptable budgeted versus actual variances.

(2) The state agency will establish and document, in advance of contract execution, an acceptable threshold for budgeted variance and mitigation plan based upon risk tolerance.

(3) The state agency will perform a documented review of budgeted versus actual cloud spend on a monthly basis and maintain records for at least 24 months or in compliance with retention schedules, whichever is longer.

60GG-4.004 Cloud Security and Risk Mitigation Strategy

(1) The state agency will document a risk mitigation strategy including but not limited to an exit strategy specific to application criticality and business continuity needs.

(2) The state agency will ensure that the documented risk mitigation strategy is supported by the contract with the cloud service provider.

(3) The state agency will identify and document all current security rules (to include Chapter 60GG-2, Florida Administrative Code, Information Technology Security) and applicable standards that apply to state agency applications regardless of hosting infrastructure. The state agency will base the data classification on the Federal Information Processing Standards (FIPS) Publication No. 199.

(4) The state agency will develop a security plan that documents compliance with applicable data classification requirements.

(5) The state agency will conduct and document a security assessment for the implementation of each cloud service, which will contain data classified as moderate or higher based on the data classification of FIPS Publication No. 199, and consider the potential risk of breach of data deployed in the cloud. This assessment may be performed by a third party (to include a government entity).

(6) To prevent Internet Protocol (IP) routing conflicts, state agencies will consult with the Division of State Technology (DST) prior to the use of cloud-based services where DMS allocated IP addresses (including RFC1918
IP addresses) will be assigned to cloud-based resources that have State Data Center (SDC) or state intranet connectivity requirements. The state agency will document such consultation in writing.

*Rulemaking Authority*282.0051(19) FS. Law Implemented 282.0051(6) FS. History-New_____.

**60GG-4.005 State Agency Request for Variance or Waiver**

A state agency may request a variance or waiver from these rules by filing a petition with the Department of Management Services (DMS) agency clerk, with a copy to the Joint Administrative Procedures Committee in accordance with section 120.542, Florida Statutes, and Chapter 28-104, Florida Administrative Code, Variance or Waiver. The DMS Secretary, or designee, will review the request and provide an approval or rejection.

*Rulemaking Authority*282.0051(19) FS. Law Implemented 282.0051(6) FS. History-New_____.