8-607. Cloud computing.

(1) Cloud computing, defined.

This standard incorporates the following definition from the National Institute of Standards and Technology (NIST SP 800-145, September 2011 [footnotes omitted]):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprised of multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound

together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Other Deployment Models [not part of the NIST definition]:

Government community cloud. A community cloud infrastructure provisioned solely for use by federal, state, and/or local government.

State cloud. The private cloud infrastructure provided by the Office of the CIO.

(2) Standard.

(a) The following table contains the acceptable uses of cloud computing by state agencies. The classification of the data to be processed or stored using cloud computing determines the acceptable options. If there is a mix of data classifications, the most restrictive data classification must be used.

Data Classification	Cloud Deployment Models					
	State Cloud	Private Cloud	Government Community Cloud	Community Cloud	Public Cloud	Hybrid Cloud
RESTRICTED	✓	△	△	△	⊘	△
CONFIDENTIAL	✓	△	✓	△	⊘	△
MANAGED ACCESS PUBLIC	✓	✓	✓	✓	✓	✓
PUBLIC	✓	✓	✓	✓	✓	✓

(✓) means an approved deployment model for cloud computing;
(⊘) means an unapproved deployment model for cloud computing; and
(△) means prior approval by the Office of the CIO is required.

(b) Prior approval process. An agency requesting prior approval of a cloud computing service must submit a service request to the Office of the CIO Service Desk. The request should provide detailed information about the cloud deployment model and data to be processed or stored using cloud computing. The Office of the CIO will respond to the request within four business days. The Office of the CIO may approve the request, approve the request with conditions, deny the request, or request additional information.

(c) Exemption for existing services. Cloud computing services in use on December 31, 2017, are exempt from the requirements of this section. The exemption for an existing service ends when either: (1) the current term of the agreement for such service expires; or (2) there are significant changes to the service.

(d) FedRAMP compliance. If the cloud service provider (CSP) does not have an official FedRAMP certification by an accredited third-party assessor organization (3PAO) and the CSP may store or process any CONFIDENTIAL or RESTRICTED data, the following conditions must be met or addressed in an agreement with the CSP:

(i) The cloud service provider or third-party host (CSP/3PH) must provide evidence of secure storage of access credentials that are at least equal to that of state's internal systems;

(ii) Access to the cloud service must require multi-factor authentication based on data classification levels;

(iii) De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials;

(iv) Information must be encrypted using IT approved technology for information in transit as well as information stored or at rest;

(v) Encryption key management will be controlled and managed by the state unless explicit approval for key management is provided to CSP/3PH by the agency;

(vi) All equipment removed from service, information storage areas, or electronic media that contained state information must have the information purged using appropriate means. Data destruction must be verified by the state before allowing that equipment, information storage space, or media to be destroyed or assigned for reuse. A certificate of destruction must be provided for equipment that has been destroyed;

(vii) CSP/3PH must provide vulnerability scanning and testing on a schedule approved by the state information security officer. Results will be provided to agency;

(viii) Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at state;

(ix) CSP/3PH must meet all state requirements for chain of custody and information breach notification. CSP/3PH will maintain an incident management program that notifies the state within one (1) hour of a breach;

(x) CSP/3PH will provide evidence of audit and assessment of the security of the service environment, and will agree to reasonable inspection of such security by gency-authorized parties;

(xi) CSP/3PH is required to advise the state on all geographic locations of stored state information. CSP/3PH will not allow state information to be stored or accessed outside the United States. This includes both primary and alternate sites;

(xii) Privileged access roles at the CSP/3PH are required to meet the same vetting standards of privileged access personnel at the state, such as background checks, etc.;

(xiii) CSP/3PH's must have SLAs in place that clearly define security and performance standards;

(xiv) CSP/3PH will provide adequate security and privacy training to its associates, and provide the state information security officer with evidence of this training;

(xv) CSP/3PH will provide the state with the functionality to conduct a search of the data to meet public records requests; and

(xvi) Before contracting with a CSP/3PH, the state shall have proactive records planning in place to ensure the ability to have timely and actual destruction of records in accordance with Department record retention policies.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-607.pdf