Idaho Technology Authority (ITA)

ENTERPRISE CLOUD POLICY – P1000 GENERAL POLICIES

Category: P1080 – Cloud Computing

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-5745C(3)

Idaho statute states in part "the Idaho Technology Authority shall:

> Within the context of its strategic plans, establish statewide information technology and telecommunications policies, standards, guidelines, conventions and comprehensive risk assessment criteria that will assure uniformity and compatibility of such systems within state agencies;"

II. ABSTRACT

This Cloud Computing policy is designed to help agencies to use State resources wisely. While a connection to the Cloud offers a variety of benefits to the State of Idaho, it can also expose the State to significant risk to its data and systems if appropriate cyber security controls and data protection procedures are not employed. Inappropriate Cloud usage may also expose the State of Idaho and/or the agency to legal liability.

III. DEFINITIONS

1. Cloud - Cloud computing is a computing practice where scalable and adaptable IT-enabled capabilities are delivered as a service to external customers using Cloud based solutions. Cloud services can be delivered by a third-party Cloud Service Provider (CSP), or internally through the establishment of state owned services and infrastructure.

2. Private cloud computing is a form of cloud computing that is used by only one organization, or that ensures that an organization is completely isolated from others.

3. **Service Models:**

    a. *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.
    b. *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.
    c. *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).
    d. *Desktop as a Service (DaaS).* The capability provided to the consumer is to use the provider's cloud infrastructure to deploy a virtualized desktop experience, delivered to a customer on demand from a remotely hosted location. The customer accesses a customized virtualized desktop from various client devices. The consumer does not manage or control the underlying desktop infrastructure, with the possible exception of limited user-specific application configuration settings.

4. **Deployment Models**

    a. *Private cloud.* The cloud infrastructure is provisioned for exclusive use by a single organization comprising 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.
    b. *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.

c. *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.

d. *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).

IV. POLICY

A. Cloud Monitoring

Each agency shall ensure that Cloud use from all computers and devices connected to the state network are monitored. Records of the monitored traffic should be retained based on agency requirements. [CSPs shall support State and applicable Federal compliance requirements supporting the design, implementation, testing, use, and monitoring of supporting cloud services.]

B. Cloud Filtering

Each agency shall ensure that access to websites and protocols that are compliant with the ITA Policy P4570 (Firewall Security).

C. Cloud Use

1. When considering cloud services, the highest priority should be given to ensuring the security of confidential state data. Agencies are encouraged to evaluate and utilize Cloud Services as a tool for meeting the business needs of the agency. Where practical, agencies are encouraged to consider shared cloud services across agency boundaries to take advantage of economies of scale where practical without jeopardizing the privacy and security of a given agencies data.[Ensure that logical and physical separation of information and data controls are in place. See ITA Policy P4120 (Online File Storage Services) for additional guidance.
2. Agencies will keep an inventory of all cloud services and provide that inventory to the OCIO.
3. The state agency will be the explicit owner nominated for all cloud services utilized by an agency.
4. There will be a documented decision process to categorize any data for cloud services ranging from high sensitivity to Public information.
5. All privileged users of cloud services shall utilize strong authentication practices, all users of cloud services that contain sensitive data shall also utilize strong authentication practices.

6. Agencies utilizing cloud services shall have documented contingency planning procedures to cover at a minimum termination of services, extended outages, and permanent outages.
    a. Terms of Service of the online file storage service vendor must include provisions that the data, once it is in the cloud, does not become the property of the vendor or become public data provide data backup procedures to include purging (IAW NIST 800-88 & ITA Policy P4120) after the end of storage life
    b. An exit clause in the online file storage Terms of Service shall include provisions for allowing the retrieval of all state owned data when a contract is ended by either party
7. Cloud access falls under the State's computer use policy and as such the State has the right to monitor the use of cloud services at any time. Therefore, users should not have any expectation of privacy as to their Cloud usage via State computers and networks
8. The primary purpose of Cloud services is to conduct official State business. Standing State computer acceptable use policies and other State policy applies to Cloud services at all times
9. A Cloud user can be held accountable for any breaches of policy, security, or confidentiality resulting from their use of the Cloud. Such violations of this policy may result in disciplinary action.

V. EXEMPTION PROCESS

Refer to ITA Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework).

VI. PROCEDURE REFERENCE

NIST SP 800-145, SP 800-144, SP 800-53 R4, ITA Policy P4570 (Firewall Security), ITA Policy P1040 (Employee Electronic Email and Messaging Use), ITA Policy P4120 (Online File Storage Services)

VII. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.

VIII. RESPONSIBILITIES

Users should schedule, wherever possible, communications-intensive operations such as large file transfers, video downloads, and the like for off-peak usage times.

REVISION HISTORY

9/8/2016 – Revised to add “Desktop as a Service” (DaaS) to the Service Models definitions.

2/23/2016 – Section C.1. Revised to include additional language related to security of data.

Date Established: December 8, 2015