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 measures and data protection policies are not employed. Unlawful 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 service provider, 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. Gartner defines public cloud computing as a style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies—i.e., public cloud computing uses cloud computing technologies to support customers that are external to the provider's organization. Using public cloud services generates the types of economies of scale and sharing of resources that can reduce costs and increase choices of technologies. From a government organization's perspective, using public cloud services implies that any organization (in any industry sector and jurisdiction) can use the same services (e.g., infrastructure, platform or software), without guarantees about where data would be located and stored.

4. *Hybrid* **cloud computing** refers to policy-based and coordinated service provisioning, use and management across a mixture of internal and external cloud services.

5. *Cloud 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 a thin client interface such as a Web browser (e.g., Web-based email). 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.

6. *Cloud 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 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 application hosting environment configurations.

7. *Cloud 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, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

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.

B. Cloud Filtering

Each agency shall ensure that access to websites and protocols that are deemed inappropriate (e.g. the criteria in Section C, sub-section 6, A thru M) are blocked.

C. Cloud Use

1. 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.

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.

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 use 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 *Policy 1010 – Information Technology Policies, Standards, and Guidelines Framework*.

VI. PROCEDURE REFERENCE

There are no procedure references to this policy. (References?)

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

Date Established: TBD