Idaho Technology Authority (ITA)

ENTERPRISE CLOUD POLICY – P1000 GENERAL POLICIES

Category: P1090 – Cloud Services

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-833

II. ABSTRACT

This Cloud Services policy is designed to help agencies use State resources wisely. While a connection to the Cloud Services 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. Accountability for security and privacy in public cloud deployments cannot be delegated to a cloud provider and remains an obligation for the agency to fulfill.

III. DEFINITIONS

See ITA Guideline G105 (Glossary of Terms) for any definitions.

IV. POLICY

Agencies shall meet the following minimum requirements when using Cloud Services:

a) Prior to enabling cloud service usage, agencies shall classify all data according to ITA policy P4130 – Information Systems Classification.
b) All Non-Public State Data shall be encrypted at rest and in transit with controlled access. All encryption shall be consistent with validated cryptography standards such as the current standards in FIPS 140-2, Security Requirements for Cryptographic Modules, or the then-current NIST recommendation
c) Classification Level 4 data is not allowed on any Cloud Service.
d) Cloud Service provider's Terms-Of-Service (TOS) agreements must include provisions:

i) That the data, once it is in the cloud, does not become the property of the vendor or any other entity, or become data in the public domain.
ii) For allowing the retrieval of all State data when a contract is ended by either party.

e) Agencies shall centrally manage the creation and de-activation of Cloud Service accounts.
f) Agencies shall conduct periodic audits to prevent and identify the misconfiguration or misuse of Cloud Service services.
g) Data in Cloud Services must be securely disposed of once the contract has been terminated and data has been retrieved to the satisfaction of the State agency.
h) Contractors doing work for state agencies may only host data and records classified as Level 1 on Cloud Service services after receiving the supported agency's explicit written approval.
i) Employees and contractors are only permitted to use official, agency-provided Cloud Service accounts for state business.
j) See ITA Guideline G595 (Public Online File Storage Service Guidelines) for additional guidance.

V. EXEMPTION PROCESS

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

VI. PROCEDURE REFERENCE

NIST SP 800-145: The NIST Definition of Cloud Computing

NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing.

NIST SP 800-53A Rev. 5: Assessing Security and Privacy Controls in Information Systems and Organizations

FIPS-199: Standards for Security Categorization of Federal Information and Information Systems

ITA Policy P4130 (Information System Classification Levels)

ITA Policy P4570 (Firewall Security),

ITA Policy P1040 (Employee Electronic Email and Messaging Use),

ITA Guideline G595 (Public Online File Storage Service Guidelines)

VII. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

REVISION HISTORY

Date Established: Approved by ITLC: April 16, 2024