# Information Technology Authority (ITA)

# ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

**Category: P4120 – PUBLIC ONLINE FILE STORAGE SERVICES**

**CONTENTS:**



## I. AUTHORITY

Authority: Idaho Code § 67-5745(C)(3)

## II. ABSTRACT


Online or cloud file storage services such as DropBox, Google Drive, iCloud, OneDrive, etc., provide a fast and convenient way of sharing files with other people, entities and the use of different devices. Although convenient these services pose a significant information security risk enabling employees to bypass agency information security controls, circumvent legal discovery requirements and ignore records retention policies. 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

**Agency** – All state departments, boards, commissions, councils and institutions of higher education; but not elected constitutional officers and their staffs, the legislature and its staff, or the judiciary [per Idaho Code, 67-5745(A)].

**Classification Levels -** The State of Idaho supports the following classification levels (ITA Policy P4130):

a. Classification Level 1: “Unrestricted” includes, but is not limited to, any information relating to the conduct or administration of the public's business prepared, owned, used or retained by any state agency, independent public body

corporate and politic or local agency regardless of physical form or characteristics. The agency's worst case scenario for a breach of confidentiality, integrity, and availability is considered low impact (FIPS-199).

Examples: Press releases, brochures, pamphlets, public access web pages, and materials created for public consumption.

b. Classification Level 2: "Limited" includes sensitive information that may or may not be protected from public disclosure but if made easily and readily available may jeopardize the privacy or security of agency employees or individuals. The agency's worst case scenario for a breach of confidentiality, integrity, or accessibility is considered medium impact (FIPS-199).

Examples: Enterprise risk management planning documents, published internal audit reports, detailed financial transactions, email, non-public phone numbers, or building schematics, names and addresses that are not protected from disclosure.

c. Classification Level 3: "Restricted' includes sensitive information intended for agency use that may be exempted from public use and disclosure. Unauthorized disclosure may jeopardize the privacy or security of agency employees, organizations, or individuals. Direct access is limited to internal parties authorized in the performance of their duties. External agencies requesting this information for authorized agency business must be under contractual obligation of confidentially or confidentiality with the disclosing agency (for example, confidentiality/non-disclosure agreement) prior to receiving the information. The agency's worst case scenario for a breach of confidentiality, integrity, or accessibility is considered high impact (FIPS-199).

Examples: Network diagrams, information systems and telecommunications systems configuration information, security plans, administrator level passwords, personally identifiable information, bank account numbers, child welfare and legal information about minors, student education records, social security numbers, other information exempt from public disclosure.

d. Classification Level 4: "Critical" includes extremely sensitive information. Information disclosure could potentially cause major damage or injury up to and including death to the named individual, or agency employees. The agency's worst case scenario for a breach of confidentiality, integrity, or accessibility is considered high impact (FIPS-199).

Examples: Disclosure that could result in loss of life, disability or serious injury or regulated information with significant penalties for unauthorized disclosure. Included is information that is typically exempt from public disclosure.

**Online File Storage Service** – A file hosting service, cloud storage service or online file storage provider, file transfer facilitator or file share systems such as Torrent services, external storage devices, or ANY data storage and or data transfer solutions otherwise not supported and authorized by the State of Idaho that is designed to host or backup user files on the Internet. Online File Storage Services allows users to upload data, download data, store data at rest, transfer data, and share data which then is accessed over the Internet from other computers, tablets, smartphones, mobile devices, or other networked devices, by the same user or by other designated users.

**Sensitivity:** A measure of the importance assigned to the information by its owner for the purpose of denoting the need for protection (ITA Policy P4130).

## IV. POLICY

1. Each online file storage service shall meet the following minimum requirements when an agency is determining a cloud file storage solution:

a) Classification Level 2 & 3 information must be encrypted in transit to and at rest on online file storage services (the cloud). Classification Level 4 data is not allowed on any online file storage service.
b) Online file storage service provider's Terms-Of-Service (TOS) agreements must include provisions that the data, once it is in the cloud, does not become the property of the vendor or become data in the public domain.
c) Agencies shall centrally manage the creation and de-activation of online file storage service accounts.
d) Agencies shall conduct periodic audits and implement a Cloud Access Service Broker (CASB) or equivalent to prevent the misconfiguration or misuse of online file storage services.
e) Agencies shall ensure that the service provider's TOS include provisions for allowing the retrieval of all State owned data when a contract is ended by either party.
f) Data on the online cloud storage service must be securely disposed of once the contract has been terminated and data has been retrieved to the satisfaction of the State agency.
g) Agencies must ensure that online file storage of State data is expressly authorized and is stored in compliance with this policy.

2. Contractors doing work for state agencies may only host data and records classified as Level 1 on online file storage services after receiving the supported agency's explicit approval.

3. Employees and contractors are not permitted to use personal online file storage accounts for state business.

## V. EXEMPTION PROCESS

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

## VI. PROCEDURE REFERENCE

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

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

ITA Policy P4130 (Information System Classification Levels)

ITA Guideline G595 (Public Online File Storage Service Guidelines)

## VII. CONTACT INFORMATION

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

## REVISION HISTORY

9/8/2016 – Revised to clarify and expand definitions; added Classification Level 4 to definitions.

Established: February 25, 2015