Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G595 PUBLIC ONLINE FILE STORAGE SERVICES GUIDELINE

CONTENTS:

I. DEFINITIONS

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

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 designed to host or backup user files on the Internet. It allows users to upload files that can then be accessed over the Internet from other computers, tablets, smartphones or other networked devices, by the same user or by other designated users.

II. RATIONALE

These guidelines provide recommended best practices for agencies to use when allowing users to store files via online services, in accordance with ITA Policy P4120 (Public Online File Storage Services).

III. GUIDELINE

Agencies should make a deliberate, informed decision on whether to authorize the use of online file storage services for agency records depending on the situation.

An agency, when authorizing the use of online file storage services should consider the following:

1). If the data is released to the public what is the risk to your agency or the state?
2). Do people depend on this data to do their job?
3). If the data is unavailable will the agency or division still be able to function?

4). What is the online file storage service provider's incident response plan?
5). How and when will the service provider notify you of a breach of your data?
6). When the data is deleted where does it go?

Agencies should review the Terms of Service (TOS) for the online file storage service provider prior to the approval of use of any online file storage service as these constitute a binding agreement between the agency and the service provider. It is also recommended that the agency consult their Deputy Attorney General (DAG) before executing such an agreement. Certain terms may preclude an agency from using a particular service. At a minimum, consider the following when reviewing the "Click-through" Terms of Service:

1). Will the data be stored in the United States?
2). Is an agency able to maintain control of and delete data when services are terminated?
3). Is the service provider expressly prohibited from using state records for any purpose other than providing services to the agency, such as "data mining"?
4). Assess for risk, critical terms that may be missing and for unacceptable terms in light of the intended use and type of records to be stored.

Discuss the following Terms of Service considerations with your DAG:

1). Do the terms provide that the agency agrees to waive the right to a jury trial?
2). Do the terms state that the agency agrees to indemnify the service provider?
3). Do the terms provide for jurisdiction and venue in, or applying the laws of, another state?

Prior to the use of any online file storage services, an agency should develop agency specific policies or guidelines that address business productivity, legal ramifications, public disclosure, records management and IT security concerns.

Select an appropriate online file storage service that meets the agency needs for sharing and storage of data but that also addresses the agency records management requirements.

Ensure that logging and monitoring tracks all add, change, delete, copy/sync activity for each file. Agency administrators should be able to review these logs.

Provide high availability infrastructure, all within the United States.

Educate the employees regarding the data classifications, the sharing of this data and the regulations, laws, rules and potential risks or financial loss of miss-use of agency data. Education of online file services use should also include:

1). The benefits versus risks of using online file storage services.
2). The services approved for agency use.
3). The types of agency records that can and cannot be stored on the file storage

service.

4). The employee's role and responsibilities as custodian of agency records and how this may differ from how they handle information as private individuals.
5). Recommend ways to configure and use the service to obtain expected benefits and how to avoid the risks from unauthorized data access or disclosure.
6). How to avoid the commingling of agency and personal data on online storage services, mobile devices, personal email systems, home computers, etc.
7). The risks to the state for misuse of misconfiguration of online storage services.

Employees must use only agency approved online file storage services and agency approved accounts on those services to share state/agency data or access them from other computers or mobile devices.

Employees are not allowed to use personal accounts, even on approved services, for state business.

Use shared folders not public folders, allowing authorized access to specific individuals or groups.

Usage and shared folder membership should be reviewed frequently and permissions should be reviewed and updated as needed.

If a record has been modified in the collaboration process, the agency should sync interim versions with the system of record if the service allows, since the modified record is no longer a "copy". The agency must ensure that the final or "original" version is stored back on the agencies system of record.

IV. PROCEDURE REFERENCE

Policy for online file sharing services are detailed in ITA Policy P4120 (Public Online File Storage Services)

Idaho Code §§ 9-337 through 9-350 – Idaho Public Records Law

Idaho Public Records Law Manual

Purchasing Rule 38.05.01.112 - PENDING

V. CONTACT INFORMATION

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

REVISION HISTORY

8/16/2016 – Revised to align with revisions to ITA Policy P4120 (Public Online File Storage Services); added Classification Level 4.

Established: December 18, 2014