Joint Records Management Advice and Information Technology Guidance

Issued: February 2019

Joint Office of the CIO/State Archives Records and Cloud Storage Guidelines

February 2019/Version 1
Security classification of this document: CAT1 – Public

Purpose

This Guidance builds upon and supersedes the *Electronic Records Management: Can Public Records be Stored in the Cloud* published by the Washington State Archives, 2018 and *Online File Storage Guidance* published by OCIO in 2014.

Scope

This is for unstructured data and records; for structured data see data and technology standards from

- Office of the Chief Information Officer (OCIO) (including 187.10 Metadata and 141.10 Securing IT Assets)

- State Auditor's Office (SAO) (Uniform Chart of Accounts)

This is not meant to supplant agency security assessments under OCIO 141.10 and other applicable standards. Agencies retain responsibility for securing their records and systems.

Statement:

Agencies can store and manage public records appropriately in the cloud, provided they know the risks, sustain collaboration between teams with responsibilities for management, and observe minimum requirements.

As required by state law, the State Archives requires agencies must:

1. Retain legal custody of records and information;
2. Maintain record and information controls over cloud storage;
3. Specify provider recordkeeping responsibilities in contracts;
4. Plan in the contract for future migration, transfer, and destruction of the records.

Records in the cloud must:

1. Retain accountability, integrity, compliance, authenticity, and reliability;
2. Be available, searchable, and retrievable;
3. Be protected from unauthorized deletion;
4. Be retained for the minimum retention period;
5. Be destroyed/transferred in accordance with the appropriate records retention schedule.

Minimum requirements for compliance:

1. **Agency Retains Legal Custody** – Agencies must not transfer legal ownership of the public records to the cloud service provider or other non-government entity. This satisfies the “legal custody” requirements in WAC 434-615-020.
2. **Agency Controls Access** – Agencies need to control who has access to their public records while they are stored with the third-party cloud service provider. This satisfies the “physical custody” requirements in WAC 434-615-020.
3. **Agency Complies with IT Security mandates** – Agencies must ensure that the cloud service provider, applications, and data comply with applicable standards, such as the OCIO IT Security Standards 141.10, city, county, or agency policies.

Teams that should collaborate on cloud records management:

- Records and Information Management
- Public Records
- Information Technology
- Risk Management
- Information/Data Governance
- Security
- Contracts and legal counsel
- Privacy

Risks:

The creation, storage, and maintenance of a record in the cloud provides a variety of business and legal risks when asserting the accuracy and validity of records. Planning for the cloud must consider these risks and staff should conduct a risk and record assessment before entering into any agreement with a cloud vendor. This is important because it is often difficult to conduct on-site assessments or investigations of a cloud provider or work backwards to correct human behaviors in record creation and storage.

Office of the Secretary of State
Washington State Archives

WA - Office of the Chief Information Officer

Joint Records Management Advice and Information Technology Guidance

Issued: February 2019

Recordkeeping Considerations for the Cloud

1. Legal compliance
2. Unauthorized access to records
3. Loss of access to records
4. Limit customization of the cloud
5. Establish record controls in the cloud
6. Do Your Regular Records Inventory
7. Vendor going out of business
8. Have an exit strategy
9. Establish a Continuity Plan in the event of disaster
10. The evidential value of records may be damaged
11. The cloud vendor disposes of digital records without the approval of the agency
12. Other jurisdictions' laws may affect obligations for retention and management

1.) Legal Compliance

Sending or storing records outside of Washington State may require records to conform to local record and public disclosure laws. It is important to understand where the record will be stored because local jurisdictions may require additional disclosure burdens for the agency. For example, it is possible for the agency to need to disclose records held within another state according to their public disclosure laws.

Before entering into agreements with cloud computing providers, agencies should investigate any legislative impediments to the transfer or storage of records outside the physical boundaries of the State. There is a risk that when cloud computing providers send records outside the geographic boundaries of Washington State they might fail to comply with records management RCW and WAC requirements.

2.) Unauthorized Access to Records

Security should be a primary concern when protecting records in the cloud. It is highly recommended to follow OCIO security standards for cloud computing.

The disclosure and processing of data and information by third-party processors for data mining or other marketing efforts should be avoided. Cloud vendors should be required to obtain prior approval and written permission before engaging in the use of third-party processors to interact with records and information stored in the cloud to prevent the unauthorized disclosure of personal information, protected health information, proprietary information, and controlled information.

3.) Loss of Access to Records

As cloud computing services are provided over the internet, it is more likely that there may be some periods of disruption to service where records are unavailable. For business activities where continuous access is imperative, the impact of a loss of access may be severe. Cloud storage may not be appropriate in these situations. Poor record controls may make it difficult to distinguish an official record from duplicate or near-duplicate records. Using the cloud requires serious consideration of proper records control to mitigate these risks.

4.) Limit Customization of the Cloud

As with all electronic information systems, it is best practice to limit customization. Customizations generally lead to loss of service as personnel change or systems need to be upgraded. Generally, use standard approaches with repeatable activities to safeguard the system and improve user acceptance. Avoiding customization does not mean for the agency to allow for the uncontrolled design of the cloud environment, rather it means it should be planned according to the business activities along with the impact upon other business activities.

5.) Establish Record Controls in the Cloud

Information lifecycle management is essential in the cloud environment. Records should not be introduced into the cloud without specific controls in place. It is recommended that records and information management processes be implemented to build accountability, integrity, compliance, availability, retention, disposition, and transparency. This means integration of file plans, records metadata standards, records naming standards, and other record controls as necessary. Automation should be encouraged and used if available. Utilization of records metadata will provide the ability to create records in a controlled and predictable manner, place specific retention standards on the record, and allow for disposition in a controlled and defensible manner. Additionally, metadata, if enabled, would allow for version control of records and assist in retrieval of records during public records disclosure activities.

Controls to prevent additions, modifications, or deletions of records by unauthorized parties will help demonstrate the authenticity, maintain the chain of custody, and help protect the evidentiary value of the record (WAC 434-662-060).

6.) Do Your Regular Records Inventory

Business and service components change over time, as do our needs from electronic storage systems. Inventory and assessment allows the agency to adjust its cloud needs based on empirical evidence gathered in the process. The assessment should map data inputs and outputs, establish event triggers, understand the nature of records, and determine if the cloud is being utilized in the most efficient manner. Assessments should also validate access, security, and control. Assessments should be conducted using specific auditing standards such as ISO 15489-1. *Refer to guidance from the State Archives, Privacy Office, and OCIO*

7.) Vendor Going Out of Business

Vendors may go out of business during the contract period. The vendor could also be taken over by another company. The new company may not honor the contract or provide the agreed level of service. While this is possible due to the nature of constant changes in IT, it is rare. Migration planning can assist with migration from one vendor to another, but it must be assumed service disruption could result.

8.) Have an Exit Strategy

Before signing a contract with a vendor for the cloud, the agency should plan for migration, data portability, and future usability of records from the cloud. Portability planning would determine acceptable media formats for records in the cloud. Formats should be non-proprietary and use open-architecture to improve the chance of migration and reduce the threat of records loss. It will be important to establish emergency protocols and storage locations should the vendor go out of business. Rapid transfer of records may not be possible. Essential records, those needed for continuing of agency functions, need to be identified and migrated first.

Vendors may conduct upgrades to hardware and/or software which is not compatible with agency systems. Contracts should specifically speak to this risk and outline notification procedures for the agency to assess and plan for any migration requirements needed during an upgrade. Not doing so means there is a risk of data loss or of records not being readable upon return.

9.) Establish a Continuity Plan in the Event of Disaster

Cloud vendors have similar risks to disasters as any agency. These risks should be mitigated through proper continuity planning and risk management. It is important to identify all essential records in the cloud and categorize them according to the specific timeline needs of the agency after a disaster in the cloud. Understand the vendor’s backup plans and locations. If the vendor only has one storage location and it's in a high risk zone for disaster, consider a different vendor. Most cloud vendor’s today stage storage sites in multiple locations with built-in redundancies to account for disaster. Cyber attacks should also be addressed in continuity planning.

10.) The Evidentiary Value of Records May be Damaged

Agency cloud records need to be managed in such a way that they can be shown to be authentic (free from tampering) and reliable.

11.) The Cloud Vendor Disposes of Digital Records without the Approval of the Agency

At no time does a vendor have the authority to dispose of records in the cloud without prior written authorization. If authorized in a contract, the contract must specify appropriate methods for disposal by the vendor based on security classifications. The vendor must provide evidence of disposition activities through audit records or systems event history logs.

It is common for vendors to replicate records for multiple backups by sending copies to storage sites at different locations. This can mean that time-expired records are not properly deleted from every server held at every site. This poses a serious risk where there is a specific requirement for information to be destroyed, such as records containing personal or confidential information or records exceeding retention standards. It is important to outline in the contract that once disposition activities are initiated by the agency, all record copies are destroyed as a result of the action, no matter the location.

12.) Other jurisdictions' laws may affect obligations for retention and management

Cloud services very often involve the storage of personal information outside the US, or access to it from outside the US. Though Washington law does not currently address this question, careful inquiries should be made before entering into cloud services arrangements involving personal information storage in jurisdictions where control of data cannot be assured.

When collaborating with other jurisdictions such as the Province of British Columbia, the State of Oregon, or certain federal agencies, there may well be specific records retention or storage requirements that apply – and that differ from the requirements in Washington State. For example, BC provincial agencies are advised that BC law prohibits access to or disclosure of personal information outside Canada. Agencies should consider how, where and by whom records of such a collaboration will be stored, shared, and disposed of.

Records and Information Management Cloud Readiness Checklist

This is not an exhaustive list. It is adapted from the Washington State Department of Health (DOH) Records and Information Readiness Process for onboarding into Enterprise Content Management Systems. Additional needs may be identified.

1. The agency owns records placed in the cloud.
   - Ensure agency complies with Custody of Public Records (434-615 WAC)
   - Ensure agency complies with records requirement found in Preservation and Destruction of Public Records (40.14 RCW)
   - Ensure agency complies with electronic records requirements found in Preservation of Electronic Records (434-662 WAC)
2. Records in the cloud must be authentic, accurate, and trusted
   - Map records to locations - see e.g. Privacy Office Data Mapping Checklist
   - Determine the adequacy of cloud vendor’s audit logs and system logs
   - Determine cloud security
   - Be aware of third party processors
3. Records in the cloud should be complete and unaltered
   - Consider the impact of altered records
   - Consider the format of records created or stored for migration

4. Records in the cloud should be secured from unauthorized access, alteration, and deletion
   - Consider who has access to, and use of, agency records
   - Assess the provider viability
   - Consider the risk of incomplete and unauthorized destruction of records
5. Records in the cloud should be retrievable and readable
   - Consider the readability and usability of records created in the cloud
   - Ensure records can be retrieved
   - Evaluate the impact of corrupted records
   - Establish controlled languages to allow for accurate creation, storage, and retrieval of records
   - Consider the metadata requirements needed to identify and retrieve records
   - Consider establishing file and record naming standards
6. Records in the cloud should be related to other relevant records
   - Consider the need for metadata maintenance and management
   - Understand how records in the cloud relate to other records stored at the agency
   - Apply records classification through the establishment of file plans

Glossary of Terms

Cloud Service / Cloud Service provider

Cloud computing is defined by the National Institute of Standards and Technology (NIST) as:

“a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Mobile Device

Any hand-portable device capable of text, voice, email, instant messaging (“IM”), photo messaging or other types of data communication. This policy is not meant to apply to: cars, boats, airplanes, laptop computers, desktop computers, unpiloted aerial vehicles (drones), GPS receivers, radios.

Online File Storage Service

A file hosting service, cloud storage service, or online file storage provider that hosts user files via the Internet. Users can upload files that can be accessed over the internet from other computers and mobile devices, by the same user or other designated users. Examples include but are not limited to: Box.com, OneDrive for Business.

Public Records Request

A request under chapter RCW 42.56 for the inspection and copying of a public record. An agency is prohibited from destroying or erasing a record, even if it is about to be lawfully destroyed under a retention schedule, if a public records request has been made for the record. Agencies are required to retain potentially responsive records until the public record request is resolved. Where notified of a public records request, employees must, with regard to potentially responsive records, suspend the destruction of records, conduct a reasonable search for records, and gather or segregate records so they may be reviewed and, if necessary, produced. Like other records, records created or stored with an online file storage service are subject to the requirements of the Public Records Act.

Legal Hold

A legal hold is a communication issued as a result of current or anticipated litigation, public records request, audit, government investigation or other such matter that suspends the normal disposition or processing of records. The specific communication to agency business or IT organizations may also be called a "hold," "preservation order," "suspension order," "freeze notice," "hold order," or "hold notice".

Further Reference:

- Securing Information Technology Assets (141)
- Securing Information Technology Assets Standards (141.10)
- Media Handling and Data Disposal Best Practices (141.10.10)
- Open Data Planning (187)
- Metadata Standard (187.10)
- Geospatial Data Management Policy (160.00)
- Records Retention Schedules – State Agencies (Washington State Archives)
- Records Retention Schedules – Local Governments (Washington State Archives)
- Public Records Act Definitions (RCW 42.56.010)
- Preservation and Destruction of Public Records (chapter 40.14 RCW)
- Custody of Public Records (chapter 434-615 WAC)
- Standards for the Accuracy, Durability, and Permanence of Public Records (chapter 434-660 WAC)
- Preservation of Electronic Public Records (chapter 434-662 WAC)