New Jersey Division of Revenue and Enterprise Services

Records Management Guidelines for Cloud-based Records Storage

11/2020

Introduction

As a response to the COVID-19 pandemic, as well as in the development of strategies for new operating models, government agencies are promoting remote work programs. To foster remote work capabilities, agencies are turning increasingly to the use of Cloud-based computing systems/services that enable mobile work forces to access government systems outside of traditional office settings.[1] As these use cases unfold, agencies are generating and storing increasing volumes of public records on Cloud platforms. Therefore, in addition to complying with policies/procedures set forth by their legal, technology and information security authorities, agencies employing Cloud-based systems/services must plan to manage these records in accordance with the State's public records management requirements.[2]

Whether stored in the Cloud or in agency-owned storage systems, public records are evidence of taxes paid, services rendered, decisions made and obligations met. These records are crucial to the organization of our society and essential to the daily operation(s) of government. Additionally, the value of some records endure beyond their active use, because they provide unique evidence of significant actions and transactions that have affected the public. Records may be created in any format including electronic mail and documents, text files, chats, social media posts, data bases, images, graphics/drawings, audio-video recordings, etc. and stored in any format – hard copy or electronic. Given the significance and value of public records, State Law (N.J.S.A. 47:3 et seq.) specifies that they be maintained, preserved and disposed of in accordance with specific requirements.

This document sets forth basic guidelines for building records management requirements into Cloud facilities that house public records. The presentation is narrow in scope and deals primarily with records management-related considerations. Agency records and information management professionals may wish to use these guidelines when developing or managing contractual engagements with Cloud system/service providers.

[1] The State-wide Information Security Manual, page 162, provides a definition of Cloud computing, which is based on NIST's original overview of the concept.

[2] New Jersey State agencies must also comply with policies and procedures set forth by the Office of Information Technology (https://www.state.nj.us/it/services/governance.shtml) and NJ Office of Homeland Security and Preparedness.

It is important to note that the development, maintenance and/or procurement of Cloud-based systems/services is a complex process involving multiple disciplines. Therefore, when seeking to apply these guidelines, records and information management professionals should work across disciplinary lines. Several key disciplines with a stake in this practice space include:

- Procurement professionals
- Internal auditors
- Legal advisors
- Information technology staff (for example, Chief Technology and Chief Information Officers)
- Information/internal security staff
- Agency managers
- Records management liaisons
- Risk management professionals

Key Contacts

The contact for the records management topics covered below is the New Jersey Division of Revenue and Enterprise Services' Records Management Services Unit (RMS): 609-777-1020 or 609-292-8711. Guidance on preservation of permanent and historical records can be obtained from the State Archives: 609-633-8304 or 609-292-6260

Guidelines

1. **Make it clear to the contractor that agency records stored in the Cloud facility are public records and, as such, belong to the agency.**

   Following is sample of language that articulates this requirement. Consult with your procurement team and legal advisors about the use of ownership provisions in notifications to vendors, RFPs and contracts.

   > Records created, received, retained, retrieved or transmitted under the terms of this contract may constitute public records as defined by N.J.S.A. 47.3-16, and are legal property of <agency name>. The vendor(s) named in this contract must agree to administer and dispose of such records in compliance with the State's public records laws and associated administrative rules.
   >
   > <Agency> has identified the following as public records under this contract, subject to the above-cited provision:
   >
   > <List all public records by series title and number as set forth in the agency's record retention schedule approved by the State Records Committee. **(See approved New Jersey State, County and Local records retention schedules.)>

Although <agency name> has used its best efforts to identify all records which qualify as public records under this contract, <agency name> reserves the right to amend the above list from time to time as warranted.

2. **Ensure that Cloud storage facilities allow the agency to classify stored records in accordance with approved State/County/Local records retention schedules.**

   This can be somewhat complicated. Cloud facilities store a wide variety of records using various file formats including electronic mail, electronic documents (for instance, word processing and spreadsheet formats), presentations, social media posts, chats/text messages, audio-visual sessions and databases. In many cases, a direct mapping of Cloud storage content to records series will prove challenging. This has been the case historically for electronic mail and databases.

   For concepts on electronic mail retention scheduling see the State Records Manual and the Municipal General Schedule M100000/0013, item 0800-0000 - 0800-0001. For additional concepts on how to approach retention scheduling of electronic mail, databases and unstructured content see the State General Schedule G100000/011, items 2200-0000 – 2216-0000. Contact RMS for guidance on electronic records management.

3. **Require the use of controls that prevent unauthorized access, manipulation, distribution, defacement and/or destruction of records stored in the Cloud facility.**

   These controls center on the information security regime(s) employed by the Cloud service provider and include elements like user identification and log-in protocols with dual-factor authentication, role-based access control, data encryption, network and application firewalls, anti-malware software, intrusion detection/prevention processes, system monitoring, security event escalation/management and more.

   Typically, your information technology, information security and information disclosure officers will be most knowledgeable in this area and will be able to articulate the specific requirements. For instance, your agency may seek to comply with general information security frameworks such as those set forth by the International Standards Organization (ISO 27001/27002) and National Institute of Standards and Technology (NIST 800-53). Your agency may also be subject to specific content-oriented regimes such as those associated with the Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) requirements and Internal Revenue Service SafeGuards program.

   Information and records managers may wish to focus in particular on two key compliance regimes for Cloud system/service providers: System and Organizational (SOC) 2 reports from the American Institute of Certified Public Accountants; and the Federal Risk and Authorization Management Program (FedRAMP), which incorporates NIST 800-53 security controls.

The State of New Jersey's State Information Security Manual is an excellent source of information on security controls for the Cloud and for information systems in general. The Manual sets forth information security requirements for New Jersey's Executive Branch and has a section dedicated to Cloud security and it references compliance regimes and benchmarks such as FedRAMP and Cloud Security Alliance's Cloud Controls Matrix.

4. **Be aware of storage location restrictions.**

   In many cases there will be restrictions about where Cloud-based records may be stored. Commonly, there are requirements to ensure that records **are not** stored in foreign jurisdictions and there may also be concerns about being subject to the laws of other states. Check with your legal advisors for guidance on location restrictions.

5. **Provide for life-cycle management of records stored in the Cloud – that is, management of the records from receipt, creation, storage, use and dissemination to authorized disposition (destruction or transfer to another records repository).**

   Cloud-based records must be available and readable throughout their life cycles. In this regard, life-cycle management should include the preservation of meta-data that documents the content, structure (format) and context of stored records. The National Archives and Records Services' (NARA) guidance on metadata for the transfer of permanent electronic records illustrates the type of meta-data that could also be specified for general Cloud-based storage. NARA's minimum elements are: identifier or file name; record ID or unique record identifier assigned by the agency; title or name given to the record; description of the contents of the file/record; creator of the record; creation date; and rights/restrictions – any access/use restrictions associated with privacy and confidentiality and/or intellectual ownership.

6. **Prohibit the contractor from deleting/destroying Cloud-based records unless the agency specifically directs the action.**

   Before directing a records destruction action, the agency must obtain approval pursuant to State law (N.J.S.A. 47:3 et seq.). Contact RMS for guidance on authorized records destruction.

   For authorized destruction actions, require the contractor to securely delete/destroy all records from the Cloud platform, including back-up records. This involves obliterating records or otherwise rendering them permanently inaccessible and unreadable.

   Note that while the guidance in this area focuses on preventing the unauthorized deletion/destruction of public records, the agency should endeavor to apply records

retention schedules to Cloud-based records and regularly dispose of records that are eligible for disposition. Failure to do so leads to over-retention and exposes the agency to risks of increased storage costs and costs associated with retrieving and producing records that might otherwise have been disposed of legally.

7. **Institute data/content management protections.**

   These protections complement life-cycle records management and retention/disposition controls. They include: back-up/restore services to guard against the loss of records due to system malfunctions and/or errors; business continuity processes that assure continued operations following outages that affect storage facilities; and disaster recovery regimes that allow for full recovery of facilities and data/content affected by disruptive events within specified timeframes.

8. **To the maximum extent possible, use non-proprietary and/or widely used (de-facto standard) file formats for Cloud records storage.**

   Seek to employ file formats that are non-proprietary or widely used and documented. This will facilitate the transfer of records from one computer platform to another with minimal programming effort. It will also provide for flexibility when it becomes necessary to switch Cloud service providers and/or when the agency wishes to transfer records to alternate repositories such as data warehouses or long-term research facilities. Further, use of non-proprietary and widely used/documented formats bolsters records preservation and facilitates migration of records from one format to another as technologies change.

   The National Archives and Records Services' (NARA) format guidance (Appendix A: Tables of File Formats) for the transfer of permanent electronic records illustrates some of the file types that could also be specified for general Cloud-based storage. The preferred and acceptable formats cover a wide range of record types including computer aided design files, structured data, email, scanned text (document) images, digital video, audio and moving images, textual data and web records.

9. **Employ documented change management for Cloud-based records. Require contractors to document any changes in format or programming that affect the access and use of stored records.**

   The availability of change documentation supports the ability of agencies to transfer records from one platform to another and/or one format to another, thereby facilitating the on-going accessibility, integrity and reliability of records over time. Documented change management is likely to be a key consideration in cases where the contractor is providing turn-key applications and databases to the agency – for example; Software as a Service

applications/data associated with customer relationship management, case management, accounting, payment processing, etc.

10. Specify records transfer requirements for contract-exit processes and other operational purposes.

Over the course of time, the agency may need to transition to new a Cloud contractor and this will likely involve switching to a different Cloud storage platform (**contract exit**). Also, the agency may need to routinely transfer records from the Cloud platform to other storage locations owned by the agency or other firms/organizations. To address these requirements specify the format in which the records are to be transferred (a format that is compatible with the agency's system and/or new Cloud platform) and set timeframes for the transfers. In the case of exit processes, require the contractor to securely delete/destroy all records from their platform, including back-up records, after verifying that the transfer is complete and successful. As noted previously, secure deletion/destruction involves obliterating records or otherwise rendering them permanently inaccessible and unreadable.

11. Ensure that records are retrievable and reproducible in response to Open Public Records Act (OPRA) requests, audits, subpoenas and investigations.

The agency must be able to find Cloud-based records responsive to OPRA, subpoena, audit and investigative requests in an expeditious fashion and be able to extract, preserve and provide the records to authorized parties. Accordingly, the Cloud storage platform must include searching features that enable the agency to locate request-relevant records (discovery). The platform must also include functions that allow for **litigation or legal holds.** Litigation/legal hold functions prevent relevant records from being deleted/destroyed prematurely. Moreover, the Cloud platform must enable the agency to extract/segregate, copy and transfer records to authorized requesting parties in readable formats.

For more information on OPRA, see the State's Reference Material. For a general discussion on litigation holds, discovery and related concerns, see the State Records Manual, pages 65-67. The Electronic Discovery Reference Model (EDRM) provides a useful framework for understanding the steps involved in conducting discovery processes, including litigation hold actions.[3]

[3] Hill provides an overview of the EDRM. See Hill, D. (2014). Investigations: Overview of the steps of the electronic discovery reference model. In O'Hanley, R. & Tiller, J. (Eds.), *Information security management handbook* (6th Ed., pp. 291-300). Boca Raton, Fl.: Auerbach Publications.

12. Participate in planning for service levels with your information technology and procurement teams.

Service levels are the functional and performance outcomes that agencies seek to obtain from a Cloud computing contractor. In this regard, service levels should be used to articulate, in actionable contract terms, the records management considerations covered by these guidelines.

Following are examples of service levels that relate to the records management considerations covered in items 1-11 above, along with other common and potentially useful service levels pertaining to service availability, performance and breach protocols. It is important to note that ***DORES is providing these examples for illustrative purposes only***. Work with your procurement, information security, information technology and legal advisors when developing formal service levels. The examples **do not** constitute an exhaustive list of Cloud service levels.

Examples of Records Management-related and Other Common Cloud Service Levels
The contractor shall provide a system/service that meets the following service levels:

- 99.99% system availability (uptime) between the hours of <start hour> am and <end hour> pm Monday through Friday.
- 99.99 uptime Saturday – Sunday, from <start hour> a.m. to <end hour> p.m.
- All unexpected downtime during the above hours must be reported immediately to <agency contact name and contact information> .
- Scheduled maintenance and down time must be performed during off hours – that is, hours that fall outside of the production time frames cited above and contractor must give at least one week's notice of these maintenance events to <agency contact name and contact information>.
- Response time to end user entries or records access requests shall not exceed an average of <list time segment – for example, in milliseconds or seconds>. For purposes of this engagement, response time means the elapsed time from receipt of a client request at the contractor's server(s) through to response received by <agency name>'s network.
- Facilities must ensure the logical and physical segregation of <agency name>'s data and records from other organizations' data and records and provide for the transfer of same to the <agency name>'s <list alternate storage facilities owned by or affiliated with the agency>, in whole or in part, upon demand. (****Note:** Procurement, budgetary or other constraints may require the agency to place its data/records in shared storage spaces in the Cloud instead of segregated spaces as envisioned in this service level. For guidance on operating in shared multi-tenant environments, see the State-wide Information Security Manual, page 167.)
- All data and records stored in the Cloud facility must be within the 48 contiguous

United States of America; contractor must disclose the precise location(s) of <agency names>'s State data/records.

- Cloud storage facility must allow <agency name> to classify stored records in accordance with specific record series found in <list approved records retention schedules that apply to the agency>.
- Contractor's system must enable tracking of all data and records in the Cloud facility from creation/receipt through to authorized deletion/destruction or transfer (**life-cycle management**) and include logs that show actions taken on data and records throughout their life cycles**.** Systems logs must be made available to <agency name> upon request.
- Contractor must ensure metadata is captured and made accessible for all data and records. The minimum metadata requirements are <list the required metadata elements>.
- Contractor may not delete/destroy any data/records without the express authorization of the agency's < list name and contact information for the agency's records management representative>. When <agency name> authorizes records deletion/destruction, contractor must securely delete/destroy the targeted records by obliterating them or otherwise rendering them permanently inaccessible and unreadable and provide written confirmation of the deletion/destruction.
- Contractor may not modify or transfer any records without <agency name>'s consent.
- Contractor must document and execute back-up and restoration plans for all data/records stored pursuant to this contract.
- Contractor's systems must include redundancy and fail-over capabilities that assure continued compliance with the previously stated uptime service levels in the event of a system or facility failure (operational continuity).
- Contractor must implement and maintain a disaster recovery program for all facilities that store <agency name>'s records, which ensures return to operation in 24 hours following a disaster, with the data recovery point at no more than <list the time frame – in hours, calendar days, business days, etc.>.
- Contractor's Cloud system/services must provide functions that allow <agency name> to implement electronic discovery in response to OPRA requests, audits, subpoenas and investigations. The required steps are identification, preservation, collection, processing, review, analysis, production and presentation of targeted records.[4]
- Cloud facility must use/support de-facto standard and non-proprietary file formats. At a minimum, the platform must use/support the following file formats: <list the file formats>.
- Cloud facility must achieve compliance with <list the required compliance regime(s) – for example, State-wide Information Security Manual, SOC 2, FedRAMP, SafeGuards, etc.> and maintain said compliance for the length of the contractual engagement.

[4] These are the core action steps within the EDRM mentioned previously.

- Contractor must have a documented information breach protocol to be used in the event of theft or unauthorized access, transfer, destruction or defacement of public records classified as sensitive, confidential or private.
- Contractor must provide for the transfer of the following records to <list the computing facilities to which the records are to be transferred>: <list records to be transferred>. Said transfer shall occur <list the timetable(s) for the transfer(s)>.
- Upon contract termination, per the instructions of <agency name>, contractor must transfer all data/records residing on its platform to a designated storage location in a file format(s) specified by <agency name>. Following the complete and successful transfer of all data/records, contractor must securely delete/destroy the targeted records from its platform, including all back-up data/records, by obliterating them or otherwise rendering them permanently inaccessible and unreadable. Contractor must provide written confirmation of the deletion/destruction.

Additional Reading, Examples of Public Sector Records Management Guidelines for Cloud Computing Systems

NARA Bulletin 2010-05, Guidance on Managing Records in Cloud Computing Environments

State of Kentucky, Cloud Computing: Implications and Guidelines for Records Management in Kentucky State Government

State of North Carolina, Best Practices for Cloud Computing

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

State of Wisconsin, Public Records Board Guidance on the Use of Contractors for Records Management Services Managing Records in Cloud Computing Environments