NEW JERSEY RECORDS MANUAL

New Jersey Department of the Treasury

Division of Revenue and Enterprise Services

Contents

Chapter 1

Introduction

The purpose of this manual is to introduce public agencies to the methods available for controlling public records entrusted to their care, with emphasis on the tools needed to solve record- keeping problems, increase efficiency, improve services and save money.

This manual applies to all public agencies in New Jersey. It provides general guidance and links to regulations based on State law (including records management standards), forms, online services and general records retention schedules. It blends sections that cover traditional records management topics with sections that address various aspects of electronic records management.

The sections on traditional records management – covering topics such as records retention and disposition, records centers, files and forms management, are largely descriptive and designed to sharpen the reader's understanding of basic records management techniques. Collectively, the techniques set basic benchmarks for implementing records management programs in various organizational settings. The Division encourages agencies to exceed these benchmarks whenever possible, while staying in compliance with the New Jersey's legal framework for records management.

The sections on electronic records management include descriptive elements and discussions on best practices in this rapidly evolving arena. Here again, the Division encourages agencies to exceed the practice levels covered by the manual, while staying in compliance with the New Jersey's legal framework for records management.

The Division also encourages agencies to think beyond the segmented format of the manual and view all records as assets that are amenable to consolidation, use and management within integrated frameworks – frameworks that leverage information (including meta-data), processes, governance, policies and procedures for maximum sustained effectiveness, efficiency, accountability and responsiveness.

Notwithstanding the preceding statements, public agencies are not required to implement all of the programs described in this document. Provided they meet mandated standards and legal requirements referenced herein, public agencies may employ techniques that are compatible with their organizational cultures and resources levels. When developing records management programs, public agencies need to consider costs/benefits, available budgetary and staffing resources, and the value of the records involved.

By using appropriate records management techniques on a consistent basis, government agencies will realize demonstrable benefits. They will avoid the costs of unnecessary space, equipment, supplies and labor for record-keeping and processing operations. Sound records management practices also set the stage for service improvements and innovations.

Agencies are encouraged to contact the Division for further guidance on records management. The Division welcomes feedback on the usefulness of the manual itself. To this end, the Division offers an on-line forum for comments, feedback on new techniques for addressing records management issues, and collaborative dialogue on problem-solving and requests for assistance. To interact with the Division, click on the RMS Interact icon, which appears throughout this document.

Background

New Jersey's Records Management Services Program (RMS)

Operating as an integral unit of the Division of Revenue and Enterprise Services (DORES) of the Department of the Treasury, the State's records management program consists of three distinct areas of responsibility. All program operations are located within the State Records Center, 2300 Stuyvesant Avenue, Trenton.

Records and Forms Analysis

1. Assists local agencies and authorities in conducting records inventories,
2. Appraises records of state, county and municipal governments, and schedules the records for retention, transfer and disposition through the auspices of the State Records Committee,
3. Offers advice in records management, files management, office automation, vital records programs, and disaster prevention,
4. Participates in records disaster recovery efforts through records identification,
5. Provides advice about forms analysis and design,
6. Processes records disposal requests, and
7. Coordinates with the State Archives, assisting in efforts aimed at preserving the State's documentary heritage.

Records Storage

1. Provides centralized storage of semi-active records for state agencies and authorities,
2. Provides records retrieval services for authorized state officials,
3. Advises all public sector agencies about semi-active records storage options, and
4. Administers third party records center services on behalf of other state agencies.

Image Processing

1. Provides systems consultations and assists in estimating cost for image processing projects (microfilm and digital imaging),
2. Conducts and/or coordinates selected projects for state, county and municipal agencies on a charge-back basis,
3. Assists public agencies in managing microfilm and digital image records systems, and
4. Monitors for compliance with standards relating to image processing

Public Records Defined

It is important to develop and maintain records management programs because of the nature and value of public records.

Any information that a public agency generates or receives in the transaction of its official duties is a public record. This is true regardless of the medium used to store the information – e.g., paper, microfilm, magnetic disk, etc., and includes duplicates or copies.

The term "public" can have two basic meanings:

1. Ownership

A record is public when it is evidence of activities of an operating unit of government or an agent of government, which receives a substantial contribution of tax dollars to conduct its activities. In this very important sense, public records are assets owned by the citizenry from whom taxes and other payments are collected in support of governmental programs.

A record is private when it is evidence of activities of an organization that does not receive any substantial contribution of tax dollars to conduct those activities.

2. Access

Agencies may allow unrestricted access to records because of open public records considerations. Under other circumstances, an agency may restrict access to records because of considerations of privacy, confidentiality or security.

Accessibility is not a factor in determining whether a record is publicly or privately owned. For instance, classified military records concerning the national defense are public records with a high degree of confidentiality, and consequently are not freely accessible.

For the purposes of this manual, whenever the term public record is used, it signifies ownership of public records, which are public assets. The discussion below amplifies the value of public records as assets that require management.

Value of Public Records

Public records are evidence of taxes paid, services rendered and obligations met. These records are crucial to the organization of our society and essential to the daily operation of government. Additionally, the value of some records endures beyond their active use, because they provide unique evidence of significant actions and transactions that have affected the public.

Legal Framework

Public records are public property and are held in trust for citizens. Accordingly, public officials must ensure that records are protected from unauthorized alteration, defacement, transfer or destruction. This is accomplished through compliance with New Jersey's general public records law (N.J.S.A. 47), the State's records management statute (N.J.S.A 47:3-15 et seq.), and administrative rules under N.J.A.C. Title 15:3 et seq. referenced throughout the manual, which enact the standards and procedures mandated by the law. Also, there may be agency-specific statutes and administrative rules that impact a public agency's records management responsibilities.

RMS will assist public agencies in addressing issues and questions that arise from application of the legal framework to records management programs and initiatives.

Chapter 2

Records Retention and Disposition

This section describes the key processes associated with records retention and disposition. Organized and controlled retention and disposition are keys to a successful records management program.

The procedural elements covered in this section relate most directly to records stored on hard copy media (e.g., paper and microfilm); however, as will be discussed in the Electronic Records, basic retention and disposition considerations apply to automated systems as well.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq. and 3-2 et seq. (Online Source)

Records Retention Scheduling Process

Following are the steps agencies take in constructing records retention schedules.

Records Inventory

Record holdings must be inventoried before appropriate controls can be instituted. An inventory is a complete listing of records by record series, together with necessary descriptions and supporting information. A record series is a group of identical or related records that is normally filed together, and that can be evaluated as a unit to determine how long they should be maintained. Examples of record series can be found in general retention schedules for State and local agencies.

A key to an effective and efficient inventory process is the application of the records series concept.

Consider a common record series like "correspondence." For records inventory purposes, there is no need to know who generated or received a particular letter or memorandum, nor what subject matter was discussed. This is equally true for any other examples of record series held by government offices, such as purchase orders, travel vouchers, cancelled checks, personnel records, etc. In all cases, the records inventory is not concerned with the particular details of content.

The inventory process focuses on the general function and overall content of records. It also provides for the identification of record medium (e.g., paper, magnetic tape and magnetic disk), filing method, reference rate, current volume and annual accumulation. All of this information is part of the records series inventory form.

Inventory data is not used exclusively for retention scheduling. Such information becomes crucial to other aspects of managing records:

1. Accumulation rates are a factor in deciding whether to convert a record series to another medium such as digital images.
2. Filing methods may illustrate problems with retrieval.
3. Frequency of use -- i.e., reference rates, will determine when to place records in inactive storage.

RMS analysts conduct records inventories for public agencies on a periodic basis and are available to aid them in reviewing their record holdings. In this connection, RMS provides planning and orientation sessions for agency staff, which summarize inventory techniques, procedures and benefits.

Records Retention Scheduling

After records are inventoried, they are placed on records retention schedules. Every record series on a schedule is:

- Assigned an item number;
- Given a title, a brief description of function and contents, including appropriate form numbers or applicable statutory references;
- Given a retention period i.e., a specification of the length of time the record must be maintained, and in some cases, how long it may be kept in semi-current storage in a records storage center; and
- Given a final disposition i.e., if the record will be destroyed, held permanently by the office of origin, or placed in archives.

The scheduling process is ongoing and involves close cooperation between RMS and the involved public officials. Many agencies have designated officials responsible for the records management of their organizations. These officials work very closely with RMS analysts.

Retention schedules include specific schedules that list record series unique to a particular, agency or office within an agency, and general records schedule that contain records that are common to most offices -- e.g., correspondence, invoices, personnel files, etc.

As new records and forms are created or received, RMS analysts and appropriate agency staff should update retention schedules at the same time. For many agencies, records schedules are often established or amended when agencies begin using a new records storage center or request authorization for records disposal from the division. RMS is continuously appraising public records and revising retention schedules.

Schedules are also used as evaluation tools in files management, and image processing system studies as well as in general office efficiency reviews.

Schedule Approval

Once a new or changed record series has been identified, RMS evaluates the record series in terms of:

1. Legal and fiscal requirements -- relevant statutory laws, regulations, statutes of limitation, administrative and court decisions, and audit requirements;
2. Administrative requirements -- past precedents, usefulness in office management, and common sense; and
3. Historical requirements -- evidence of significant actions or transactions affecting the public and worthy of permanent preservation (done in conjunction with the State Archives).

In cooperation with the involved agency, RMS makes preliminary determinations regarding retention periods based on these requirements.

Often, as part of the schedule review process, county and municipal professional associations such as the Constitutional Officers Association of New Jersey and Municipal Clerks Association, provide additional, invaluable advice.

Once RMS and the agency agree on a retention schedule, RMS submits it to the State Records Committee. This body has final authority on matters involving public records, regardless of the record's medium. The State Records Committee reviews proposed retention schedules at regularly scheduled meetings. RMS attends the meetings along with representatives from public agencies.

State Records Committee approval ensures that retention periods satisfy all legal, fiscal, administrative and historical obligations, thereby protecting the public interest. The committee approves a schedule as presented, recommends changes and approves with changes, or withholds approval pending further information.

The Secretary of the State Records Committee signs approved schedules, and the signed schedules become legal, enforceable documents that specify the minimum amount of time listed record series must be held, and indicate the manner of disposition after the retention periods have elapsed.

Schedule Publication

RMS publishes general records schedules, as well as specific retention schedules for individual offices, and provides copies of schedules upon request.

Schedule Amendments

RMS works with agencies to amend schedules to reflect the changing information requirements of government. The process of changing an existing retention schedule is the same as the approval process for new schedules. Changes can include any component of a record series: title, description, retention period or disposition. Factors that drive change include new legal, administrative or fiscal requirements.

Records Disposition Process

Records disposition involves:

1. Physical destruction -- through shredding, burning, discarding or deletion/recycling; or
2. Transfer of ownership -- through awarding custody to a facility or program other than the originating agency - e.g., a county archives, library or museum or the State Archives.

In order to legally dispose of records, agencies must fill out and submit a Request and Authorization for Records Disposal form. County and local officials may submit requests on-line.

The form is legally required to document an official request for destruction by all state, county and municipal agencies. This process ensures that records earmarked for destruction have outlived their value to the public.

RMS checks all requests against current records retention schedules. Each record series appearing on a schedule corresponds to an item number with a title, description and retention/disposition requirements.

Agencies may address unusual or unique situations, such as unscheduled records, by seeking guidance from the State Records Committee through RMS.

Benefits of Compliance

By complying with the statewide destruction authorization process, agencies avoid legal complications and liability associated with inconsistent or illegal records destruction.

Other key benefits of conforming to the State's systematic, legal disposition program include:

1. Economies -- Cost avoidance or savings through reduced purchase and maintenance of real estate, equipment and supplies; and
2. Efficiencies -- Increases in efficiency and safety through the removal of unnecessary files, and reductions in staff time allocated to managing unneeded files.

Potential Problems Associated with Noncompliance

If records are destroyed before their retention periods expire, the public interest may be impacted due to:

1. Unplanned expenses of financial settlements or loss of revenues;
2. Disruption of efficiency due to gaps in information; or
3. Irretrievable loss of historical legacy.

Because records have a life span, there is a point in time in which they are no longer needed and their continued maintenance becomes a liability due to:

1. Unnecessary expenditures for real estate, equipment and supplies;
2. Lack of efficiency as old record accumulations become unwieldy; and
3. Safety hazards because of lack of systematic storage and disposal.

Useless records become a burden in the same way any waste product does. Noncurrent records are perhaps a more insidious waste because without records management, they are not identified and are given the same treatment as the current, valuable information needed to safeguard the public interest.

Summary

A records management program begins with the records inventory process to gain knowledge of holdings. Records are then placed on records retention schedules.

Retention schedules summarize information about individual record series and designate minimum lengths of time records must be held in active and semi active storage. Retention schedules also designate when and how a record may be disposed.

Timely and consistent records disposition yields increases in efficiency and decreases in record keeping expenses. Use of the statewide disposal authorization process helps to eliminate inconsistent records destruction, thereby minimizing the likelihood of adverse legal, administrative, fiscal and historical impact.

Chapter 3

Records Storage Center Operations

It is neither prudent nor possible to keep every record created or received within the confines of most offices. Office space should contain only those records necessary for conducting daily business effectively. Alternative methods of storage are needed for the maintenance of records that must be kept for administrative, legal or fiscal reasons, but are not referred to regularly — i.e., semi-current or inactive records. This is the function of a records storage center.

Generally, agencies transfer high volume semi-current or inactive records to records centers. For purposes of this discussion, these are records that an agency references less than once per month per cubic foot of paper files (see the National Archives and Records Service's Cubic Footage Conversion Table).

Records inventories and records retention schedules (discussed previously in this manual) often provide the raw information needed to pinpoint records eligible for transfer to records centers – e.g., location, reference rates, volume, growth rates, retention period, disposition instructions, etc.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq., 3-2 et seq. and 6.3 et seq.

(Online Source)

Records Center Objectives

Record center operations aim to provide low-cost maintenance of semi-current records. Overall, a records center seeks to provide:

1. Orderly periodic transfer and storage of records which must be retained for limited retention periods but have low reference rates;
2. Standards for indexing, transferring and controlling semi-current records; and
3. Fast, efficient retrieval services, generally with a turnaround time of 24 hours or less from receipt of reference request to delivery of records requested.

Agencies can save significant amounts of money by employing records centers – chiefly through efficient use of space and equipment. For example, when records are housed in office space in standard five drawer vertical file cabinets, one square foot of storage space is needed for each cubic foot of records. (With vertical cabinets, agencies require an additional square foot of work space for each cubic foot of records.) When records are stored in steel shelves in a records center, that ratio is increased to a minimum of five cubic feet of records to each square foot of floor space. Also, records center space is significantly less expensive per square foot than prime office space.

Generally, records center facilities must meet the minimum requirements set forth at N.J.A.C. 15:3-6.3.

Protection of Records

With regard to protection, records centers feature a number of important elements.

Fire

Records center managers minimize exposure to losses from accidental fire by prohibiting smoking in the building and segregating combustible materials from records content.

Well-appointed records centers have automatic sprinklers, smoke detection systems, fire doors and walls, and electrical wiring in metal conduit – all of which are inspected periodically by general building and fire code officials.

Vermin and Contamination

Records center operations protect against damage from vermin and environmental contamination. The organic substances in leather, pastes and paper are a good source of food for vermin. Accumulated dust and debris provide a haven for the growth of insects and mold. Prevention measures depend upon the nature of the pestilence and include keeping the building clean, as well as conducting periodic exterminations and installing filtration for insects and fungus spores, if needed.

Temperature and Humidity

Records centers provide environmental controls and inspection regimes that guard against extreme fluctuations of temperature and humidity that hasten records deterioration. Periodic inspections of the storage facility include monitoring for plumbing leaks, standing water and excess humidity. Records storage boxes may be examined randomly for mold, infestation, or other signs of deterioration.

A properly run records storage center provides constant office-type temperature and humidity, with constant monitoring for unacceptable variations from preset levels.

Access Control and Physical Security

Only authorized staff members are allowed to access records stored in a records storage center. Records center managers maintain lists or registries of persons to whom records may be released. RMS' Records Center Access Authorization Form is an example of the authorization control employed by records centers.

Other security controls include video monitors, guards at stations and on patrol, key card access (for authorized personnel only), central station intrusion detection and alarm systems, and separate locks on all doors.

Records Center Services

Records storage centers provide several key services to public agencies.

Records Transfer

Preparatory Steps

Records center operations and agency staff work together to execute the transfer of records to records center facilities.

To store records at a records storage center, agency staff members check to ensure that records:

1. Appear on an approved records retention schedule;
2. Are scheduled for a minimum of one year storage (avoid storing permanent records in a records center);
3. Are properly identified and documented for transfer and reference;
4. Are properly packed in standard, 1 cubic foot records storage boxes; and
5. Have a specific date (month and year) when disposition will take place.

RMS' "Records Storage Center Criteria and Instructions for Transfer of Records" serves as a guide for transferring records to a records center.

Agency staff or records center personnel may perform the preparatory steps for records transfers. The steps include:

1. Packing records in standard records cartons in the order in which they were filed in their office of origin. To make reference easier, approximately one and one-half (1 1/2) inches of space is left in every box. All of the records, whether letter or legal size, are packed parallel to the long (15 inch) side of the carton so they will be perpendicular to the front of the shelf when stored. In case of fire, this packing method prevents records from falling out of the boxes and feeding flames. Additionally, records that are packed correctly may survive a fire with only minimal damage.
2. Preparing a Records Transfer Request form or similar manifest to itemize the contents of each box. This serves as both documentation of the transfer and later as an index for physically locating specific records for reference. (The information from the manifest can be entered into a records center locator /management database that allows for computerized management of records center holdings.)
3. Label each storage box and enter the agency-assigned box numbers on the transfer manifest. These box numbers become secondary indexes that can be used to locate records that have been transferred to a records center.

Transferring, Receiving and Storing

Records center staff handle the physical transfer, receipt and storage of records (pick-up, delivery and placing items into storage).

The staff checks the general contents of boxes against records transfer manifests to ensure accuracy of the transfer process.

Records center staff then provide a final label for each box with an assigned physical location in the records center, along with disposition dates, and then place boxes in appropriate shelf spaces. The new label replaces the preliminary label of the originating agency. The staff adds records center location numbers to the records transfer list for each box and returns a copy of the amended manifest to the agency. The amended manifest becomes the official record of the transfer. If the records center uses a computerized management system, the staff enters the updated locator and disposition information into the database

Reference Services

Records storage centers provide reference services that include retrieval and delivery of records to authorized officials. The staff may also relay information via a range of alternative formats – e.g., telephone, photocopies, mail, digital content such as images transmitted through an e-mail system, facsimile, etc. Additionally, most records centers include reference rooms where authorized personnel may examine records in person.

Note that the transferring agency retains legal custody of records that it transfers to a records center, and controls access to and use of the records. The agency must therefore update on a regular basis a list of authorized employees who may make reference requests. In turn, it is the duty of records center staff to consult the list and determine if an individual is authorized before releasing any records.

When a file or box is removed from the storage center, staff may produce an "out" slip or a carbon of the Records Request, or some similar control device. They place the slip in the location of the removed items to mark the date of removal and the official to whom the records have been delivered. If applicable, this information can also be part of the records center's computerized management system.

When the agency returns the records, the records center staff removes the "out" slip and amends it by indicating the date of return.

Disposal Services

Records center staff periodically review box transfer manifest and computerized information on their holdings to determine if disposition dates are imminent or if any records are being held beyond their retention periods. They also check current records retention schedules to determine if they have been updated and if an item in storage is affected by the change.

From information gathered during these reviews, the staff sends notices to the applicable agencies describing the cartons of records eligible for destruction, and provides instructions for requesting disposition of the records. (See the Request and Authorization for Records Disposal form. County and local officials may submit disposal requests on-line.)

Based on the information received from the records center, the office of origin verifies which records are earmarked for destruction, provides appropriate signatures and removes items it considers necessary for continuing business despite the expiration of the retention period(s).

After the disposition authorization process is complete, the records center staff removes the targeted records from semi-current storage to be destroyed, and updates the index of holding accordingly.

Records center staff then arrange for the destruction of the records. The staff employs or contracts for destruction processes that obliterate the records – e.g., cross-cut shredding of paper. This is a necessity for the destruction of confidential records. Once destruction actions are complete, the records center staff or the contractor sign a certification attesting to the secure destruction of the records, and store the certification permanently.

Developing Records Center Options

There are five basic approaches to developing facilities to house semi current records:

1. Design and construct a new building for the purpose;
2. Convert an existing building;
3. Retrofit an area within an existing building;
4. Lease common storage space from a commercial storage facility; or
5. Contract a service company which specializes in the storage, maintenance and retrieval of semi current records (With this option, ensure that reference rates are minimal. Although private storage services usually charge very little for storage itself, they do charge extra for all other services, e.g., trucking, receiving, handling, reference, and destruction.)

Choice of an approach involves consideration of a number of factors – e.g., total volume of records – current and future growth, potential cost savings (reduced costs for space, equipment, staff, etc.), budgetary levels, and design and operational factors. Seemingly expensive options such as new construction may become economically justifiable when two or more public entities share a facility. In some jurisdictions, records center services may be provided by regional facilities that serve several municipalities and counties.

As noted previously, all records center facilities must meet the minimum requirements set forth at N.J.A.C. 15:3-6.3.

Summary

Timely and consistent transfer of semi-current records to properly-designed records storage centers provides for operational effectiveness and cost savings. Through the use of records storage centers, agencies will be able reduce storage costs and associated overhead for records storage, while assuring that semi-current records remain available for access through their designated retention periods in a safe and secure environment.

Chapter 4

Paper Files Management

Filing is the process of categorizing and arranging records for effective storage and retrieval based on record series. A record series is a distinct collection of records with similar characteristics — i.e., subject matter, types of documents, or identical retention periods.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq. 3-2 et seq. and 3-6 et seq. (Online Source)

Files Management Program

The central element in files management is the agency file plan. Factor involved in developing a file plan include:

1. Records to be filed;
2. Arrangement techniques — i.e., classification and access systems;
3. Equipment and supplies; and
4. Integration of file plan with basic records management processes such as records retention and disposition and transfers of semi-current to records storage centers (see Records Retention and Disposition and Records Storage Center Operations above).

File Plan Development

The file plan development process includes the following steps:

1. Audit --An audit involves a review of record holdings by records series. This may result in a simple checklist or a detailed report, depending upon the requirements of each office. A records inventory can be used in place of a file audit. An inventory will yield basic information as well as additional details that can be useful in other records management applications.
2. Purge – This involves the segregation and destruction of duplicates or records that have exceeded their designated retention periods, and/or selection of records that can be transferred to a records storage center.
3. Choose a Classification System -- Classification refers to the method of determining and arranging subjects in a file series based on an evaluation of future retrieval needs. A classification system is logical, standardized and practical, and uses the simplest terms available. It may be based on the organization functions involved, and must be exclusive so that subject categories are not redundant. Finally, it must be flexible enough to permit future expansion. Classification systems are alphabetic, numeric or alphanumeric. All other systems are variations of these basic types. Classification is the most important part of a filing system.
    - Alphabetic classification is ideal for a simple filing system with a very low volume of files, generally under 1,000. Alphabetic systems involve filing by subject name. A name could be that of a particular project, company, individual, or geographic location. This type of system requires consistent application. For example, if one person creates a file entitled, “Trenton

Warehouse Project," all subsequent documents should be marked with this title so that they are filed in the "Trenton Warehouse Project" file. If not, someone unfamiliar with this project file could file new documents in the "Urban Property" file.

- Alphabetic classification is ideal for a simple filing system with a very low volume of files, generally under 1,000. Alphabetic systems involve filing by subject name. A name could be that of a particular project, company, individual, or geographic location. This type of system requires consistent application. For example, if one person creates a file entitled, "Trenton Warehouse Project," all subsequent documents should be marked with this title so that they are filed in the "Trenton Warehouse Project" file. If not, someone unfamiliar with this project file could file new documents in the "Urban Property" file.
- Alphabetic classification is ideal for a simple filing system with a very low volume of files, generally under 1,000. Alphabetic systems involve filing by subject name. A name could be that of a particular project, company, individual, or geographic location. This type of system requires consistent application. For example, if one person creates a file entitled, "Trenton Warehouse Project," all subsequent documents should be marked with this title so that they are filed in the "Trenton Warehouse Project" file. If not, someone unfamiliar with this project file could file new documents in the "Urban Property" file.
- Numeric systems are most useful where there are a large volume of files, generally ranging from 1,000 -10,000 files. Invoices, checks, and requisitions are most often requested by number. However, numeric filing systems require cross references for instances in which a number is not known. For example, real property can be listed numerically by block and lot numbers, with alphabetic cross references available by street address or by owners.
- Numeric systems also require maintenance. If numbers are unclear, or are transposed when typed or written, records can easily be misfiled. There are several types of numeric systems: straight numeric, duplex numeric (including middle-digit indexing and terminal-digit indexing), decimal filing systems (e.g., the Dewey Decimal System), and chronological systems. Each system has advantages and disadvantages which should be weighed before being instituted.
- Duplex numeric systems are most useful in situations with a very large number of files, generally 10,000 or more. A duplex numeric system consists of segmented file numbers divided into distinct groups that are sequentially arranged, and includes middle and terminal digit systems:
    - Middle digit systems -- The middle section is the primary division or file drawer identification; the left section is the secondary division or guide identification; and, the right section is the tertiary division or folder identification.
    - Terminal digit system — The right section, or terminal digits are the primary or file drawer identification; the middle digits are the secondary or file guide identification; and the left section is the tertiary or file folder identification.

Both middle and terminal digit systems are used for very large file series, such as patient and insurance policy files, so that filing and retrieval can be spread evenly throughout the filing system.

- Alphanumeric systems include a number/letter combination in which files are arranged in a general category by subjects, i.e., alphabetically and then assigned numbers for subdivisions. This method of filing is not usually found in office applications and is most often reserved for library classification.

4. Determine Access Method -- Access can be either direct or indirect. With a direct access method, no index is necessary to search the files. Subject categories are listed as complete words. Therefore, a direct access filing system must be alphabetic. Direct access allows a user to browse through the files. If the filing system is properly arranged, less time is spent in filing and searching. Moreover, users can readily determine where the record series begins and ends.

   An indirect access method employs the use of a code which requires an index as a cross reference. By using the indirect access method, browsing is not possible. Although indirect access is especially useful for maintaining files that require confidentiality, maintaining an index can be time-consuming.

File Plan Implementation

1. Plan for and procure equipment. Assess factors such as size and volume of records, anticipated retrieval functions, and the physical limitations of an office, especially amounts of available space, and budgetary resources. Types of filing equipment include but are not limited to vertical cabinets, lateral cabinets, open shelving and combinations of mobile and mechanized equipment. Use letter-size equipment (storage for 8.5 inch by 11 inch sheets) wherever practical; because it can result in a combined cost savings of at least 20 per cent over legal size alternatives. Legal- size equipment (8.5 inch by 14 inch sheets) is required in instances where more than one-fifth of the files are legal-size.

   Following is information on the advantages and disadvantages of various kinds of equipment:

   - Vertical cabinets — One of the most commonly-used items of filing equipment, these cabinets generally provide 25 filing inches per drawer. Vertical cabinets are most efficient in small offices where a limited number are needed. However, as the number of cabinets needed increases, space efficiency decreases because of the large amount of office space required for their use.
   - Lateral cabinets — The popularity of these cabinets for general office use has increased in recent years due their space efficiency and easy accessibility. The most common lateral cabinets are 36 or 42 inches wide and hold 32 or 38 inches of files per drawer, respectively. A vertical cabinet will hold only 25 inches of filing per drawer.

     Another advantage of lateral cabinets is their versatility. These cabinets can be adapted, by the addition or deletion of an internal bar, for either letter or legal size filing.

   - Open shelving — This alternative is usually much more economical than vertical or lateral cabinets in terms of cost per filing inch to square foot of floor space. Open shelving permits faster eye contact and retrieval of files, as well as multiple user access. However, because shelves are not enclosed in the same manner as filing cabinets, they do not offer the same protection from fire or water damage or security against unauthorized access, unless shelves are installed in a secured, fireproof vault or have pull-down doors.
   - Mobile shelving -- This configuration can provide the lowest cost per filing inch to square foot of floor space. Mobile shelving consists of shelving units installed on tracks for movement. An aisle can be created between any two units in order to gain access to a particular unit.

     A “mechanical assist” is a device which aids the user in moving shelves, and can be added to

the units. Units can also be motorized to provide faster and easier access to shelves. It is important to note that access can be severely limited in mobile shelving configurations because only one section at a time can be used.

Mobile systems can be tailored to suit a particular office. Generally, however, the amount of user access decreases as the depth of shelving aisles increases. Mobile shelving can provide security because units can be pushed together with the end unit covered and the entire system locked. This feature also provides some protection against fire and water damage.

Mobile shelving has cost and floor load disadvantages. Weight of records placed on mobile shelves can exceed the weight bearing capacity of a floor and cause collapse. When plans for mobile or mechanized shelves are being reviewed, state officials must consult an engineer to determine if the floor is capable of supporting the estimated weight of records and shelves. Another consideration is the prohibitive cost of moving when an agency relocates its offices.

- Rotating filing equipment -- This type of equipment uses motorized or power files and shelving. A motorized or power file consists of folders or trays placed on a shelf with each shelf assigned a location number. The user selects the location number of the corresponding file or item on a locator panel and the equipment rotates until the requested shelf is open to the user. The actual shelving unit is stationary; only the shelves move.

  Large quantities of records can be stored securely in a small space with this type of equipment. However, rotating filing equipment limits user access. It is also very heavy and may not be usable in some offices. Moreover, if the equipment becomes inoperative, files may be inaccessible to the user.

  Rotating filing equipment should only be considered for very large file operations in which equipment costs could be offset by significant space and labor savings. The general disadvantages of mobile shelving units also apply to rotating equipment.

2. Plan for and procure filing supplies Basic supplies for filing systems include folders, labels, guides, and charge-out cards or folders. Neatness should be consistently maintained in the preparation of file folders. For example, labels should be typed and affixed in the same position on each folder. Use straight-edge folders -- i.e., folders in which the tab spans the entire length, is recommended. This aids eye contact for file retrieval. File folders should never be overcrowded. The average folder can hold about three- quarters of an inch of paper, or approximately 75 sheets. Use a new folder when the current folder becomes greater than three-quarters of an inch thick.

   File folders come in a variety of styles. For general use throughout the filing system, 11 point reinforced tab, straight-edge cut, i.e., square cut, Kraft folders are preferred. Point size refers to the thickness of file folder stock, e.g., one point is .001 inch. This type of folder is sturdy and its dark color does not show soiling as easily as manila folders.

   Other types of folders commonly used in filing systems include:

   - Light weight manila folders-- best used for materials with a low reference rate,
   - 18 point Kraft folders -- useful for records with longer retention periods (over 5 years) and high reference activity.

- 25 point pressboard folders -- useful for records with very long retention periods and constant reference, and
- Suspension folders-- most often used in computer printout files and in many lateral and vertical file cabinets.

Use folders carefully because they can occupy up to 40 per cent of the filing capacity of a cabinet.

Use file folder guides to divide files into sections for easier reference and retrieval. Guides can indicate primary divisions, such as general subjects or secondary divisions, or more specific topics under the general subjects.

3. Put the plan into operation.
   - Arrange and label files -- Files should be arranged and labeled in accordance with the file classification system.
   - Develop and implement filing procedures -- Items should be placed into files on a regular basis -- i.e., daily or weekly, depending on the amount of items accumulated. It is important to note that records should be filed in appropriate file equipment.
   - Develop and implement file access procedures -- A central file or cross reference index should be established and a charge-out system used for borrowing files. Duplication should be strictly regulated, with the charge-out system replacing the need to photocopy documents.
   - Provide for file creation -- New files should be created as they are needed. File titles should be unique to the new subjects. A specific subject title, project title, or general title which indicates a common factor linking all documents in a particular file, is essential to an efficient filing system. Lack of specific filing, such as the use of miscellaneous files, is inefficient because it requires lengthy searches for records in alternate locations. "Miscellaneous" should never be used as a file title or label.

General Considerations

Since approximately 70 per cent of the expense of maintaining a filing system involves labor costs, agencies can realize significant savings through the selection of equipment that aids filing and retrieval efforts. The expense of equipment, repairs, operations, supplies and floor space should be considered in relationship to the annual growth rate of files and budgetary levels. Three elements that determine the general cost effectiveness of a filing system are:

- Space efficiency — The capacity of a room or area should be evaluated for accessibility to equipment and files.
- Equipment efficiency— Acquiring equipment that provides effective file storage and retrieval at the lowest possible cost per file inch is a major concern when purchasing equipment. Another factor may include potential of equipment to be updated, modified or augmented.
- The third element (mentioned above) is missing.

Summary

Files management involves the analysis, preparation, and arrangement/classification of files, and allows for rapid and efficient retrieval of records. The files management process begins with a records inventory or a file audit. An inventory or audit yields an understanding of system needs and provides a basis for choosing equipment, supplies and services.

Periodic audits of active files, implementation of records retention schedules and transfers of semi-current records to records storage centers, help to sustain the economy and effectiveness of files management programs.

Chapter 5

Forms Management

A form can be a printed (paper-based) instrument that contains predetermined blank spaces for the insertion of information. A form can also be a computer-based presentation used to collect information. Forms play a central role in the transaction of business, because they represent a standard method for collecting and conveying information that drives business processes. The information can be variable and/or static (remaining constant).

Forms are easier to prepare than open-ended instruments such as letters or reports, because when a form is well designed, desired responses are well- defined and consistent, and the respondent knows what is expected.

Forms management assures that only necessary forms are designed, produced and distributed, and that unnecessary documents are eliminated. The elements of forms management generally consist of forms analysis, forms design, forms history files, and forms procurement techniques.

By achieving control over forms, forms management helps an organization serve the purposes for which it was created. Because of their contributions to the economy and efficiency in record-keeping, forms management programs are integral parts of the records management process.

The overall objective of a forms management program is to provide the most efficient and economical collection of information that an organization needs to fulfill its purpose. The program operates through:

1. Design efficiencies -- providing properly designed, cost-effective forms, redesigning existing forms, designing new forms if needed, eliminating unnecessary forms, and combining forms where possible; and
2. Control efficiencies - controlling forms printing, handling, ordering, storage and distribution functions.

Finally, forms provide the easiest and most efficient link between manual record-keeping and data entry/automated data capture.

This section focuses mainly on traditional paper-based forms management.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq. and 3-2 et seq. (Online Source)

Forms Analysis

Forms analysis is an evaluation of the need for a form, the purpose of a form, its relationship to other currently used forms, and finally, an assessment of its effectiveness as a communications tool. Forms analysis involves a review of business processes supported by forms.

Strive to ensure that every form has a corresponding business process that fulfills one of the purposes or functions of an organization. A business process will involve all of the steps necessary to record, interpret, communicate, and retain information needed to serve a purpose or function.

Generally, one uses a form to begin a process. For example, to obtain a driver's license, the driver fills out a form. This initiates a process that eventually results in the issuance of the license.

Forms analysis encompasses:

1. Business needs -- Knowing the mission of the organization or agency, and evaluating the specific purposes that require work processes, allows for the definition of the informational content of forms. Also, needs analysis may lead the agency to identify forms that are no longer required or that can be combined with other forms.
2. Workflow -- This involves review and analysis of steps in work processes including the types of operations required and when they are performed, along analysis of staff assignments, skill levels, limits of individual responsibility, supervisory structure, and work environment, i.e., physical location, equipment, and supplies used.
3. Related activity --This centers on addressing similar processes or functions that may be occurring elsewhere. If a similar form already exists, it may be possible to alter it to accommodate a new or dual (combined) purpose.
4. Usage --The ease with which a respondent completes a form that begins a process is a key consideration, as is its ability to communicate information that supports the targeted process and to pinpoint who will keep the original and the copies.

All usage considerations bear directly upon the efficiency and cost of record-keeping operations. All forms and copies of forms that contain responses, whether created or received, are records and subject to the considerations including retention and disposition (see Records Retention and Disposition) and active files management and semi-current storage (see Paper Files Management and Records Storage Center Operations).

Importantly, from a strategic perspective, forms can be migrated to electronic formats to allow for public service enhancements – e.g., online, self-service systems with automated workflow, and for reports and applications, combined with public access to those submissions that are open to public inspection.

Forms Design

Forms design is the execution of a pencil draft or automated equivalent that shows the location of lines and copy and any specification that can be indicated by a drawing. These include items such as the location of perforations and hole-punching; paper size, color, and weight; ink color; type size and type style and fields/zones for automated data capture (e.g., Optical Character Recognition, Image Character Recognition and one and two-dimensional bar-coding).

As noted, forms can be migrated to electronic formats that enable service enhancements such as online submission and access. Agencies may consider allowing online forms completion, online submission via e-mail or to a network server or transformation of the form and underlying process to an Internet-based (Web) application that delivers data to the organization without any intermediary processes like mailing, receipt, preparation, scanning, data capture, etc. Online processing yields many benefits including increased accuracy (though automated and consistently-applied edits and business rules), efficiency (less labor effort, equipment and space needed to support processes), timeliness, convenience and security (via the use of automated access controls).

Forms may be designed by using graphics software packages. The advantages of automated forms design include increased speed in preparing drafts and revisions of forms. Also, camera-ready originals may be produced with a high quality output device.

Focus design efforts on creating forms that require the least amount of time and labor to collect and distribute accurate information.

Forms Design Elements

Ballot Boxes

Effective forms are understandable and easy to fill out. A form that uses ballot boxes and pre-printed choices can be completed more quickly and easily than a form that requires respondents to handprint or type an open-ended choice.

Ballot boxes or check boxes are usually 2/10" wide by 1/6" high, and placed in front of their respective pre-printed choices. For example, when a “yes” or “no” answer is required, a ballot box is placed in front of the word “yes,” and another placed in front of the word “no.” Be sure to include all possible choices to questions. Absence of a mark where only one choice exists could mean that the respondent simply neglected to answer.

Captions

Caption blank spaces on a form to indicate precisely what information is being requested. Captions are specific and leave no doubt about how to fill out the form. For example, do not use the caption “date” if there is any question about which date applies.

The most efficient location for a caption is in the upper left hand corner of a box. This permits optimum writing space within the box for the response. Also, a respondent’s answers are easier to read if a small caption is in the upper corner.

This is especially important when a form is being used for data entry. Improperly captioned forms slow the process down and may lead to an increased error rate. If the caption is placed on a line, valuable writing space is lost and responses may be illegible. If it is placed under the line, the respondent may choose to place information either above or below the line.

Distribution and Routing Information

Assign distribution and routing information to paper forms if they must flow to different offices. Insure multi-part forms contain instructions for the distribution of each part. Such information can be included as part of the general instructions for using the form, or may be placed at the bottom margin. Be aware that while multi-part forms provide for greater control of distribution and a reduction of copying costs, they are relatively expensive to produce.

Form Numbers and Titles

Assign numbers to all forms. Include an edition date. Use a self-explanatory title. The preferred location for the title is the top left corner or the center of the top line. Use brief titles that identify the primary subject or purpose of a form.

Ink

Black ink is the most cost-effective color to use in printing forms. Color inks add to the cost of forms not only because they are more expensive, but also because when two or more ink colors are used on the same form, an additional press run is required and the printing process becomes more costly.

Instructions

Place instructions to the immediate right of a form's title or directly below the title. Number instructions and present them in outline form to indicate the necessary steps to complete the form.

Lines

Consider using lines to separate sections on forms, to direct those completing forms to certain areas, and to produce a more aesthetically pleasing document.

Use bold lines for the border of forms, to separate major sections, or to draw attention to a particular box that summarizes or finalizes information, such as a "grand total" box at the bottom of a column of figures.

Use medium lines to separate sections within the border of a form.

Use light lines or "hairlines" to draw ballot boxes and lines within sections.

Margins

A margin on the form is the area between the ink borders and the paper edge. The standard margin is 3/10" on the left and right, and 2/6" on the top and bottom. Top and bottom margins are slightly larger than side margins to allow space for form numbers and routing information.

Some completed forms will be stored in a binder, and will require a one-half inch margin on the left side or top of the form to allow for the holes. Other forms will be placed on a clipboard and space will be needed at the top or left side of the form.

Paper Size, Weight and Color

Use industry-standard paper sizes and weights. Using a paper size that is not standard, or readily available, will increase printing costs because of the additional cutting and handling required. Use of uncommon paper sizes and shapes may also cause filing problems because oversized forms have to be folded to be placed in standard file folders and cabinets, and undersize forms are more likely to be lost.

Contemporary presses accept 17" x 22" paper from which the following four basic sizes can be cut without waste: 8 1/2" x 11", letter size sheet; 8 1/2" x 5 1/2", half of a letter size sheet; 8 1/2" x 3 2/3", approximately one-third of a letter size sheet; and 4 1/4" x 5 1/2", one quarter of a letter size sheet.

These paper sizes can be used either horizontally or vertically, and will satisfy most information recording needs. Avoid using legal size, 11" x 14" paper. It is expensive to purchase, prepare, handle, file and store legal size pages.

For single sheet, single-sided printing, standard paper stock is thirteen pound Bond. The recommendation for double sided printing is sixteen pound or heavier paper stock. For card stock, consider forms with very high reference or handling rates.

Colored paper adds to the cost of a form. Unless business reasons compel use of color, always use white paper.

Shading

Use shading to help guide the eyes, highlight columns, or draw attention to a particular part of a form. Shading also helps to isolate areas on a form that should not be completed by the respondent.

Spacing

Allowing enough space for a respondent to enter information on a form is critical. Too little space will not permit accurate information to be entered easily, while too much space may suggest that additional information is being requested. In either case, the lack of proper spacing can confuse a respondent, lengthen the completion process, and reduce the accuracy of responses.

Measuring in tenths of an inch for horizontal spacing and in sixths of an inch for vertical spacing is recommended. Use forms design paper or automated equipment that employs a grid that corresponds to these dimensions. Forms design paper is readily available from most large stationery suppliers or through art or graphics specialty suppliers.

Single lines entries are 2/6" in height and long enough to contain requested information. When entries are written or hand printed, approximately five characters will fit to the inch. If a typewriter is used, ten characters will fit to the inch. If a form will be completed with a typewriter, use typewriter spacing for vertical spacing (one-sixth of an inch).

Type Styles and Sizes

When selecting type style and size, the primary goal is ease in readability. Generally, avoid the use of ornate type, or a typeface that has many hooks or curls, called serifs. Gothic or sans-serif typeface, sometimes called “clean” type, is a better option. It enables a respondent to read captions and instructions as quickly as possible.

For most applications, type size will range from 6 points to 18 points on all forms. Use 6 point type for marginal notes, form numbers and other identifying information that appears outside form borders. For box design, use 8 point type and for heading and routing information, use 10 point type. 14 point type is appropriate for titles and major section headings, while 18 point type is appropriate for titles.

Most type is available in either regular or bold. Use bold face when special attention needs to be directed to a word or phrase, such as a title or section headings.

Forms History Files

Establishing a forms history file will enable agencies to maintain a selective, organized collection of data on the forms. This information can assist the agency in making decisions about ordering new or current forms, identifying forms that contain duplicated information, defining the cost of forms and tracking the review process of new forms.

When creating a forms history file, provide one file folder for each form. Label each folder with the form’s name and number. Organize the file by the form number. Ensure each folder contains: samples of the form; drafts of proposed revisions to the form; all communications relating to the form, including approval signatures; the camera-ready original (if a paper form); and details of ordering history -- e.g., quantities, printing methods, and information such as listings of vendors and turnaround times.

Creating a Simple Form

The upper left caption box design is the preferred method for designing a form. Place a caption in the upper left area of a box and the entry is either hand printed or typed below the caption. This design allows a respondent who is completing a form the most space for entering information.

The following steps can serve as a guide in the preliminary design of a simple form:

1. Develop a list of the information or fields that will be recorded on the form. Arranged the fields in the desired order of appearance.
2. Determine the amount of horizontal space a field will require indicated in tenths of an inch. Where possible, convert open-ended questions to pre-printed ballot box choices.
3. Proceed with forms layout using forms design paper, a sharp pencil and a ruler, or automated equipment: draw all four margins; place the form title and instructions, if needed, inside the top margin; place the fields and boxes on the form, working left to right, top to bottom, using the list of necessary information; and enter the form number in the proper location.

This preliminary design or rough draft may now be photocopied and distributed for review. Agencies that will be using the form to collect information, or any others who might enter or extract information from the form should be included in the review process.

After the draft form has been reviewed and approved by all of the offices concerned, a copy may be used to prepare the camera-ready original and print the form. This work can be performed in-house or by a private vendor.

Forms Procurement

For paper-based systems, be sure to order correct amounts. Too small a quantity will result in a higher cost per unit of the form. Insufficient quantities increase the danger of prematurely exhausting the existing supply. A lack of necessary forms can prevent an organization from doing its job.

An excessive supply of any given form will add to storage costs. If a form becomes obsolete because of changes in programs or procedures, the excess supply will become useless. A good working relationship with suppliers can aid forms management efforts. Generally, most forms vendors have broad experience in the industry and can offer good advice.

A twelve to eighteen month supply of every form used by an office is the maximum amount recommended. To avoid depleting stock, inventory control is essential. This allows regulation of purchasing so that forms are on hand when needed. Make every effort to anticipate ordering cycles so that new shipments are received when only one month's supply remains.

In considering these points, remember that use of automated forms and systems helps the agency avoid forms procure complexities and costs.

Developing Forms Management Options

Choice of an approach to obtaining forms management services centers on several factors. The content of many forms is often mandated by law or regulation. An agency can institute its own forms management program by: hiring a professional forms analyst; incorporating forms management duties into the responsibilities of existing in-house records and information management experts and providing adequate training; or contracting with a commercial forms design or printing firm to provide forms design and management.

The major concern of any arrangement that provides forms management expertise is to design and produce documents that collect information in the most efficient and effective manner possible.

Summary

Forms management assures that forms needed to collect information are designed, produced, revised and distributed in the most effective and efficient manner possible, while also assuring that unnecessary forms are eliminated.

Some basic forms management considerations include conducting forms analyses, incorporating basic forms design elements, creating forms history files, and maintaining control over the purchase of forms. Basic forms design elements include ballot boxes, captions, distribution and routing information, form number, ink, instructions, line weights, margins, paper size and color, shading, spacing, titles, and type styles and sizes.

Approaches to obtaining forms management include hiring a forms designer, incorporating forms management duties into the responsibilities of an existing, appropriate staff member, or contracting with a vendor to supply part or all of an agency's forms design and management needs.

Chapter 6

Image Processing

Image processing (IP) systems offer reliable, cost effective means of managing information resources. Briefly stated, IP involves the recording of images of documents on electronic storage media and/or photographic film. IP can be used in a variety of information management systems, from simple records storage and retrieval applications to complex configurations involving work flow, automated data capture, payment processing and group collaboration.

Most categories of paper records can be destroyed after they have been converted to image formats. Compliance with State standards set forth in New Jersey's Administrative Code assures the acceptance of imaged records.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq., 3-2 et seq., 3-3 et seq., 3-4 et seq. and 3-5 et seq. (Online Source)

General Objectives of Image Processing Systems

IP systems are designed to provide for effective, economical management of records through achieving one or a combination of the following general benefits:

1. Service Improvements/Innovations -- When agencies employ electronic IP systems in conjunction with business process re-engineering, automated workflow, Internet-based access and database technologies, they are positioned to address strategic opportunities to revitalize non- responsive and inefficient hard-copy based service programs.
2. Space Savings -- Hard copy storage space and equipment requirements can be reduced greatly, or be eliminated entirely, via use of IP technologies.
3. File Integrity -- IP systems provide for controlled/standardized storage and indexing of records on a sustained basis.
4. Security -- IP systems enable inexpensive duplication of their record contents. This allows for the low cost retention of security copies of important or vital records at an off-site location(s). If the original copies of sensitive records are lost or destroyed, duplicates can be retrieved and restored.
5. Quick and Effective Retrieval -- IP systems generally provide quicker, more accurate access and retrieval of documents than bulky paper-based systems. This is true even for the most basic IP formats.
6. Preservation -- Documents that have historical or long-term retention value are often too fragile for daily use. IP systems provide the means for generating durable working copies for researchers to use. This eliminates excessive handling of the original documents and helps prevent further deterioration.

When considering the use of IP, refer to the Association for Image and Information Management's Recommended Practice Report (AIIM ARP1-2009), which provides an excellent overview of analysis, selection and implementation of systems employing electronic image technologies. [1]

Foundations for IP Systems

Choice of Records

From a technical perspective, be aware that such factors as document size, texture, color and condition determine appropriate formats for IP systems. Also important are underlying work flows, which include work steps executed by agency staff, and updating/retrieval patterns. These factors impact the choice of IP technologies. For example, the need to manage high-volume transaction processing systems involving payments and legal filings may indicate the need for a workflow-based electronic system. Records with high reference rates and distributed end-users may require an electronic storage and retrieval solution connected to a wide area network. Customer-facing permit and licensing applications may require an Internet-based self-service approach for document image submission.

From an economic viewpoint, note that conversion of paper records to image format can be expensive, especially without proper analysis and planning. Systems maintenance involves costs as well. Procedurally, the use of IP systems requires development of guidelines for access, use and duplication.

From a strategic perspective, critical transaction flows such as permits, tax returns, legal documents, regulatory filings and associated payments offer the greatest opportunities for service enhancements and innovations. These flows impact the rights and obligations of the citizenry, and therefore, are highly valuable. IP provides a potential avenue to re-engineer these critical flows so that they provide fast, secure, inexpensive, convenient and flexible service channels with rich support information. In the same way, records systems that bear upon transparency and accountability, such as systems that document policy formulation and decision-making, can be made readily accessible to the public via use of IP.

Overall, as with any system initiative, ensure that you evaluate your records systems to identify onerous problems and/or high value opportunities. In this connection, consider the cost/benefit profiles and general feasibility of alternatives. Also, once you select IP alternatives, ensure that records management techniques – e.g., use of records retention and disposition regimes, become parts of the system design.

Before undertaking an IP system project, examine whether procedural alternatives to basic records management problems are workable and available. For instance, authorized disposal of old record accumulations may be possible simply by using current records retention schedules and submitting a destruction request (see Records Retention and Disposition above). In some cases, you may be able to reduce records retention periods to allow for disposition of burdensome accumulations of records. In the same way, revised filing procedures or diligent use of semi current records storage centers may remedy records access and storage difficulties (see Records Storage Center Operations above).

Feasibility Study

Building on the points above, DORES offers a guideline for conducting feasibility studies for IP systems. The guideline provides a structured format for documenting current records system problems/opportunities, and for analyzing/choosing records system alternatives. It consists of six interrelated sections:

IP systems are designed to provide for effective, economical management of records through achieving one or a combination of the following general benefits:

1. Current System Review
2. Success Factors/Statement of Needs
3. Preliminary Evaluation Matrix
4. Alternate System Specification
5. Alternate System Analysis
6. Final Evaluation and Alternative System Choice

Collectively, the six sections address the technical, operational and economic dimensions of current and alternate records management system feasibility.

The guideline does not emphasize a specific technology. Rather, it focuses upon objective analysis of current records systems, the development of a problem statement and general statement of needs, and analysis of various system alternatives. Subsequent to conducting feasibility studies, you may well find that automated alternatives are not feasible or are unnecessary.

Conceptual Model (General Design)

Once you have chosen an alternative IP format, map out your system and service requirements at a conceptual or general level. DORES offers another guideline for this purpose. The conceptual design guideline embodies a self-study (question/answer) process for documenting your requirements in a structured and comprehensive fashion.

Use the guideline to develop general designs for automated record image processing systems and service contracts. Information gathered through use of the guideline may also be incorporated into procurement documents such as Requests for Proposals (RFP).

The guideline does not touch upon equipment configurations. Rather, it is designed for identifying operational/capacity requirements and performance levels. Properly documented requirements and performance levels will provide prospective system vendors and service providers with sufficient information to size proposed equipment configurations and service arrangements.

Certain sections of the guideline may not be applicable to agency initiatives. For example, detailed specification of transaction work steps may not be needed if a proposed system only involves storage and retrieval of electronic images.

Development and Implementation of IP Systems and Services

Like all system development and service enhancement initiatives, successful implementation of IP systems and services depends upon the application of a System Development Life Cycle (SDLC) process and sound project management (PM). Detailed coverage of these topics is beyond the scope of this manual, but suffice it to say here that use of SDLC/PM enables agencies to achieve the functional and strategic goals and objectives of IP initiatives. As described by the National Archives and Records Administration, the SDLC provides a structured and standardized process for all phases of any system development effort – from the general design and functional requirements phases, through to development, testing, integration, implementation and ultimately, the retirement or replacement of the IP platform. In the context of the SDLC, PM centers on the control of time, cost, resources, quality, scope of work, risk, communications and

change process, by a project manager or project management team, with the goal of driving initiatives to successful completion.

State agencies are subject to specific project review and control requirements embodied in the System Architecture Review (SAR), as well as a central review process for all information technology procurements. The SAR supports the SDLC and links to the agency's PM process.

When pursuing an IP initiative, review and follow the SAR requirements if applicable. County and local agencies may wish to use the SAR as a model for their own IP and general information technology programs.

Another consideration is contract management, which is closely aligned with PM. If you are using a contract vendor for IP systems or services, assign a staff resource to monitor contractor goods and services for completeness, quality and price, as well as to handle communications with agency personnel and dispute escalation/resolution. State agencies are subject to specific requirements for contract management, set forth in Circular Letter 10-15-DPP. County and local agencies may wish to refer to this Circular Letter as a model for their own IP and general information technology programs.

DORES/RMS IP Services

RMS offers a wide range of services to public agencies designed to facilitate the change management process associated with the use of IP technologies. Consider using these services as you pursue IP initiatives.

Service Program

RMS has expertise in the development, implementation and management of IP systems and services. These systems and services encompass a broad range of activities – from electronic scanning, indexing and storage of public documents to electronic government applications that supplement or replace paper-based systems.

RMS seeks to accomplish several strategic goals in this area:

1. Comprehensively address records management and IP systems/services planning and development, with emphasis on maximizing efficient use of in-house facilities and contracted services;
2. Reduce redundant and inefficient system purchases;
3. Increase cross-agency sharing of records and information resources;
4. Ensure effective use of automated records systems and services on a sustained basis;
5. Contribute to the continuing improvement of government services; and
6. Foster adherence to core records management standards; and coordinate information technology and records management planning.

Service Packages Offered by RMS

In connection with the above, RMS offers several key service packages to public agencies.

Package 1: Planning for image processing and automated records systems/services
This involves actively assisting agencies in planning for the development of enhanced, cost effective public records systems. RMS will provide records and information management consultative services at the strategic, tactical and operational levels. It will also coordinate in-house and contracted records management, image scanning/indexing and information processing services for State agencies. Planning sets the stage for the remaining RMS service packages.

Engage RMS as early as possible in your planning efforts.

Details on Service Package 1

Package 2: Remittance processing
This involves mechanization of paper-based billing and revenue capture/deposit applications to improve cash management, enhance agency accountability and increase operational efficiency. At the State government level, RMS plans to handle all remittance processing productions operations directly on behalf of State agencies.

Details on Service Package 2

Package 3: Active document processing
Here, the focus is on systems/services designed to automate business applications that revolve around the processing of correspondence, returns, reports and related informational content. Active document processing may encompass the development of automated work flow software, and involve electronic image scanning, indexing and storage/access services -- all designed to streamline program operations, reduce operational costs and improve overall records management capabilities. In this area, for State agencies, RMS may consider an array of in-house and contracted services to meet the specialized needs of customer agencies.

Details on Service Package 3

Package 4: Back File Conversions
These efforts revolve around the conversion of existing accumulations of records to electronic formats for expeditious and efficient storage and retrieval. For State agencies, the emphasis will be on maximizing the use of in-house resources to address agency needs.

Details on Service Package 4

Package 5: Electronic Government
This is the transformational stage of system development. RMS will seek out opportunities to create or coordinate, new, streamlined digital service delivery systems using in-house computing and programming resources whenever possible. The key objective in this area is to make fundamental changes in the way public agencies employ records systems to serve the public and capture revenue. System re-engineering and cross-agency records sharing will be primary considerations in this area.

Details on Service Package 5

How to Include RMS in Planning

Begin dialogue with RMS as early as possible in your systems/services planning cycles. Contact RMS at 609-292-0951 or via e-mail.

Note on Sustainability

Ensure that your planning includes active consideration of system sustainability, particularly if you are storing records with retention periods of 10 years or electronically. Use the System Sustainability Guide or similar methodology to ensure your agency plans and budgets for system migrations at the appropriate times. Also, consult Electronic Records below for guidance on managing scanned images of textual records and other content that may be stored on an IP system.

Summary

Image processing (IP) systems offer reliable, cost effective means of managing information resources. These systems may be based on electronic storage media and/or microfilm.

Careful planning and use of structured approaches to system development life cycles and project management help to ensure the success of IP system and service initiatives.

Successful use of the technology depends upon careful planning and use of structured development techniques and project management, as well as partnering with capable system contractors and service providers.

Chapter 7

Electronic Records

Electronic technologies provide reliable, cost effective avenues for processing, storing, accessing and managing records. Automated records technologies pave the way for service innovations, increased productivity, cost savings associated with reduced staffing, space and equipment requirements, enhanced accountability and greatly improved responsiveness to the public.

Basic records management principles, including retention and disposition scheduling, apply to automated systems that house public records. Procedural and technical controls are needed to ensure that records are not lost, or altered or deleted inappropriately. This section provides guidance on how to apply basic records management principles in the context of commonly-used automated records technologies. The guidelines apply to automated systems administered directly by public agencies, as well as to systems administered by third parties on behalf of public agencies, including cloud based e-mail systems. (See examples of generic system and data-related service levels for cloud service providers.)

Different technologies are covered in separate sub sections. However, note that in reality, agencies are likely to employ several technologies simultaneously across multiple business systems and offices. Accordingly, in daily operations, you will likely need to consider a blended approach to applying the principles, practices and techniques covered below.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq. and 3-2 et seq. (Online Source)

General Use of Electronic Records Technologies

The New Jersey Uniform Electronic Transactions Act (UETA), P. L.2001, c. 116, authorizes, with certain exceptions, state and local government agencies to use electronic forms, electronic filing, and electronic signatures to conduct official business with the public after 26 June 2001.

In basic terms then, by and large, public agencies may use automated technologies to process, store, retrieve, manage, access, use and dispose of records in electronic formats. Accordingly, ensure your agency builds records management principles, techniques and practices, such as those outlined in this manual (while also being mindful of the requirements of New Jersey's legal framework), into all automated records systems.

General considerations relative to use of electronic technologies in the processing of public agency transactions follow.

Electronic Signatures

Per Section 7 of UETA (C.12A:12-7), unless exempted from the provisions of UETA (C. 12A:12-3.b and 3.c), if a law requires a record to be in writing, an electronic record satisfies the law; and if a law requires a signature, an electronic signature satisfies the law. The law defines "electronic signature" broadly as an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record (C. 12A:12-2). If a law requires a signature or record

to be notarized, acknowledged, verified, or made under oath, per C.12A:12-11, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record. In all then, agencies have a wide range of discretion with regard to how they implement electronic systems that require signatures.

The keys to choosing a signature method revolve around the significance of the transaction and its informational contents, the consequences of any disputed transaction (including risk of repudiation by the sender or receiver), revenue impacts, impaired legal rights, legal costs (to assert admissibility in the event of a legal challenge), risks of fraud, requirements for long term preservation and general costs/benefits of alternative signature regimes. The law itself (C. 12A:12-18) enables agencies, after due consideration of security, to specify and implement several elements:

1. The manner and format in which the electronic records must be created, generated, sent, communicated, received and stored and the system established for those purposes;
2. If electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;
3. Control processes and procedures appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality and auditability of electronic records; and
4. Any other required attributes for electronic records which are currently specified for corresponding non-electronic records, or reasonably necessary under the circumstances.

After considering the elements above, agencies may choose from a number of electronic signature requirements such as the following:

1. Conformed signature (typed name/title online) Consider using this approach when the laws underlying the system do not require an authenticated/verified signature and the operational, economic and service benefits of the approach outweigh the risks and impacts of repudiation or fraud.
2. Facsimile-based signature sheet: The use case here is largely the same as that of the conformed signature.
3. Personal Identification Number (PIN)
4. Authenticated user ID and password
5. Use a multi-factor/verified method for setting up an ID and password.
6. Public Key Infrastructure or PKI: This involves the use of public/private digital key pairs issued by a trusted third party. The approach offers very high degrees of security, authentication and non-repudiation. However, you will need to weigh these advantages against drawbacks like technical complexity, cost, sustainability (need to migrate/convert electronically signed documents to new generations of the technology) and potential impacts on system throughput and end user adoption rates.

Trustworthiness of Electronic Records

No matter which electronic technologies an agency employs for managing public records, trustworthiness is a key consideration. Reliability, authenticity, integrity, and usability are the characteristics of trustworthy

records systems.[2] You will see these characteristics emphasized, implicitly and explicitly through this section.

When planning to implement an electronic signature technology so that it can meet its internal business and legal needs, and external regulations or requirements. The degree of effort an agency expends on ensuring that these characteristics are present depends on the agency's business needs or perception of risk. Transactions that are critical to the agency's business needs and/or the rights of the citizenry may need a greater assurance level. For guidance on whether records are trustworthy for legal purposes, consult your attorney or legal counsel.

1. Reliability: A reliable record is one whose content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities.
2. Authenticity: An authentic record is one that is proven to be what it purports to be and to have been created or sent by the person who purports to have created and sent it. A record should be created at the point in time of the transaction or incident to which it relates, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction. To demonstrate the authenticity of records, implement and document policies and procedures that control the creation, transmission, receipt, and maintenance of records to ensure that records creators are authorized and identified, and that records are protected against unauthorized addition, deletion, and alteration.
3. Integrity: The integrity of a record refers to it being complete and unaltered. It is necessary that a record be protected against alteration without appropriate permission. Specify what, if any, additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Note and document any authorized annotation or addition to a record made after it is complete. Also maintain the structural integrity of electronic records. The structure of a record is comprised of its physical and logical format and the relationships among the data elements of the record. These should remain physically or logically intact. Failure to maintain the record's structural integrity may impair its reliability and authenticity.
4. Usability: A usable record is one which can be located, retrieved, presented, and interpreted. In any subsequent retrieval and use, the record should be capable of being directly connected to the business activity or transaction which produced it. It should be possible to identify a record within the context of broader business activities and functions. The links between records which document a sequence of activities should be maintained. These contextual linkages of records should carry the information needed for an understanding of the transaction that created and used them.

Electronic Mail

Consider following these guidelines to help your agency manage electronic mail (e-mail) messages and associated content as public records per the Destruction of Public Records Act, P.L. 1953, c. 410 (N.J.S. 47:3-16).

By managing e-mail as public records, public agencies enhance their capacity to capture, retain and dispose of electronic records in an effective and efficient manner. Acting in this fashion also improves agencies' ability to comply with New Jersey's Open Public Records Act (OPRA), P.L. 2001, c. 404 (N.J.S. 47:1A-1.1) See the guide for records custodians.

In connection with the points above, State agencies should follow Circular Letter (CL) 14-12-DORES/OIT, Enterprise Electronic Mail Retention and Disposition Framework. County and local agencies may apply the electronic mail schedules designed for them (C820000-013, 0800-0000 - 0800-0001 and M100000-013, 0800-0000 - 0800-0001). The material presented here builds on CL 14-12 and guidance and schedules produced by the National Archives and Records Administration (NARA), with an eye toward facilitating adoption of the CL and county/local e-mail schedules. Toward this same end, agencies may also wish to consider the related e-mail retention and disposition program frameworks discussed in Chapter 15.

Overview

Electronic mail systems, commonly called e-mail, are the communications method of choice for many public officials and public employees in New Jersey. Public employees use e-mail for mundane communications, as well as for communications involving substantive information or records previously committed to paper. This nexus of communications and record creation/keeping compels public agencies to treat e-mail messages as records.

The management of e-mail systems touches on many important operational concerns including privacy, business administration, vital records management, security, auditing, and public access. Given this, the need to manage e-mail messages and systems in a structured and sustained fashion is clear. In connection with this, public agencies must be aware that they are responsible for retaining, managing and disposing of e-mail messages in an orderly and accountable fashion.

Definitions

"E-mail systems" are computer-based systems that transport messages from one computer user to another. E-mail systems range in scope and size. They may be local platforms that move messages to users within an agency or office over a local area network (LAN) or enterprise-wide e-mail systems that carry messages to various users in various physical locations over a wide area network. The latter may include systems that send and receive message around the world over the Internet. Often the same e-mail system serves all three functions.

E-mail Messages

"E-mail messages" are electronic documents created and sent or received by a computer system. This definition applies equally to the contents of e-mail messages and any attachments associated with these messages. Thus, e-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

E-Mail as Government/Public Records – Impacts on Access and Retention/Disposition

Read the following section to gain an understanding of the legal requirements impacting e-mail messages in relation to public access and retention and disposition.

Access

New Jersey State Statutes Annotated (NJSA) do not include a specific definition for electronic mail; however, the Open Public Records Act (OPRA), P.L. 2001, c. 404 (N.J.S.A. 47:1A-1.1) defines a "government record" or "record" as:

"... any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data processed or image processed document, information stored or maintained electronically or by sound recording or in a similar device, or any copy thereof, that has been made, maintained or kept on file in the course of his or its official business by any officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received in the course of his or its official business by such officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof. The terms shall not include inter-agency or intra-agency advisory, consultative, or deliberative material."

Given the language above, for purposes of OPRA compliance, all e-mail communications that document an agency's functions, policies, decisions, procedures, operations or other official activities fall under the umbrella of the definition of a government record per N.J.S.A. 47:1A-1.1. These records are therefore subject to public access during their required retention periods, unless they are covered by a specific exception listed in the law and/or administrative regulations. (Consult with your legal advisors for guidance on how to review and apply exceptions to the public access mandate.)

Retention and Disposition

All public records defined in State law (N.J.S. 47:3-16, as amended), **whether open to public access or not**, must be retained according to records retention and disposition schedules approved by the State Records Committee (N.J.S. 47:3-20, as amended).

In this connection, the definition for public records under N.J.S. 47:3-16 states in pertinent part:

"… public records mean any paper, written or printed book, document or drawing, map or plan, photograph, microfilm, data processed or image processed document, sound recording or in a similar device, or any copy thereof, that has been made or required by law to be received for filing, indexing, or reproducing by any officer, commission, agency, or authority of the State or any political subdivision thereof, including any subordinate boards thereof, or that has been received in the course of his or its official business by such officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof, in connection with the transaction of public business and has been retained by such recipient or its successor as evidence of its activities or because of the information contained therein."

Accordingly, whether they are subject to public access or not, e-mail messages that fall under the inclusive definition above must be maintained and disposed per approved public records retention and disposition procedures.

Two general approaches to e-mail retention scheduling and authorized disposition that are available to public agencies in New Jersey are discussed below.

****Note:** Due to the still-evolving nature of e-mail technologies and processes, RMS anticipates that new and improved approaches to e-mail management (including retention and disposition regimes) will emerge

as time goes on. Accordingly, agencies are encouraged to share with RMS their experiences in applying the two approaches, or indeed, to propose alternative retention/disposition regimes designed to meet the legal requirements of the public records law. Such feedback will help RMS develop and post responsive guidance in this manual on a continual basis.

Approaches to Retention Scheduling/Authorized Disposition

Agencies may consider two general approaches to e-mail retention scheduling and authorized disposition:

- Approach 1 – Itemized content-based appraisal and classification (by individual record series)
- Approach 2 -- General scheduling (sometimes called large bucket or broadband scheduling) as prescribed in Circular Letter 14-12 DORES/OIT and schedules and C820000-013, 0800-0000 - 0800-0001 and M100000-013, 0800-0000 - 0800-0001.

Approach 1, Content-based Appraisal/Classification

This approach assumes that adopting agencies have the ability to classify e-mail records by individual record series, and if applicable, to identify and manage non-record e-mail in a precise fashion. It also assumes that when requesting to dispose of e-mail messages/attachments, agencies have the ability to segregate and dispose of the records by individual records series/date ranges, and to attest that only the e-mail records named in a disposition request are being disposed of.

Note that under Approach 1, agencies have the option of classifying e-mail as both non-record e-mail items and official e-mail records.

Non-Record E-mail

Delete e-mail messages that do not meet the criteria of N.J.S. 47:3-16 at any time, unless they become part of some official record as a result of special circumstances. These types of messages may include:

- Personal Correspondence -- Any e-mail not received or created in the course of state business, may be deleted immediately, since it is not an official record. Examples include unsolicited e-mail advertisements, commonly called "SPAM," personal messages, or the "Let's do lunch" (not a State-business meeting over lunch), or "Can I catch a ride?" type of note.
- Non-Governmental Publications -- Publications, promotional material from vendors, and similar materials that are publicly available to anyone, are not official records unless specifically incorporated into other official records. This includes listserv messages (other than those you post in your official capacity), unsolicited promotional material, files copied or downloaded from Internet sites, etc. Delete these items immediately, or maintain them in a "Non-Record" mailbox and delete them at a later time, just as you might dispose of unwanted publications or promotional flyers received in the mail.

  Caution: While it may be efficient to allow employees to delete non-record e-mail content, agencies must determine whether there are legal and compliance exposures associated with allowing employees to make their own decisions in this area. Agencies may find that the safest and most effective approach, all factors considered, is to treat all e-mail messages/attachments as public records.

Official E-mail Records

E-mail messages/attachments that meet the definition of a record in N.J.S. 47:3-16 are official public records. Schedule, retain and dispose of them as such in accordance with records retention schedules approved by the State Records Committee. Most records will fall under one of the record series listed on an approved general retention schedule.

Do not dispose of any e-mail records that are classified as Permanent or Archival or targeted for Archival Review until provisions have been made to preserve the records for long-term or permanent uses as deemed appropriate by the agency (county and local government levels) or State Archives (State government level). As applicable, plan to preserve all permanent e-mail records (see Long Term Retention of E-mail and Managing Electronic Mail, Filing Options below).

Approach 2, Broadband/General Scheduling

Pursuant to CL 14-2 DORES/OIT and schedules M100000-013, 0800-0000 - 0800-0001 and C820000-013, 0800-0000 - 0800-0001, this approach calls for the management of e-mail records based on a broadband or general seven year retention period. It assumes that e-mail records managed in this fashion are, essentially, general administrative records that require retention for up to seven years.

Importantly, Approach 2 entails two key pre-requisites:

- That agencies have the ability to individually classify any e-mail records associated with longer-term (greater than seven-year) retention requirements and to manage them in separate records-keeping systems; and
- That when requesting to dispose of e-mail records, agencies can attest that records with greater than seven-year retention requirements are kept in separate record-keeping systems and that their e-mail systems include certain core functional elements*.

*See CL 14-2 DORES/OIT and schedules C820000-013, 0800-0000 - 0800-0001 and M100000-013, 0800-0000 - 0800-0001 for the core functional elements.

General Considerations and Guidelines

Following are considerations and guidelines that apply generically to e-mail records management, and are thus relevant to both of the approaches to retention scheduling and authorized disposition discussed above.

Record Copy E-mail

E-mail messages are often widely distributed to a number of various recipients. Determining which individual maintains the record copy of the message (i.e., the original, official message that must be retained for the length of the official retention period) is an important consideration relative to efficient e-mail management.

In many cases, the record copy responsibility rests with the creator of the policy document. Generally, consider the individual who sends an e-mail message and the primary recipient ("To" not "CC") as the persons who retain the record copy of the message. Be aware that that notwithstanding this general

practice, given the varied uses and wide distribution of e-mail, you may need to make exceptions to this rule.

Likewise, if you are confronted with system limitations that prevent you from segregating record copies from extraneous copies, you may opt to retain all e-mail messages (an inherently less efficient practice, but one that mitigates risks of inappropriate deletions). In the same connection, be aware that your agency may be able to employ automated de-duplication techniques that eliminate demonstrably redundant copies of e-mail messages from an e-mail system. De-duplication makes e-mail systems much easier to manage and reduces disk space consumed by redundant information.

Filing

File e-mail in a way that enhances its accessibility, and facilitates records management tasks.

In all cases, ensure e-mail contains searchable meta-data and content, including:

- Names and e-mail addresses of recipients and senders, including names and addresses of all members of distribution lists*

  *The policy for State agencies can be found in the Office of Information Technology's naming standards -- Personal Naming Standards for E-Mail Addresses (94-04-NJOIT). If your agency uses an electronic mail system that identifies users by codes or nicknames or identifies addressees only by the name of a distribution list, instruct staff on how to retain names on directories or distributions lists to ensure identification of the sender and addressee(s) of messages.

- Time and date that the e-mail was sent and delivered

  If your agency employs request acknowledgments or receipts showing that a message reached the mailbox or inbox of each addressee, or that an addressee opened the message, issue instructions to e-mail users specifying when to request such receipts or acknowledgments for record-keeping purposes and how to preserve them.

- Subject line that describes the content of the e-mail

The information above identifies the context in which e-mail records exists.

Content that must be filed includes text in the body of e-mail messages and attachments, if applicable. To the maximum extent possible, ensure you employ widely used file formats for attachments such as pdf, and/or formats that can be converted readily from one application program to another – e.g., popular word processing and spread sheet files that can be converted from one product suite to another (see Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats). Procure conversion programs for attachments and e-mail messages when migrating from one e-mail system to another.

If you wish to use itemized classification of e-mail records, as in done under Approach 1, consider directing employees to transfer e-mail messages from their in and out boxes to folders that list the subject matter involved, such as "Budget and Planning", "Human Resources", "Project XYZ", etc., and that parallel the associated retention requirements (3 years, 4 years, delete after superseded, etc.). The drawback to this approach is that by allowing employees to classify their own messages, the agency almost inevitably assures inconsistency, because each staff member will follow his/her own views of how best to classify

items. To deal with this issue, consider adopting mandatory filing schemes that specify the folder/file names and filings rules. Bear in mind, however, that this approach may also have limitations; it will likely be a substantial undertaking, and difficult to enforce and sustain over time.

In line with the thoughts above, as a future consideration, note that newer forms of software that classify e-mail based on controlled vocabularies/enterprise-wide taxonomies and automated records classification processes offer the promise of fully automated, itemized retention scheduling and authorized disposition management. While not generally in use today, this type of technology may ultimately prove to be the best alternative to controlling and documenting e-mail retention and disposition. Developments in this area are well worth tracking.

Exceptions to Public Access

Where and when appropriate, it may be advisable for e-mail users to label their e-mail (in the subject line) as containing confidential or inter-agency or intra-agency advisory, consultative, or deliberative material or other information which falls under the exceptions to public access under the Open Public Records Act (OPRA).

Storage and Archiving of E-mail

Explore several options for retaining e-mail records: on-line storage; electronic records systems; journaling/archiving; and off-line storage.

For practical reasons, **plan on employing more than one storage option.**

It is important to remember that messages only have to be retained and stored for as long as the retention period requires. Very few messages must be maintained for a long period of time or permanently.

- On-line Storage -- On-line storage is defined as storage of e-mail messages, metadata, and attachments directly in the agency's production e-mail system. On-line storage maintains the full functionality of the e-mail message, and allows users to recall the message at any time for reference or responding. A disadvantage of on-line storage is the potential costs and effects of storage on the performance of the e-mail system.
- Electronic Records Systems --Electronic records systems accommodate storage of e-mail messages, metadata, and attachments on computer platforms that that are separate from, but linked to, the e-mail system. These systems provide for the capture, classification, storage, preservation, access/use and disposition of e-mail transferred from the online system. They facilitate centralized management of e-mail and other electronic records. (The more robust systems also accommodate features such as litigation holds that locate, segregate and preserve items relevant to investigations, audits or law suits. They may also provide facilities that control paper files, records centers and electronic imaging systems.)

  Electronic records systems are not e-mail archive/journaling systems (discussed below), but rather separate automated systems designed to centralize control over and access to various electronic records, including but not limited to, e-mail. They may include near line storage that use tape or disk libraries to retrieve required content.

  If your agency employs an electronic records management system, set up protocols that enable the controlled transfer of e-mail messages from the on-line platform to the centralized system.

Store content transferred to an electronic records system in a format that is compatible with agency operations, and filed according to filing practices established by the agency and/or user.

Discourage the transfer of e-mail to local (desk top) hard drives, because individual employees typically do not use adequate backup policies and procedures on a consistent basis. Also, this practice can hamper and/or greatly complicate retrieval efforts (for OPRA compliance and/or responses to investigations or legal discovery).

- E-mail Journaling/Archiving** (or Vaulting) -- This approach involves the transfer of all e-mail sent to/received by an agency, from the online system to a dedicated computing platform -- for preservation, access and ultimately, disposal. Transfers can occur in real time as items are sent/received, and/or on a timed basis.

  Unlike the more encompassing electronic records systems described previously, journaling/archiving systems are typically focused on e-mail. They store items on high density electronic media and index e-mail in a way that streamlines retention and disposition actions, reduces system overhead for storage, and simplifies and optimizes searching independent of the original authors/recipient of the e-mail.

  Like electronic records systems, journaling/archiving systems also accommodate features such as litigation holds that locate, segregate and preserver items relevant to investigations, audits or law suits.

  **The term “archiving” in this context does not indicate transfer to an official archival repository program. Here, the term relates to the technology employed.

- Off-line storage -- Off-line storage is defined as the storage of e-mail messages, metadata, and attachments outside of an electronic record-keeping environment. The clearest example of this type of storage is to simply print out an e-mail message to paper, with its contextual information and attachments in place, for filing within existing filing systems. Off-line storage may also include such methods as computer-output-to-microfilm (COM) or the writing of e-mail messages, attachments and metadata to electronic storage media such as magnetic tape, magnetic disk or optical disk. Be aware that in off-line storage environments, e-mail messages may no longer be searchable or retrievable in electronic form and/or the searching and retrieving functionality may be dramatically reduced.

Long Term Retention of E-mail

Plan to schedule the transfer of e-mail messages that must be retained for more than seven years or permanently from the on-line e-mail system to a separate record-keeping system – for example, an electronic records management system, journal/archive and/or off-line facility.

Develop a plan to refresh, update and/or replace the separate record-keeping system to ensure it supports organized retention, access and disposition of e-mail records on an on-going basis (see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats). If your agency aims to replace its system with newer technology, be sure to plan for the migration and/or conversion of long term retention items to the new platform.

Finally, remember that off-line storage of records must be in compliance with State records storage standards set forth in N.J.A.C. 15:3-6.

E-mail Messages and the Rules of Evidence

With regard to the use of records in legal proceedings, courts concentrate on assurances that records, and the systems used to generate and manage them, are trustworthy. Specifically, courts seek to determine whether: records are used in the routine course of business; render complete and accurate representations of the underlying facts, transactions or decisions they purport to document; and the authors/recipients are who they purport to be. Trustworthiness is the key for admissibility of records as evidence in legal proceedings. In connection with this, work to ensure that your e-mail system:

- Has up-to-date systems documentation
- Has documented system security controls and back-up programs that run regularly and consistently (See the research paper entitled Security for the Networked Enterprise, Elements of a Holistic Approach in the Appendix for more background information on security in networked computing environments.)
- Retains all data and audit trails necessary to prove its reliability – that is, be able to prove that all messages are created, received and retained in the normal course of agency business, and that the record copies of messages are identified and maintained in accordance with approved records retention schedules
- Coordinates back-up procedures with disposition actions so that no copies of destroyed records are maintained after their retention periods have expired
- In addition to the above, plan for training staff with regard to their responsibility for retaining e-mail records, especially in relation to identifying and retaining record copies (see Record Copy E-mail above). Finally, e-mail system administrators should have the right and capability to prevent destruction of records for legal and/or audit purposes.

Retrieval/Access

Maintain e-mail in a format that preserves contextual information (metadata described previously), and that facilitates retrieval and access. Also, to prevent inappropriate disclosure, set up procedures and processes that provide for deletion of messages after their retention periods expire.

Roles and Responsibilities

Define roles and responsibilities of agency personnel involved with e-mail. It is especially important for agency records management personnel to work with their senior managers, legal counselors and information technology staff to establish policies and procedures for e-mail management.

Make sure employees understand that most e-mail messages are public records and cannot be deleted or destroyed on a discretionary basis.

Work with system administrators to ensure that unauthorized users are not able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology managers and server administrators share responsibility for managing electronic records. Endeavor to clarify these roles, and adopt supporting procedures, training programs and compliance auditing techniques. In conjunction with system administrators, take appropriate measures to preserve data integrity, confidentiality and physical security of e-mail records.

When an employee separates from an agency, whether it is due to resignation, retirement, or termination, have a knowledgeable agency administrator(s) review the employee's e-mail account to determine which e-mails should be retained and what the appropriate retention periods should be, and then act accordingly.

Deletion of Content and Disposal of Storage Media

Be aware that normal deletion processes do not assure the full destruction of e-mail records. In most cases, deletion only removes the index information that points to the records. Talk to your IT support staff about using a form of secure deletion (on both online storage and back-up media), which effectively obliterates the targeted contents.

If an e-mail system is retired or converted to another platform and it becomes necessary to dispose of the storage media that had housed e-mail content on the retired/converted system, ensure that the media are destroyed in such a way as to obliterate any traces of the content they had contained. In this regard, State agencies must follow the policies, standards, and procedures set forth by the Office of Information Technology -- Information Disposal and Media Sanitization (09-10-NJOIT). [3]

Scanned Images of Textual Records

To facilitate effective and efficient preservation, processing and access to scanned images of textual records stored in electronic image processing systems, follow the guidelines below. The guidelines on file formats and image quality are drawn from information posted by NARA.

File Formats

To ensure that images can be migrated to new or upgraded systems in the future, store them in at least one of the following formats.

1. Tagged Image File Format (.tiff, .tif).
2. Graphics Interchange Format (.gif)
3. Basic Image Interchange Format (.bif, .biif)
4. Portable Network Graphics (.png)

Note: If the scanned records are classified as archival or designated for archival review, contact Records Management Services for further guidance on how to ensure you will be able to transfer the images to an archival facility.

Image Quality

Comply with acceptable image quality specifications. Ensure that you follow minimum requirements for scanning resolution and pixel (bit) depth.

1. Bitonal (1-bit) - Scan at 200-600 ppi.(300 recommended default setting) This is appropriate for documents that consist exclusively of printed type possessing high inherent contrast (e.g., laser printed or typeset on a white background).
2. Gray scale (8-bit) - Scan at 300-400 ppi. (400 recommended default setting) This is appropriate for textual documents of poor legibility because of low inherent contrast, staining or fading (e.g., carbon copies, thermofax, or documents with handwritten annotations or other markings), or that contain halftone illustrations or photographs.
3. Color (24-bit RGB [Red, Green, Blue]) - Scan at 300-400 ppi. (400 recommended default setting) Color mode (if technically available) is appropriate for text containing color information important to interpretation or content.

Records Management Controls

Address basic records management controls by incorporating the following into electronic systems. This will help to ensure that scanned records provide adequate and proper documentation of agency business for as long as the informational content is needed.

Incorporate controls into the electronic information system itself or integrate them into a recordkeeping system that is external to the system.

1. Retention and disposition: These are basic retention and disposition controls that relate to approved retention and disposition scheduling. Most scanned images will correspond directly to agency-specific or general records retention schedules. Retain scanned images that serve as the official or record copies of public records for the length of their designated retention periods and, at a minimum, provide for deletion of the records following the receipt of approval for the disposition action. If you maintain a mix of different record series within individual case of transaction files, and cannot readily separate the series for retention and disposition purposes, use the longest retention period to guide your disposition actions. If you store long term (retention greater than 10 years), permanent or archival records on an electronic system, be sure to address guard against technical obsolescence (see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats).

   Be aware that normal deletion processes do not assure the full destruction of imaged records. In most cases, deletion only removes the index information that points to the records. Contact your system administrator to determine whether it would be appropriate to employ a form of secure deletion (on both online storage and back-up media), which effectively obliterates the targeted contents.

   If a system is retired or converted to another platform and it becomes necessary to dispose of the storage media that had housed electronic records, ensure that the media are destroyed in such a way as to obliterate any traces of the content they had contained. In this regard, State agencies must follow the policies, standards, and procedures set forth by the Office of Information Technology -- Information Disposal and Media Sanitization (09-10-NJOIT).

2. Reliability: Controls that ensure the records are full and accurate representations of the transactions, activities in a trustworthy fashion. Following image processing system standards set forth in NJAC.15:3 et seq. and records retention and disposition practices will bolster reliability (see Records Retention and Disposition).
3. Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment - for example, role-based user access controls.
4. Integrity: Controls, such as audit trails, to ensure records are complete and unaltered. Key considerations here include preserving:
   - The original informational contents of the records as produced by the author or process that created the record.
   - The organizational, functional and transactional context of the record, including links to related records that reflect the business, legal and regulatory circumstances in which the record was produced. In this area, maintenance of meta-data is a key – for example, record type, date/time of creation/receipt, version numbers, name of author, date/time of submission and

approvals (for instance, names/titles of people who authorize an action or grant a benefit requested in the record).
- The original physical and logical structure of the records and the relationships between the data elements they contain.

5. Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted. Ensure you develop and maintain consistent classification schemes for records – for example, classify by responsible office, function, and/or informational content. Also, maintain indexes that allow authorized users to locate stored records. – e.g., unique document ID's and meta-data fields such as author/submitter name, data sent/received, topic keywords, etc.
6. For new systems development or significant system enhancements, address records management and preservation as integral parts of the system planning process and design specification. As part of the planning and systems development life cycle, ensure:
   - That core records management controls (1-5 above) are part of the system design.
   - That all records in the system will be retrievable and usable for as long as needed to conduct agency business (i.e., for the length of their State- approved retention periods). Where records must be retained beyond the anticipated life of the system, plan and budget for the migration of records and their associated metadata (index and related data) to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.
   - If the scanned records involved are classified as archival or designated for archival review, contact Records Management Services for further guidance on how to ensure you will be able to transfer the images to an archival facility.
7. Provide for standard interchange formats (e.g., ASCII or XML) when needed to permit the exchange of electronic documents between offices using different software or operating systems.
8. Guard against technological obsolescence. Design and implement migration and/or back-up strategies to counteract hardware and software dependencies, especially if the electronic records must be maintained beyond the anticipated life of the system used to create and/or capture them originally (risk of technological obsolescence). To successfully protect records against technological obsolescence:
   - Monitor actively and consistently for system viability and plan/act accordingly (see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats).
   - Determine if the State-approved retention period for the records will be longer than the life of the underlying system. If so, plan for the migration of the records to a new system before the current system is retired.
   - Carry out upgrades of hardware and software with the goal of retaining the functionality and integrity of the electronic records stored within the system. To maintain record functionality and integrity:
     - Retain the records in sustainable formats (by following these guidelines) until their authorized disposition date.
     - Ensure new storage media are compatible with the underlying hardware and software platforms.
     - Maintain a link between records and their metadata through conversion or migration process.

- If applicable, ensure that migration strategies address non-active electronic records that are stored off-line.

9. Focus on building and employing appropriate electronic recordkeeping functions into all electronic recordkeeping systems:
   - Declare records. Assign unique identifiers to records.
   - Capture records. Where applicable, provide for the import of records from other sources via manual and/or automated processes, maintaining content, context and structure as outlined previously, or link records to other related systems.
   - Organize records. Associate records with approved records schedules and disposition instructions.
   - Maintain records security. Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.
   - Manage access and retrieval. Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.
   - Preserve records. Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business and to meet State-approved retention and disposition requirements. Develop procedures to enable the migration of records and their associated metadata to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.
   - Execute disposition. Identify and delete temporary records that are eligible for disposal in accordance with State-approved retention and disposition instructions. If applicable, identify and effectuate the transfer of archival records to a repository designated by the State Archives, based on State-approved records schedules. Apply records litigation hold or freeze on disposition actions when required.

     Note: Do not rely on system and file backup processes and media to cover electronic recordkeeping functions.

10. Take appropriate actions to maintain electronic information systems.

    Maintain inventories of electronic information systems and review the systems periodically for conformance to established agency procedures, standards, and policies. Determine if records have been properly identified and described, and if the records schedule descriptions and retention periods reflect current informational value and use. Modify records schedules as required.

    Maintain up-to-date documentation about electronic information systems that is adequate to:

    - Specify all technical characteristics necessary for reading and processing the records contained in the system;
    - Identify all inputs and outputs;
    - Define the contents of the files and records;
    - Determine restrictions on access and use;
    - Understand the purpose(s) and function(s) of the system;
    - Describe update cycles or conditions and rules for adding, changing, or deleting information in the system.

- Ensure the timely, authorized disposition of the records in accordance with approved retention schedules.

11. When required, dispose of storage media that housed electronic records so that the media are destroyed in such a way as to obliterate any races of the content they had contained. In this regard, State agencies must follow the policies, standards, and procedures set forth by the Office of Information Technology -- Information Disposal and Media Sanitization (09-10-NJOIT).
12. Maintain media containing permanent, archival and unscheduled records in a facility that ensures continual temperature and relative humidity ranges: temperature at 62 – 68 degrees Fahrenheit; and relative humidity at 35% to 45%. Also, maintain media containing permanent, archival and unscheduled records in smoke-free environments.

    For additional guidance on the maintenance and storage of CDs and DVDS, agencies may consult the National Institute of Standards and Technology (NIST) Special Publication 500-252, Care and Handling of CDs and DVDs.

    Test magnetic computer tape media no more than 6 months prior to using them to store electronic records that are unscheduled or scheduled for permanent or archival retention. Verify that magnetic computer tapes are free of permanent errors and in compliance with industry standards.

    Periodically read a statistical sample of all magnetic computer tape media containing permanent, archival or unscheduled records to identify any loss of data and to discover and correct the causes of data loss. Replace magnetic tapes with 10 or more errors. When possible, restore lost data. Read and correct, as appropriate, all other magnetic computer tape media that might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling).

    Before media are 10 years old, copy permanent or unscheduled data on magnetic records storage media onto tested and verified new electronic media.

    Consider using disk to disk back-up and/or replication of images and related content to an alternate site via a data communication channel, or hybrid systems that employ both on premises resources (tape and/or disk) and remote site replication and/or back-up.

Organizational Roles and Responsibilities

Define roles and responsibilities of agency personnel involved with image processing systems. It is especially important for agency records management personnel to work with their senior managers, legal counselors and information technology staff to establish policies and procedures for electronic image management. Work with system administrators to ensure that unauthorized users are not able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology (IT) managers and server administrators share responsibility for managing electronic records. Endeavor to clarify these roles, and adopt supporting procedures, training programs and compliance auditing techniques. In conjunction with system administrators, take appropriate measures to preserve data integrity, confidentiality and physical security of electronic records.

Shared Drives and Collaboration Sites

Agencies use shared (networked) drives, including collaboration sites, to store electronic records and other content such as reference and working (transient) materials – e.g., drafts and publications, which are used to produce documents and other formal communications.

Typically, shared drives contain content in a variety of formats including word processing documents, text files, scanned text records, photographic images, audio and video recordings, spreadsheets, presentations and structured databases. This content can be stored in organized file folders that are arranged in various ways – e.g., by projects, cases, institutional functions, individual employees, discussion groups, etc.

Shared drives/collaboration sites may also be used to store content associated with social network applications that agencies employ for outreach purposes and/or citizen participation in policy formulation, service program development or other collaborative initiatives. Social network content may include blogs and micro-blogs (essentially discussion streams), Wikis (group-created and edited documents) and other collaborative content [4]. Further, as agencies begin to adopt uniform, digitally-based communications platforms, these drives may capture mobile text communications, chats, digital voice recordings and/or videos of staff/citizen interactions.

Because shared drives typically feature a diversity of content, it may be difficult to apply records management principles and practices to them. They are likely to contain public records; therefore, agencies will need to address the records management challenges that arise from the use of shared drive technology. This section provides basic guidelines designed to assist agencies in addressing these challenges. The guidelines are based on information provided by NARA.

Note that shared drive technology and collaboration sites are evolving to newer forms of content management platforms that provide for integration and control of workflows, record content and associated meta-data, across office boundaries, while encompassing a variety of digital file formats. The Division anticipates that use of these enterprise-level contents and case/process management platforms will facilitate the application of the basic guidelines set forth here.

Records Management and Shared Drive Technology

A key determination that centers all planning and records management actions relative to shared drives is whether the records stored on the drives contain original, official versions or record copies. It is possible that shared drives contain only draft or working materials, which need not be retained beyond their immediate administrative uses. More likely, however, shared drives will contain both working materials and record copies of documents, publications and other official communications. In these cases, plan to apply the following records management principles and practices.

Organization

Arrange folders, sub-folders, and files so that they are associated with their corresponding records retention schedule/record series. Also consider using a file plan for organizing content on drives. You may find traditional file management techniques (classification plans) to be useful conceptual models for this purpose.

Records Scheduling/Disposition

Identify the records series that correspond to the records content of drives. Record series relate directly to agency-specific or general records retention schedules. Retain record copies of public records for the length of their designated retention periods and, at a minimum, provide for deletion of the records following the receipt of approval for the disposition action. If you maintain a mix of different record series within individual folders and files, use the longest retention period to guide your disposition actions. If you store long term (retention greater than 10 years), permanent or archival records on an electronic system, be sure to address and guard against technical obsolescence (see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats).

Be aware that normal deletion processes do not assure the full destruction of electronic records. In most cases, deletion only removes the index information that points to the records. Contact your system administrator to determine whether it would be appropriate to employ a form of secure deletion (on both online storage and back-up media), which effectively obliterates the targeted contents.

If a system is retired or converted to another platform and it becomes necessary to dispose of the storage media that housed electronic records, ensure that the media are destroyed in such a way as to obliterate any traces of the content they had contained. In this regard, State agencies must follow the policies, standards, and procedures set forth by the Office of Information Technology -- Information Disposal and Media Sanitization (09-10-NJOIT).

Meta-Data

For all content, ensure that your agency maintains basic meta-data for all items, including:

- Names of content creators/contributors
- Agency or functional attribution (organization or function responsible for the records
- Time and date of creation
- Title/Subject

Reliability and Trustworthiness

Ensure all record copies are stored in a reliable and trustworthy fashion.

1. Authenticity: Institute controls to protect against unauthorized addition, deletion, alteration, use, and concealment - for example, role-based user access controls.
2. Integrity: Implement controls, such as audit trails, to ensure records are complete and unaltered. Key considerations here include preserving:
    - The original informational contents of the records as produced by the author or process that created the record.
    - The organizational, functional and transactional context of the record, including links to related records that reflect the business, legal and regulatory circumstances in which the record was produced. In this area, maintenance of the meta-data listed above is a key.
    - The original physical and logical structure of the records and the relationships between the data elements they contain.
    - Usability: Employ mechanisms to ensure records can be located, retrieved, presented, and interpreted. Ensure you develop and maintain consistent classification schemes for records –

for example, classify by responsible office, function, and/or informational content. Also, maintain indexes that allow authorized users to locate stored records. – e.g., unique document ID's and meta-data fields such as author/submitter name, data sent/received, topic keywords, etc.

New Drive/Site Configuration

For new drives and collaboration sites, make records management and preservation integral parts of the configuration planning process and design specification by ensuring that:

1. Retention and disposition scheduling are parts of the drive/site design.
2. All records will be retrievable and usable for as long as needed to conduct agency business (i.e., for the length of their State- approved retention periods).
3. Where records must be retained beyond the anticipated life of the system, plan and budget for the migration of records and their associated metadata (index and related data) to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.
4. If records are classified as archival or designated for archival review, contact Records Management Services for further guidance on how to ensure you will be able to transfer the content to an archival facility.

With regard to records management functions, be sure the configuration planning process and design specification includes the following. Note that the functions support the generation/storage of meta-data and reliable/trustworthy content.

1. Declare records. Assign unique identifiers to records.
2. Capture records. Where applicable, provide for the import of records from other sources via manual and/or automated processes, maintaining content, context and structure as outlined previously, or link records to other related systems.
3. Organize records. Associate records with approved records schedules and disposition instructions.
4. Maintain records security. Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.
5. Manage access and retrieval. Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.
6. Preserve records. Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business and to meet State-approved retention and disposition requirements. Develop procedures to enable the migration of records and their associated meta-data to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.
7. Execute disposition. Identify and delete temporary records that are eligible for disposal in accordance with State-approved retention and disposition instructions. If applicable, identify and effectuate the transfer of archival records to a repository designated by the State Archives, based on State-approved records schedules. Apply records litigation hold or freeze on disposition actions when required.

   Note: Do not relay on system and file backup processes and media to cover electronic recordkeeping functions.

Safeguards against Technical Obsolescence

As with all forms of automated records technologies, you will need to guard against technological obsolescence. Design and implement migration and/or back-up strategies to counteract hardware and software dependencies, especially if the electronic records must be maintained beyond the anticipated life of the system used to create and/or capture them originally (risk of technological obsolescence). To successfully protect records against technological obsolescence:

1. Monitor actively and consistently for system viability and plan/act accordingly (see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats).
2. Determine if the State-approved retention period for the records will be longer than the life of the underlying system. If so, plan for the migration of the records to a new system before the current system is retired.
3. Carry out upgrades of hardware and software with the goal of retaining the functionality and integrity of the electronic records stored within the system. To maintain record functionality and integrity:
    - Retain the records in sustainable formats (by following these guidelines) until their authorized disposition date.
    - Ensure new storage media are compatible with the underlying hardware and software platforms.
    - Maintain a link between records and their meta-data through conversion or migration process.
    - If applicable, ensure that migration strategies address non-active electronic records that are stored off-line.

Organizational Roles and Responsibilities

Define roles and responsibilities of agency personnel involved with shared drives and collaboration sites. It is especially important for agency records management personnel to work with their senior managers, legal counselors and information technology staff to establish policies and procedures for electronic records management.

Work with system administrators to ensure that unauthorized users are not able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology (IT) managers and server administrators share responsibility for managing electronic records. Endeavor to clarify these roles, and adopt supporting procedures, training programs and compliance auditing techniques. In conjunction with system administrators, take appropriate measures to preserve data integrity, confidentiality and physical security of electronic records.

When an employee separates from an agency, whether it is due to resignation, retirement, or termination, have a knowledgeable agency administrator(s) review the employee's account to determine which records need to be retained and what the appropriate retention periods should be, and then act accordingly.

Audiovisual Records and Transcripts

Public agencies use tape-based and electronic sound and video recording systems to document public proceedings. Such recordings are integral parts of the record keeping practices of courts, governing bodies, and various other agencies that conduct open public meetings. The recordings of agencies that receive a substantial contribution of tax dollars are considered public records. The minutes or transcripts generated from such recordings are also public records.

Officials may prefer to transcribe recorded audio portions of proceedings onto written documents, which, in turn, can be scanned and stored on electronic systems and/or stored on long term microfilm or high-quality, acid-free paper (see Scanned Images of Textual Records above and N.J.A.C. 15:3-2.7 and 3-3 et seq. for microfilm and paper storage standards).

Verbatim transcriptions or approved summaries of the audio recordings of public proceedings are considered the official or "record copies" of the proceedings. Requirements for generating transcriptions or minutes from recording devices and records retention requirements for the original tape or digital recordings vary according to the type of public proceeding, and are typically spelled out in approved records retention schedules.

State schedules cover a variety of venues including: judicial proceedings such as trials and hearings; meetings of public officials like school boards, governing bodies, state and local agencies and commissions; meetings of public officials pursuant to the Municipal Land Use Law including planning and zoning boards of adjustment; and hearings with public testimony offered to State agencies to help establish formal policy.

In all cases, once a recording of a public proceeding has been created, whether voluntarily or in compliance with statutory requirements, it becomes subject to retention and destruction provisions of State law. Accordingly, identify the records series to which recordings/transcriptions correspond, and retain record copies for the length of their designated retention periods. For digital content, at a minimum, provide for deletion of the records following the receipt of approval for the disposition action.

Be aware that normal deletion processes do not assure the full destruction of imaged records. In most cases, deletion only removes the index information that points to the records. Contact your system administrator to determine whether it would be appropriate to employ a form of secure deletion (on both online storage and back-up media), which effectively obliterates the targeted contents.

If a system is retired or converted to another platform and it becomes necessary to dispose of the storage media that had housed electronic records, ensure that the media are destroyed in such a way as to obliterate any traces of the content they contained. In this regard, State agencies must follow the policies, standards, and procedures set forth by the Office of Information Technology -- Information Disposal and Media Sanitization (09-10-NJOIT).

If you plan to store tape-based or digital versions of hearings in addition to or in place of transcriptions, follow the best available commercial or public standards and guidelines for the tape or electronic media. NARA offers more detailed guidance in this area. If you plan to store audiovisual records in digitized format within your general information technology complex, employ the techniques discussed in the Shared Drives and Collaboration Sites section above. Also, see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats.

Geospatial Records and Geographic Information Systems (GIS)

Digital geospatial records and digital cartographic data files are associated with Geographic Information Systems (GIS). State laws may continue to limit the use of this technology for official records keeping or record copy purposes. Contact RMS for guidance with respect to specific cartographic content that you seek to convert to automated formats.

Notwithstanding legal limitations on the use of GIS, application of the technology for operational purposes may yield many benefits for public agencies and the citizens they serve. For example, the use of digital parcel information GIS can help foster: streamlined, timely, responsive and efficient processing of information (such as tax mapping and associated tax assessment work); improved security (via tailored access restrictions and use of back-up/recovery to guard against loss or defacement of records); improved land use planning, decision-making and revenue collection through the use of standardized, accurate shared data; and improved public safety operations via timely access to critical infrastructure information.

The use of geospatial data and GIS continues to be an evolving area. Monitor the work of standards committees at the State and national levels for media, file format and meta-data (see System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats). Most of the general records management practices for Shared Drives and Collaboration sites discussed above apply to the management of GIS systems, irrespective of the underlying technology

Structured Databases

Structured databases are groupings of logically related data fields that are defined, stored, retrieved/used, and maintained within a software complex, or database management system, in support of specific organizational functions. These functions can be simple list management applications or agency-wide/Enterprise level activities such as budget and fiscal management, revenue recording and financial reporting, human resources and benefits management, payroll, tax and collections administration, motor vehicle/driver registry, data warehouses, etc. Structured databases may support other records systems – e.g., provide index/inquiry management for a digital imaging system, serve as official systems of record for key functions/transactions, or provide both support and official record keeping services. Therefore, databases may be the hubs of institutional business activity and/or be components in any of the electronic records systems touched upon in this section -- from electronic mail systems, to image processing systems, through to shared drive complexes and GIS.

Because of their functional diversity, it may be difficult to apply records management principles and practices to structured databases. Like shared drives, however, they are likely to contain public records. Therefore, agencies will need to address the records management challenges that arise from the use of the technology. This section provides basic guidelines designed to assist agencies in addressing these challenges.

You will note that many of the techniques suggested for shared drive/collaboration site management apply to structured databases.

Records Management and Structured Databases

A key determination that centers all planning and records management actions relative to structured databases is whether the records stored in them contain original, official versions or record copies. If a database contains only support information such as abstracts of underlying, complete records stored in image or other formats, the information need only be retained for the length of time it has active administrative value. If the database contains record copies of transactions or other events, plan to apply the following records management principles and practices.

Organization

Arrange directories, tables, folders, sub-folders, and files so that they are associated with their corresponding records retention schedule/record series.

Records Scheduling/Disposition

If possible, identify the records series that correspond to the records content on the database – e.g., pension case file, complaint case file, permit application record, payroll disbursement, tax payment transaction, etc. Record series relate directly to agency-specific or general records retention schedules. Retain record copies of public records for the length of their designated retention periods and, at a minimum, provide for deletion of the records following the receipt of approval for the disposition action. If you maintain a mix of different record series within individual directories, folders and files, use the longest retention period to guide your disposition actions. If you store long term (retention greater than 10 years), permanent or archival records on an electronic system, be sure to address and guard against technical obsolescence (see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats).

Be aware that normal deletion processes do not assure the full destruction of imaged records. In most cases, deletion only removes the index information that points to the records. Contact your system administrator to determine whether it would be appropriate to employ a form of secure deletion (on both online storage and back-up media), which effectively obliterates the targeted contents.

If a system is retired or converted to another platform and it becomes necessary to dispose of the storage media that housed electronic records, ensure that the media are destroyed in such a way as to obliterate any traces of the content they had contained. In this regard, State agencies must follow the policies, standards, and procedures set forth by the Office of Information Technology -- Information Disposal and Media Sanitization (09-10-NJOIT).

Meta-Data

- For all content, ensure that your agency maintains basic meta-data for all items, including:
- Names of record creators and editors (those who modify database records)
- Dates/times of entries, modifications and deletions
- Agency or functional attribution (organization or function responsible for the records
- Time and date of database creation and update
- System level meta-data
- Data element descriptions (via data description language and/or data dictionaries)
- Entity relationship diagrams

- Database management system name and version(s)
- Operating system name and version(s)

Reliability and Trustworthiness

Ensure all record copies are stored in a reliable and trustworthy fashion.

- Authenticity: Institute controls to protect against unauthorized addition, deletion, alteration, use, and concealment - for example, role-based user access controls.
- Integrity: Implement controls, such as audit trails, to ensure records are complete and unaltered. Key considerations here include preserving:
    - The original informational content of the records as produced by the author or process that created the record.
    - The organizational, functional and transactional context of the record, including links to related records that reflect the business, legal and regulatory circumstances in which the record was produced. In this area, maintenance of the meta-data listed above is a key.
    - The original physical and logical structure of the records and the relationships between the data elements they contain.
    - Usability: Employ mechanisms to ensure records can be located, retrieved, presented, and interpreted. Ensure you develop and maintain consistent classification schemes for records – for example, classify by responsible office, function, and/or informational content. Also, maintain indexes that allow authorized users to locate stored records. – e.g., unique document ID's and meta-data fields such as creator/editor name, date record created/edited, etc.

New Database Management Systems

For new systems, make records management and preservation integral parts of the configuration planning process and design specification by ensuring that:

1. Retention and disposition scheduling are parts of the drive/site design.
2. All records will be retrievable and usable for as long as needed to conduct agency business (i.e., for the length of their State-approved retention periods).
3. Where records must be retained beyond the anticipated life of the system, plan and budget for the migration of records and their associated meta-data (index and related data) to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.
4. If records are classified as archival or designated for archival review, contact Records Management Services for further guidance on how to ensure you will be able to transfer the content to an archival facility.

With regard to records management functions, be sure the configuration planning process and design specification includes the following. Note that the functions support the generation/storage of meta-data and reliable/trustworthy content.

1. Declare records. Assign unique identifiers to records.
2. Capture records. Where applicable, provide for the import of records from other sources via manual and/or automated processes, maintaining content, context and structure as outlined previously, or link records to other related systems.

3. Organize records. Associate records with approved records schedules and disposition instructions.
4. Maintain records security. Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.
5. Manage access and retrieval. Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.
6. Preserve records. Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business and to meet State-approved retention and disposition requirements. Develop procedures to enable the migration of records and their associated meta-data to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.
7. Execute disposition. Identify and delete temporary records that are eligible for disposal in accordance with State-approved retention and disposition instructions. If applicable, identify and effectuate the transfer of archival records to a repository designated by the State Archives, based on State-approved records schedules. Apply records litigation hold or freeze on disposition actions when required.

   Note: Do not relay on system and file backup processes and media to cover electronic record-keeping functions.

Safeguards against Technical Obsolescence

As with all forms of automated records technologies, you will need to guard against technological obsolescence. Design and implement migration and/or back-up strategies to counteract hardware and software dependencies, especially if the electronic records must be maintained beyond the anticipated life of the system used to create and/or capture them originally (risk of technological obsolescence). To successfully protect records against technological obsolescence:

1. Monitor actively and consistently for system viability and plan/act accordingly (see the System Sustainability Guide and Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats).
2. Determine if the State-approved retention period for the records will be longer than the life of the underlying system. If so, plan for the migration of the records to a new system before the current system is retired.
3. Carry out upgrades of hardware and software with the goal of retaining the functionality and integrity of the electronic records stored within the system. To maintain record functionality and integrity:
   - Retain the records in sustainable formats (by following these guidelines) until their authorized disposition date.
   - Ensure new storage media are compatible with the underlying hardware and software platforms.
   - Maintain a link between records and their meta-data through conversion or migration process.
   - If applicable, ensure that migration strategies address non-active electronic records that are stored off-line.

Organizational Roles and Responsibilities

Define roles and responsibilities of agency personnel involved with shared drives and collaboration sites. It is especially important for agency records management personnel to work with their senior managers, legal counselors and information technology staff to establish policies and procedures for electronic records management.

Work with system administrators to ensure that unauthorized users are not able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology (IT) managers and server administrators share responsibility for managing electronic records. Endeavor to clarify these roles, and adopt supporting procedures, training programs and compliance auditing techniques. In conjunction with system administrators, take appropriate measures to preserve data integrity, confidentiality and physical security of electronic records.

When an employee separates from an agency, whether it is due to resignation, retirement, or termination, have a knowledgeable agency administrator(s) review the employee's account to determine which records need to be retained and what the appropriate retention periods should be, and then act accordingly.

Web Sites

Web sites are groupings of digital content, organized as pages, that center on and allow online access to related topics, functions and/or services via hyperlinks and other automated navigational tools. Web site contents may include various combinations of elements such as information encoded in a hyper mark-up language, style sheets, audiovisual files, application software code (executables), presentations and various types of electronic documents.

Currently, New Jersey does not develop retention schedules for web sites per se, but rather focuses on the individual documentary/transactional elements that may appear online such as reports, filing transactions, payments, etc., which are typically stored, for official record-keeping purposes, in back-end production databases and network file shares. If your agency uses web sites to store official or record copy versions of public records, basic records management requirements will apply to the content of those sites.

NARA provides guidance on categorizing and scheduling records found on web sites using the following three general groupings:

1. Web content records including: the content pages that compose the site, inclusive of the HTML markup; records generated when a user interacts with a site; and if the agency chooses to document its site, lists of the URLs referenced by site's hyperlinks.
2. Web management and operations records that document the site’s context including: web site design records; records that specify an agency's web policies and procedures by addressing such matters as how records are selected for the site and when and how they may be removed; records documenting the use of copyrighted material on a site; records relating to the software applications used to operate the site; and records that document user access and when pages are placed on the site, updated, and/or removed.
3. Web management and operations records that document the site’s structure including: site maps that show the directory structure into which content pages are organized; and application software

configuration files used to operate the site and establish its look and feel, including server environment configuration specifications.

Use the guidelines for Shared Drive and Collaboration Sites for applying general records management principles and practices to the grouping above.

Beyond basic records management considerations, it seems clear that selected preservation of web sites is needed because of the role they play in documenting the evolution of governmental functions, programs and policies. For long term retention and preservation formats see Suggested Formats and Supporting Information for Long Term Retention of Electronic Records Formats).

A Note on Enterprise Electronic Records Management Systems

As highlighted in the Electronic Mail section above, electronic records systems accommodate storage of e-mail messages, meta-data, and attachments on computer platforms that that are separate from, but linked to, the e-mail system. Electronic technology could also be employed more broadly, at the Enterprise-level, to encompass other sources of digital records managed by public agencies. That is, electronic records management could provide for the capture, classification, storage, preservation, access/use and disposition of various forms of electronic records across storage media types and office boundaries, while supporting litigation holds/research functions that locate, segregate and preserve items relevant to investigations, access requests, audits or law suits. They may provide facilities that control paper files, records centers and electronic imaging systems as well. Finally, Enterprise-level content and case/process management technologies will facilitate the application of basic records management guidelines.

RMS anticipates that these technologies will grow in functional capacity and applicability as time goes on and will have positive impacts on public records management programs going forward.

For more information on electronic system functionality and architecture, consult the standard issued by the Department of Defense -- (DoD) 5015.2-STD.

Litigation Holds, Electronic Discovery and Related Concerns

While a detailed discussion of litigation holds and electronic discovery (e-discovery) for legal proceedings is beyond the scope of this manual, a mention of the topic is warranted. Increasingly, records managers, along with information technology professionals, legal staff and agency managers will be called upon to participate in litigation holds and discovery processes. Further, these processes may parallel those employed to respond to Open Public Records Act (OPRA) requests, audits and internal investigations – all key concerns for New Jersey's public sector as well. Be aware that OPRA entails program specific formats. In all cases, consult with your legal advisors when dealing with litigation holds and e-discovery.

Put broadly, when an agency has a reasonable expectation that litigation exists or is imminent, it has an obligation to identify and preserve electronic records (e.g., e-mail, digital images, documents, spreadsheets, etc.) as well as hard copy records, which are relevant to the case.[5] The requirements for identification, preservation, and ultimately, production and presentation of relevant records are likely to

be broad. They may span multiple storage platforms such as shared drives, database stores, e-mail systems, microfilm and file cabinets. They may involve multiple individual, and/or cross multiple offices and locations. Again, OPRA requests, audits and investigations may have similar characteristics.

For reasons that will discussed in the context of the following outline, agencies that employ the records management techniques and practices discussed in this manual will be in a good position to address litigation holds and e-discovery, as well as the aligned processes of OPRA responses and producing materials for audits and investigations.

Outline of Litigation Hold Process

Legal professionals have outlined the basic steps in the litigation hold process, which is a foundational support for e-discovery. [6] Review this outline to develop an understanding of how records management is an integral part of the process.

1. Create and maintain support team – The support team responsible for handling litigation holds typically includes members representing records management, information technology, legal, human resources and line management offices.[7] To address litigation holds, consider expanding the charter of the governance team that covers records management and/or electronic records matters to include responsibility for litigation holds, as well as OPRA, audit and investigation actions.
2. Development and use of a legal hold notice – The Department of the Treasury's notice is an example of this element. Have your records management team work with you agency's legal advisors and management team to develop the notice format and distribution method. Consider using similar formats for other records-related activities such as noticing custodians in the event of an audit or investigation. For OPRA matters, see the guide for records custodians.
3. Identify/notify records custodians – Identification of custodians is part of records inventory and retention scheduling programs, as well as electronic records management processes, including meta-data management. Use this information to pinpoint records sources and responsible agencies and their custodians (for litigation holds and OPRA requests)

   Make sure the notice to custodians includes basic elements such as clear title indicating the purpose of the notice, name and authority of the issuing office, the basic subject of the notice (e.g., pending litigation), the target individuals, offices, systems and/or hardcopy sources, and the names/types of records, date ranges and response time requirements if applicable. You may wish to use the same notice format, with basic modifications, for audits and investigations.

4. Identify records -- Consider identifying, accessing and managing information about electronic and other records sources via the records management sources discussed in this manual, including records inventories, records retention schedules, meta-data libraries, data dictionaries, system documentation produced during system development lifecycles, file classification plans, records center inventory management systems and indices to electronic images. Optimally, the agency will have an Enterprise level view and control of all records sources – e.g., through the use of an Enterprise (jurisdiction-wide) electronic records-keeping and management system. More likely, however, it will be necessary to span multiple records sources using a combination of automated and manual processes.

Preserve and present records -- Your ability to copy/preserve or preserve in-place targeted content will depend upon the media and systems you use to capture and store records. Seek to procure and implement litigation hold software for electronic records and indexed records stored in central file rooms and records centers. For e-mail in particular, consider using vaulting software that automatically stores in-bound and out-bound communications independent of the creators and receivers of the messages. Also consider placing segregated/copied records in off-line systems and/or dedicated paper and electronic folders for preservation. If possible, present to the requestor with electronic records in open file formats such as those discussed in this manual, and if feasible, convert any hard copy material to the same open formats. This approach will enable you to provide all records in a consolidated, uniform fashion.

5. Monitor and manage the hold process – This involves monitoring the litigation hold through its lifecycle, including tracking of custodian compliance, communicating status and changes in the scope of the records requests, and ultimately closing out and terminating the hold order. The same types of activities may apply to audits and investigations as well. OPRA requests usually involve accelerated turnaround time windows (7 days), but still, the need to monitor and manage the requests through to completion is of paramount importance. Legal and/or human resources staff members are likely to take the lead in this area. However, records management staff and their expertise may be required to assist these staff members – e.g., by developing and implementing litigation hold work flow applications and providing records conversion services (for preservation and presentation purposes).

Electronic Records Summary

Agencies use shared (networked) drives, including collaboration sites, to store electronic records and other content such as reference and working materials – e.g., drafts and publications, which are used to produce documents and other formal communications. Most likely, shared drives contain both record copy and working (transient) materials in a variety of formats. Accordingly, agencies will need to employ records management principles and practices, such as those set forth in this section, when dealing with shared use technologies.

Chapter 8

Vital Records Management

There are two types of vital records: 1) those that contain the information agencies need to conduct their core functions; and 2) those that provide direct evidence of the legal rights and obligations of the agency and the citizens it serves.

Vital records management processes, which center on the identification and protection of vital records, are based on traditional records management activities such as inventorying, retention scheduling and files management.

Vital records management is a form of self-insurance that supports the continuity of government operations and helps to preserve the legal viability of the public sector.

Only a fraction of an agency's records are vital – perhaps ranging from 1 to 7 percent. Still, without these records, the daily operations of an agency would cease, and the public interest would be endangered because of problems such as:

- Vulnerability to litigation;
- Exposure to financial settlements or loss of revenues;
- Disruption of vital services (health and safety);
- Failure to protect the rights of the citizenry (e.g., loss of property records); and
- Loss of regulatory records and audit trails

Be sure to integrate vital records management with disaster recovery programs and continuity of operations plans. Increasingly, these programs are located under the authority of the agency's information technology operation. For this reason, it is imperative for records management staff and operational managers to work with their information technology teams to ensure that a holistic view of these interrelated programs guide decisions about how to institute vital records management.

View an example of a high-level plan template that blends elements of business continuity and disaster recovery plans.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq. 3-2 et seq., 3-3 et seq., 3-4 et seq. and 3-6 et seq.(Online Source).

Vital Records Management Program Elements

Records Classification

Knowledge of record holdings is necessary before appropriate controls for vital records protection can be instituted. Identification and analysis of record series is most easily accomplished during a routine records inventory conducted as a first step in developing a records management program, during a file audit (see Paper Files Management above) used to organize active records or during the development of computer-

based systems, especially during the planning and general design phases of the system development life-cycle.

In connection with computer-based systems, State agencies are subject to specific project review and control requirements embodied in the System Architecture Review (SAR). The SAR includes classification of the information content of systems and can serve as a foundation for vital classification. County and local agencies may wish to use the SAR as a model for their own initiatives in this area.

Published records retention schedules, which contain lists of records that exist in most public offices, are good sources for identifying vital records. They include descriptions of records, as well as instructions regarding retention and disposition for each record series listed.

In the context of records classification for vital records, there are four general categories:

1. Nonessential Records -- This type of record is listed on a records retention schedule for routine destruction in accordance with statewide guidelines. Loss of these records presents no obstacle whatsoever to restoring daily business.
2. Useful Records --These are records that, if lost, might cause some inconvenience but could be easily replaced. Loss of these records does not present any real obstacle to restoring daily business.
3. Important Records -- This category of records, although replaceable, is reproduced only at considerable expense of funds, time and labor. Loss presents aggravating but surmountable obstacles to resumption of operations, and
4. Vital Records-- These records are absolutely essential to the continuity of agency operations and/or protection of the legal rights and obligations of the agency and the citizens it services. These records cannot be lost under any circumstance.

Examples of vital government records include regularly updated information needed for daily activities such as accounts receivable, tax files (e.g., general tax records, property tax records, property ownership records, etc.), minutes of governing boards, authorities, and commissions, and standing executive orders of mayors or county executives.

Be sure to include operational managers, records professionals, audit and legal advisors and information technology staff in the records classification process.

Protection Methods

Estimating the severity of a calamity that could destroy an agency's records is a basic step in determining appropriate protection measures for vital records. This projection, along with an examination of costs of protection methods and budgetary levels, provides a basis for choosing options.

The three most commonly used ways to secure vital records are duplication/, on-site storage and off-site storage.

1. Duplication/Dispersal — Many records can be protected by simply distributing duplicate copies to one or more locations other than the central or primary building.

   Duplicates may be created in paper, microfilm or electronic media. In choosing a format, consider the volume, frequency of updates, storage environment (especially any need for special

environmental controls), storage space, equipment, software and power requirements, along with costs and budgetary levels.

Once duplicates have been created, they may be distributed or dispersed in a variety of ways. Records are often distributed to locations other than the agency's primary building as part of regular operating procedures. These dispersed records are kept for their minimum retention periods and are available to appropriate officials. For electronic content, networked based duplication or replication options may be available – through your agency and/or third party service providers, on-premises or via the cloud.

In cases where vital records are not being dispersed as part of routine procedures, special disbursal measures can be adopted solely for the purpose of vital records protection. Use of this technique has practical limits imposed by the degree of care given to records by offices that have no specific need to receive them.

2. On-site Storage -- On-site vital records considerations include the analysis and improvement of buildings or facilities, equipment and supplies, as well as the institution of procedural controls. Examples include:
   - Building -- Consider the adequacy of floor load capacity, lighting and ventilation, fire ratings of walls and doors, smoke and fire alarms, sprinklers or halon fire suppression systems, and eliminating such hazards as leakage and infestations by insects or vermin
   - Equipment-- Consider construction of fire-resistant vaults, or the purchase of cabinets or safes that meet or exceed Underwriter Laboratories specifications.
   - Underwriter Laboratories rates storage and filing equipment on the basis of interior temperature and humidity levels during various lengths of exposure to fire. As a general rule, paper begins to deteriorate at 350 degrees Fahrenheit with humidity greater than 65 percent, while the limits for magnetic tape, microfilm and photographs are considered to be 150 degrees Fahrenheit and 85 percent humidity
   - Procedures -- Consider updating vital records routinely, prohibiting food, beverages and smoking in records areas, segregating combustible material and conducting periodic electrical, building and fire inspections.

     If possible avoid over-reliance on on-site vital records protection measures. The potential for total or near total destruction of a single location in a disaster is a significant risk factor.

3. Off-site Storage – This option involves keeping vital records in a single location separate from the agency's main building. Locate the off-site storage center close enough for access, control and updating. Consider use of suitable public buildings owned by a government agency that are reasonably secure. It is important to note that whenever vital records are semi-current, they are eligible for storage in a records storage center (see Records Storage Center Operations above).

   The advantages of central, off-site storage include:

   - General effectiveness — It is less likely that an off-site storage facility, such as an off- site records storage center, will be affected by the same disaster that occurs to an agency's main building.
   - Ease of retrieval — Unlike dispersal techniques that involve distribution of vital records to a number of off-site locations, central off-site storage simplifies access.

- Ease of control — Centralized storage provides for uniform storage conditions and standardized access and security procedures and use of standardized equipment.
- Trained staff – Most often, trained records professionals manage centralized facilities with trained records professionals to administer the facility.

Program Coordinator and Vital Records Team

For agencies that have already established a records management program, the records manager is an appropriate choice for coordinating and managing the vital records program. Information technology professionals are also good candidates for the position.

If the vital records coordinator is not a records manager or connected on a daily basis with record-keeping systems and procedures, be sure that he/she is becomes familiar with record holdings -- by conducting records inventories and/and by interviewing representatives from the operations involved to review their record holdings.

An important part of successful vital records programs is the appointment of appropriate staff members to assist the vital records coordinator. The major function of this team of agency officials is to aid the coordinator in identifying vital records and to institute appropriate protection regimes. Consider including experts in administration, finance, audit, law, information technology/security, and records management on the team.

Communications and Testing

Because identifying vital records and selecting appropriate protection measures is necessary to prevent loss of critical information in the event of disaster, it is important for the vital records coordinator to communicate policy and procedures to all offices and enlist their active participation and support.

Consider publishing a vital records manual or incorporating a vital records section into your official policy and procedures documents, as well as conducting periodic seminars for officials and operational staff. If you operate within a smaller agency consider using a more informal procedure, such as a vital records master list.

Best practice is to test the vital records program periodically through simulations to ensure that protection methods are operating as intended and that vital records can be reproduced from duplicated/disbursed sources. At a minimum, review the program annually to identify areas requiring updates.

Vital Records Management Summary

Vital records management programs are instituted to prevent the loss of information critical to the daily operations of agencies during a calamity or to reestablish services afterward, as well as to ensure the continual availability of records that document the rights and obligations of agencies and the citizens they serve.

It is imperative that agencies integrate vital records management with disaster recovery programs and continuity of operations plans. The vital records program itself includes several interrelated elements

including vital records classification, choice/use of protection methods and procedures, assignment of the program coordinator and team, communications process and testing.

Chapter 9

Disaster Prevention and Recovery

From a records management perspective, disaster prevention and recovery involves the on-going protection of vital records and recovery of these records following a catastrophic event such as a computer system crash, security breach or terrorist attack, or following massive damage to agency facilities due to a disaster such as a flood, fire or earthquake.

Be sure to integrate disaster prevention/recovery with vital records management and continuity of operations plans. Increasingly, these programs are located under the authority of the agency's information technology operation. For this reason, it is imperative for records management staff and operational managers to work with their information technology teams to ensure that a holistic view of these interrelated programs guides decisions about how to institute vital records management.

This section supplements and amplifies information found in the State's administrative rules.

View an example of a high-level plan template that blends elements of business continuity and disaster recovery plans.

Rules and procedures that apply to this area: N.J.A.C. 15:3-1 et seq. 3-2 et seq., 3-3 et seq., 3-4 et seq., 3-4.11, and 3-6 et seq. (Online Source)

General Considerations

Effective disaster prevention/recovery requires proper on-site and off-site storage facilities. Align the scope of plans, and the specific coverage techniques adopted, with risks relative to the loss of records stored in vital records systems. This includes consideration of likely threats to the systems and the impacts of lost records in areas such as revenue intake, the rights/obligations of the government and its citizenry, security/confidentiality, and continuity of essential services for public health and safety. Assess whether the records can be reconstructed via other sources and determine the costs associated with guarding against records loss. Determine the maximum time frame that can be tolerated for recovery (recovery point objective) and how current restored vital records must be – e.g., up to the minute, from last back-up, from last meeting cycle, etc. (recovery point).

Balance the costs of disaster prevention/recovery programs with the likelihood and impacts of records losses. Risk assessments may help agencies determine the period of time within which systems, applications or functions must be recovered after an outage, and the economic feasibility of various recovery options.

Disaster Prevention Services

Disaster prevention efforts are restricted to vital records protection because records salvage techniques are expensive and time consuming, and therefore, are feasible for non-vital records holdings.

There are two basic disaster prevention services:

1. On-site and off-site storage – This includes the use of storage facilities or on-site areas that protect against damage or destruction from fire, water and other disasters, fluctuations of temperature and humidity, infestation by pests and vermin, and pollution.

   For computerized records and database systems, work with your information technology team to obtain off-site back-up and/or replication of vital records that are stored in digital format.

2. Safeguarding privacy and security of records — This is accomplished through creation of access authorization procedures and institution of theft prevention measures.

Although there can never be an absolute guarantee against destruction from a disaster, vital records protection can provide a cost-justifiable strategy to minimize the effects of a calamity. Time and money spent to prevent a records disaster will always be less than the cost of a salvage operation.

Recovery Operations

Despite the steps taken to prevent disaster, systems may fail and records will occasionally be damaged. Plan to recover vital records that have been impacted by a disaster. Both hard copy and computerized records will be involved.

While a full discussion of recovery operations for computerized systems are beyond the scope of this presentation, generally, there are several options to consider. You may install redundant systems at an alternate site which become fully operational when the main system fails, with restoration of records from off-site back-up's, or use of full failover coverage with records that have been replicated to the alternate site in real time (fail over protection). You can arrange for installation of computing equipment in a fully appointed computer room using back-up's to recover once the site is made operational (cold site). Also consider the use of third party cloud based computer platforms for back-up, replication and/or fail over coverage.

Hard Copy Records Recovery

Once conditions become favorable for records deterioration, reversing damage becomes more difficult as time goes on. For example, mold will grow on wet paper within 48 hours. Be aware of the following if you must conduct a salvage operation

1. Building inspection — As soon as possible after fire, flood, explosion or other calamity, have officials with expertise in electrical, building and fire safety examine affected facilities for potential hazards and certify their safety.
2. Communications Center — In some cases, it may become necessary to set up temporary location in the immediate vicinity of the salvage operation with telephones, walkie-talkies and/or wireless communications devices.
3. Recovery Coordination — Establish lines of authority and responsibility in a clear fashion. Designate the following:
   - Coordinator – Assign an appropriate official to oversee recovery efforts.

- Departmental Liaisons – Assemble officials with custody of records damaged in the disaster to aid in identification of records.

4. Logistical Support – Be aware that staff and equipment will be needed to conduct a records salvage operation successfully. Logistical elements include:
   - Employees – Various support personnel may be required to assist in the salvage operation, including truck drivers, sanitation workers, local police and fire officers, and building maintenance workers.
   - Equipment and supplies – The nature of these items will depend upon the type of records disaster and can include temporary lighting, communications, transportation, tables, containers, and chemicals.
   - Consultants – Contract professionals may be needed to assist in salvage operations. These may include records analysts to identify retention requirements and authorize legal disposition, and an archivist to treat salvageable records or identify future conservation needs. In some instances, a contract vendor may be required to execute one or more of the salvage methods highlighted in the next section.

Salvage Methods

The coordinator, departmental liaisons and consultants begin to salvage records by:

1. Determining if a list of the records involved in the disaster exists, and where the list is kept.
2. Determining if there is an off-site storage location with duplicate records (e.g., electronic back-up files, dispersed paper duplicates, microfilm copies in a records storage center, etc.).
3. Examining salvageable records to determine:
   - What can be saved.
   - What can be destroyed through the Request and Authorization for Destruction process. Submit requests on-line (authorized users only).

   In either of these cases, the identification of record series and their corresponding retention and disposition requirements forms the basis for decisions to save or destroy.

4. Packing and labeling of salvageable records to ensure continuing identification of the records.

After these steps have been taken, identify appropriate methods for salvaging vital records. Recommendations depend upon the nature of the records disaster:

1. In either of these cases, the identification of record series and their corresponding retention and disposition requirements forms the basis for decisions to save or destroy.
   - Fast drying -- A blueprint or photographic dryer can be used for small quantities of wet records. To prevent scorching or curling, run documents through several times at a low temperature setting.
   - Slow drying -- A photocopy dryer can be used. It is similar to a blueprint dryer, but removes moisture more slowly and can generally accommodate larger documents.
   - Space drying --Spreading records on tables or floors in a room with fans circulating warm, dry air at slow speed can remove moisture from larger quantities of wet records. Salvaging water damaged records by this method requires an area large enough to accommodate the records and involves turning the records periodically.

- Freeze-drying -- This is a process for drying substances by freezing them first and then going directly from solid to gas in a high vacuum at a low temperature. This minimizes water damage. Plastic milk crates are ideal containers for packing waterlogged records, because they readily allow for evaporation. After packing, acquire freezer space. Arrangements may then be made with a private vendor to freeze-dry the records.
- Blotting --Bound volumes require special drying, which includes placing them on end with covers spread apart and pages interleaved with blotting or absorbent paper that must be changed frequently. After the bindings become partially dry through exposure to air, use wax paper jackets to allow flat storage with closed covers. Next, stack volumes with blotters under and between them with light pressure applied to flatten sheets and prevent warping of covers.
- Film salvage -- Keep water-soaked film wet to prevent it from sticking together. Remove dirt and debris from film gently to avoid abrasion. Store film in clean water. Rinse clean, wet film in a solution to harden the emulsion (image forming layer) before it is dried.

In those instances where mold has begun to grow on wet records, as soon as the records have been dried, spray the records with a thymol-trichlorethylene.

Note that drying alone may not be enough to preserve certain records. Assistance may be necessary to duplicate singed, scorched, or charred records. For example, seemingly illegible charred documents can often be read by exposure to ultraviolet light.

Other preservation and conservation strategies include:

1. Encapsulating documents in mylar or other polyester film; and
2. Microfilming or scanning damaged documents to produce durable working copies and to address long term storage (thus eliminating excessive handling of the damaged originals).

Be aware that salvageable permanent records may not be destroyed. However, if such records are inactive, you may consider postponing their complete restoration, provided their condition is stabilized, and a delay in the application of conservation techniques would not threaten the records.

Records salvage is expensive and time consuming. Ensure salvage efforts are conducted by qualified, experienced professionals. Agencies can minimize the adverse impact of disasters by implementing vital records protection programs and establishing a disaster prevention/recovery plan. Such a plan confers authority and identifies the elements of a records salvage operation before a calamity strikes.

For additional information on salvage operations, access the National Archives and Records Services' guidelines.

Disaster Prevention and Recovery Summary

Disaster prevention and recovery involves the on-going protection of vital records and recovery of these records following a catastrophic event such as a computer system crash, security breach or terrorist attack, or massive damage to agency facilities due to a disaster such as a flood, fire or earthquake. The preliminary concerns include instituting a vital records protection program and providing security. Necessary elements of a salvage operation include a building safety inspection immediately following the disaster, the

establishment of a communications center, the appointment of a recovery coordinator and appropriate departmental liaisons, and obtaining logistical support which includes necessary employees, equipment and supplies, and consultants.

Use records retention schedules to help determine which records to salvage or destroy.

Chapter 10

System Sustainability Guide

On an annual basis, for each automated record system your agency maintains, address the following factors and considerations, and when appropriate, develop a migration/conversion strategy to assure that the public records involved are preserved in accordance with State of New Jersey retention and disposition policies set forth in approved records retention schedules.

Sustainability Factors

1. Technical

   Indicate the extent to which the core technology (e.g., operating system, database management system, network, file formats, etc.) is used/supported in the broader marketplace.

   - Is the technology widely used/supported?
   - Is it based on proprietary (vendor specific) or open technology?
   - Are the underlying application system software and file formats documented?
   - Is the business application involved based on Cloud computing, including Software-as-a-Service, Platform-as-a-Service and/or Infrastructure-as-a-Service? If so, is there a robust market place with several contractors who can provide the application services on a sustained basis?
   - Is there an imminent risk of technical obsolescence (within three years)?

2. Support

   Is there availability of contractor and/or knowledgeable in-house maintenance support for the core system components in the next three years?

3. Budget

   Will there be sufficient funding for support and necessary system upgrades in the three year time frame?

Sustainability Risk Matrix

Indicate the risk levels associated with severe degradation or failure in each of the three areas above – from low to high for each area, in a three year period.

Factor/Likelihood of Severe Degradation or Failure	Low	Medium	High
Technical			
Support			
Budget			

Migration Strategy

If any of the factors on the matrix above registers as High, determine how your agency will ensure that the informational and records contents of the system survive from one technological generation to the next.

The strategy may include any, or a combination of the following:

1. Preserve the original technology used to create or store the records through an in-house support arrangement.
2. Emulate the original technology on a new technology platform(s).
3. Migrate the software necessary to retrieve, deliver, and use the records to another platform.
4. Migrate the records to a new system and up-to-date format.
5. Convert the records to another open format.
6. Other (specify)

**Consider using the Suggested Formats and Supporting Information for Long Term Retention of Electronic Records when planning for and executing system migrations.

You may also find the State of Tennessee's approach to sustainability, which focuses strongly on file formats and specific storage platforms, to be useful.

RMS Review of Migration Strategies

If you wish to RMS' written review of your migration strategy for use in planning and supporting your migration process, send your sustainability assessments, migration strategy and supporting material to RMS.

Suggested Formats and Supporting Information for Long Term Retention of Electronic Records (Selected File Types)

Use these guidelines when addressing management of records scheduled to be retained for 10 years or more. Generally, these guidelines will prove helpful in planning for the transfer of electronic records to long term electronic storage or digital archival facilities. Use of the suggested formats and supporting information may also ease migration and conversion of records content to different production information systems over time.

By and large, the guidelines stress the use of open systems formats. However, it is important to highlight that use of native (product specific) formats within sustainable automated systems is of vital importance as well. As long as agencies provide for controlled and sustained access to and preservation of electronic records within native operational systems, the foundations for long term retention remain in place.

The guidelines are tentative. They draw heavily from documents and information posted by the National Archives and Records Service (NARA) [8] and North Carolina State Archives. Also, the Library of Congress

posts valuable discussions on system sustainability factors, which provide conceptual foundations for understanding the guidelines.

Notwithstanding the emphasis on the above-referenced sources, the work of various state records management and archives programs inform this discussion. Indeed, with respect to the broad contours of long term retention practices and the conceptual foundations for electronic records management programs, there appears to be overarching consensus regarding the need for approaches such as those outlined herein. (View to a selected list of links to state government electronic records policies, procedures and guidelines.)

Be aware that the guidelines are subject to change, pending the receipt of further guidance from the New Jersey State Archives, including guidance on media and meta-data requirements, relative to records transfers to archival facilities. In the interim, if you wish to review a more detailed treatment of meta-data and digital media, access the State Minnesota's suite of guidelines, as well as North Carolina's guidelines.

Electronic Mail and Attachments

Formats

Consider converting long term e-mail messages to one of the following formats.
Have users select and store long term e-mail content in one of these formats, or migrate selected e-mail/mail boxes via programming or bulk import to one of the formats.

1. Standardized Generalized Mark-up with Document Type Declaration (SGML/DTD)* – This format uses tags to define records structure (from/to, date, message body, etc.) and style (formatting) information.
2. Extensible Mark-up Language with Document Type Definition (XML/DTD)* – This format also uses tags to define records structure and style information.
3. Text format (ASCII or UTF-8, .txt) – This format does not migrate records structure and formatting information. Exercise caution when using this format if such information is important to interpreting the context of messages and determining their authenticity.

   *Mark up languages are designed to be self-contained and portable (i.e., independent of any proprietary system).

For attachments, consider use of the following:

1. Portable Document Format (PDF)/A-1a or A-1b (.pdf) (A-1a is preferred; see information provided by the Library of Congress on PDF/A, ISO 19005-1) – Use this format for word processing documents, spreadsheets and presentations. Note that the PDF/A1a will render content as it appeared in its native file format, but will not translate elements such as spreadsheet formulas.
2. For older material stored in PDF format, consult NARA's guidelines.
3. Standardized Generalized Mark-up with Document Type Declaration Type Declaration (SGML/DTD) – Use for a wide variety of file types.
4. Extensible Mark-up Language with Document Type Definition (XML/DTD). Use for a wide variety of file types.

5. Open Document Formats (.odt for documents; .ods for spreadsheets; and .odp for presentations) – This is an open systems format that can be used with different word processing and office productivity programs.
6. Text format for documents produced by text editor programs (ASCII or UTF-8; plain text or tab delimited = .txt or comma delimited = .csv)

Be aware that staging e-mail and associated content for migration and conversion may involve extracting selected e-mail content or entire e-mail boxes to an intermediate bulk format such as the Microsoft® Outlook® Personal Storage Table (.pst) or MBOX family of formats (or successor formats) or different e-mail systems.

Documentation

NARA provides helpful information in this area.

In all cases, endeavor to maintain documentation that identifies the application software used to create the records and the version(s), and the operating system and version(s). Take care to maintain meta-data such as names of senders/receivers, dates (created, sent, received), and versions if applicable.

Maintain the following supporting information when scheduling permanent e-mail records.

1. Technical documentation
   - Operational guidelines, work instructions, workflow manuals, process maps, or other documentation of business processes affecting the records
   - Systems documentation, if applicable (e.g., user manuals, database schemas, data dictionaries, design documents, requirements specifications)
2. Documentation of historical or planned system upgrades, data migrations, and other changes to the system or records
3. Documentation of quality control inspections performed on the records
4. File format information
   - File format(s) and version(s)
   - Software/hardware used to create the record, including version
   - File format conversion/migration procedures, if applicable
5. Finding aids
   - Finding aids, meta-data, indexing and retrieval systems
   - Search technologies used by the agency
6. Documentation of protection mechanisms
   - Computerized mechanisms used to safeguard the records against unauthorized access, alteration, or deletion such as passwords, digital signatures, and/or encryption (if e-mail content is to be transferred to a long term facility, removal of protection mechanisms may be required)

Scanned Images

For scanned images of textual records that have long term retention requirements, consider applying the following guidelines. Consult NARA's bulletin on the subject as well.

File Formats for Raster (Bit Map) Images

Use any of the following formats:

1. Tagged Image File Format (.tif or.tiff)
2. Graphics Interchange Format (.gif)
3. Joint Photographic Experts Group (JPEG) 2000 or JPEG (.jp2, .jpg, or.jpeg)
4. Portable Network Graphics (.png)
5. PDF/A-1a

Scanning Resolution

Employ minimum scanning resolution and pixel per inch (bit) depth for potential archival preservation and long term use:

1. Bitonal (1-bit) scan at 300-600 ppi. Use this resolution for documents that consist exclusively of clean printed type possessing high inherent contrast (e.g., laser printed or typeset on a white background).
2. Gray scale (8-bit) scan at 300-400 ppi. Use this resolution for textual documents of poor legibility, because of low inherent contrast, staining or fading (e.g., carbon copies, thermofax, or documents with handwritten annotations or other markings), or that contain halftone illustrations or photographs.
3. Color (24-bit RGB [Red, Green, Blue]) scan at 300-400 ppi. Use color mode (if technically available) for text containing color information important to interpretation or content.

Documentation

Maintain the following supporting information when scheduling permanent scanned records:

1. Imaging system and version(s) (i.e., application software and storage system)
2. Operating system and version(s)
3. Records Management Application (if applicable) and version(s)
4. Image file format(s) and version(s)
5. Image quality specifications (i.e., resolution, pixel (bit) depth, compression technique)
6. Structure of image header if applicable (e.g., .tiff, .png, .gif, etc.)
7. Meta-data (e.g., for each document, date/time of creation, organization/person responsible for document, version number, structure of the file header
8. Finding aids, indexes, and other information used to retrieve the records
9. The Optical Character Recognition (OCR) versions of the images (i.e., additional files enabling full text searches linked to the appropriate scanned image), if applicable

Digital Photographic Records

For digital photographs produced from digital cameras and scanned images of photographic prints, slides, and negatives, use the following guidelines and consult NARA's general information.

File Formats

Use the following formats:

1. Tagged Image File Format (.tiff, .tif).
2. JPEG File Interchange Format (.jfif, .jpeg) -- Create JPEG files using at least high quality compression settings (no loss of fidelity).

Resolution

Use the following levels as applicable:

1. Continuous-tone gray scale or color raster images, 8-bit or 16-bit per channel.
2. Color images in RGB (Red Green Blue) color mode as 24-bit or 48-bit color files.
3. If using a digital camera, captured images at 6 megapixel files or greater with a minimum pixel array of 3,000 pixels by 2,000 pixels.
4. Scan photographs as minimum 3,000 line files to approximate a 6 megapixel file according to the following image size and resolution guidelines:
    - Scan an 8" x 10" original (print, slide or negative) at 300 dpi to produce a file that is 2,400 x 3,000 pixels.
    - Scan a 4" x 5" original (print, slide or negative) at 600 dpi to produce a file that is 2,400 x 3,000 pixels.
    - Scan a 35-mm original (print, slide or negative) at 2100 dpi to produce a file that is 2,000 x 3,000 pixels.

Documentation

Maintain documentation that reflects:

1. Meta-data – e.g., unique photograph identification number and/or file name. (Maintain agency naming conventions if applicable.)
2. Captions or narrative text describing each individual image
3. Photographer--the full name and organization of the photographer, if available.
4. Copyright – description of any restrictions on the use of that image because of a copyright or other property rights, with beginning and ending dates if applicable.
5. File format and version
6. Bit depth, compression and image size (see Resolution above)
7. Image source --the original device used to capture the images (e.g., the make and model of the digital camera)

Digital Drawings

For technical drawings – e.g., architectural and engineering drawings, produced via automated applications like computer-aided design packages, consider using the following guidelines for long term retention.

File Formats for Vector Images (Containing Mathematically Derived Graphics or Shapes)*
*If your system employs raster formats, see the file format and documentation guidelines for raster images above. Also, review Geospatial Records below.

Use any of the following formats:

1. Scalable Vector Graphics 1.1 (.svg)
2. AutoCAD® Drawing Interchange Format (.dxf)
3. PDF/A-1a

Maintain the following supporting information:

1. Application system and version(s) (i.e., application software and storage system)
2. Operating system and version(s)
3. Records Management Application (if applicable) and version(s)
4. File format(s) and version(s)
5. Meta-data (e.g., for each document, date/time of creation, organization/person responsible for document, version number, structure of the file header
6. Finding aids, indexes, and other information used to retrieve the records

Structured Databases

Structured databases are implemented via different data models with the most prevalent being the relational model (series of related fields grouped into related tables linked by common fields or keys). Increasingly, however, database platforms make use object-oriented technologies that integrate diverse data items like geospatial data, audio-video content and digital images.

NARA provides general information on this subject.

Formats

For long term retention of structured databases, consider taking scheduled snapshots or executing complete exports to one of the following formats:

1. Delimited Flat File(.txt, comma or tab delimited)
2. Tagged format file such as .xml

**In this area, North Carolina points to the availability of Software Independent Archiving of Relational Databases (SIARD) format, which is XML based.

Documentation

In all cases, provide documentation that lists the data model and describes the underlying data (data description language and/or dictionary or comparable tool).

Other valuable documentation includes:

1. Key process flow descriptions (to help bolster understanding of the uses of the data)
2. Application system and version(s) (i.e., application software and storage system) if appropriate
3. Operating system name and version(s)
4. Database management system name and version(s)
5. Input sources/documents
6. Outputs (reports, extracts, exports, etc.)

7. Entity relationship diagram (data elements, objects and tables)

Web Sites

North Carolina points to the availability of a web archive format, WARC, which it employs within the context of web crawling/harvesting operations using the open source Heritrix tool and Archive-It service. Currently, there is no comparable arrangement in New Jersey. Hence, agencies may wish to periodically create and store snap shots of their sites using the PDF/A-1a. Be aware that this approach will not preserve the dynamic elements of web sites.

Geospatial Records

Digital geospatial records are digital cartographic data files that are typically parts of Geographic Information Systems (GIS). This appears to be an evolving area. The best advice to follow here, as with most automated records systems, is to employ technologies that follow recognized national standards. NARA lists several standards. However, best practices for long term preservation of geospatial data sets may be evolving more rapidly within the context of state government archival programs. You may find it helpful to review the shape file format originally designed by the Environmental Systems Research Institute (ERSI) that includes the .shp (main shape file), .shx (index file), .dbf (table containing feature attributes) extensions, along with several optional files (see the Library of Congress overview of the format). Also, you may find the proposed geographic meta-data guidelines from The Federal Geographic Data Committee helpful. North Carolina references both items in its file format guidelines.

Audiovisual Records

For long term storage of electronic audiovisual records, consider applying the following guidelines. NARA provides information on resolution and documentation.

File Formats

- Broadcast WAVE Format LPCM and WAVE Format WAVE Format LPCM (.wav)
- AIFF (uncompressed,.aif, .aiff)
- Standard MIDI (.mid, .midi)
- Windows®Media Audio WMA (. wma)
- MPEG3 (.mp3)
- MP4 AAC (.m4a)
- NARA also offers additional guidance on audiovisual formats.

Documentation

Maintain documentation that reflects:

1. Meta-data – e.g., unique identification of event and/or file name. (Maintain agency naming conventions if applicable.)
2. Narrative text describing each event
3. Administrative agency responsible for the event
4. Copyright – description of any restrictions on the use of the recording because of a copyright or other property rights, with beginning and ending dates if applicable.
5. File format and version

Chapter 11

Feasibility Study Outline Overview

This Records System Feasibility Study Guideline provides a structured format for documenting current records system problems/opportunities, and for analyzing/choosing records system alternatives.

The Guideline consists of six interrelated sections: Current System Review

Success Factors/Statement of Needs

Preliminary Evaluation Matrix Alternate System Specification Alternate System Analysis
Final Evaluation and Alternative System Choice

Collectively, the six sections address the technical, operational and economic dimensions of current and alternate records management system feasibility.

The Guideline does not emphasize a specific technology. Rather, it focuses upon objective analysis of current records systems, the development of a problem statement and general statement of needs, and analysis of various system alternatives. Subsequent to conducting feasibility studies, an agency may well find that automated alternatives are not feasible or are unnecessary.

1.0 Current System Review

1.1	General Overview
1.1.1	List the agency's name (Department, Division, Bureau, etc.).
1.1.2	Describe the agency's mission and objectives.
1.1.3	List the records series that are being targeted for conversion to an alternate format.
1.1.4	Describe the organizational function(s) that the records series supports.
1.1.5	Specify the deficiencies of the current records system. For example:
	Integrity problems
	Non-availability of records/inability to integrate and share information/records
	Inaccuracy
	Lack of space
	Lack of security
	Inadequate access speed
	Lack of integration with information architecture
	Processing delays

Records deterioration High cost

Insufficient capacity (disk storage, read/write drives, connected users, etc.) Poor customer service

Lack of accountability

Technical obsolescence

**Whenever possible, quantify records management problems.

1.1.6 Provide a brief summary of desired performance criteria and outcomes for an alternate records system approach. Describe, in general terms, what an alternate records management system must do to address identified deficiencies.

1.2 Current System Elements

1.2.1 Provide details on targeted records series:

1.2.2 List the formal retention schedule/records series number and retention periods for targeted records series and any certifications issued by the Division of Revenue and Enterprise Services (microfilm and/or image processing).

1.2.3 Describe the detailed physical elements of the records series. Address each document type involved (correspondence, maps, drawings, checks, etc.).

1.2.4 For paper records:

1.2.4.1 Document volume (in pages, cubic feet or linear feet)

1.2.4.2 Double/single sided pages

1.2.4.3 Color and/or color coding schemes

1.2.4.4 Weight

1.2.4.5 Recording characteristics -- e.g., hand written, typed or combinations

1.2.4.6 Physical condition

1.2.5 For microform records, if applicable:

1.2.5.1 Microform format

1.2.5.2 Film width -- 16mm, 35mm, 105mm, etc.

1.2.5.3 Reduction ratio

1.2.5.4 Background density

1.2.5.5 Resolution

1.2.5.6 Film base

1.2.5.7 Image orientation -- Cine or Comic

1.2.5.8 Blipping

1.2.5.9 Frame numbering

1.2.5.10 Film thickness

1.2.5.11 Packing density

1.2.6 For computer-based records, if applicable:

1.2.6.1 Storage medium

1.2.6.2 Format – e.g., text, image or structured data

1.2.6.3 Record/file layouts, if applicable

1.2.6.4 Record types, if applicable (fixed, variable, indexed, etc.)

1.2.6.5 Underlying software product, if applicable – e.g., DBMS package, word processing product, e-mail system, image processing system, etc.

1.2.7 In narrative and/or flow chart format, describe the procedures currently used in managing and processing transactions involving the records series. If applicable, describe in general terms any relationships with data processing/office automation systems and other support systems such as off-site storage, central file controls, etc. Include data/process flows that relate to the targeted records series if possible.

1.2.8 Provide a profile of the records series usage. At a minimum, include the following:

1.2.8.1 Number and locations of users

1.2.8.2 Annotation requirements (addition of notes, attachments and authorization signatures/ initials subsequent to creation or retrieval of records)

1.2.8.3 Access/retrieval rates and patterns

1.2.8.4 Printing/copying volumes

1.2.9 Specify the disposition policy and procedures for the targeted records series.

1.2.10 Specify how the record series and document types within the record series, if applicable, are indexed

1.2.11 Indicate privacy, security and other regulatory constraints on access and use of records

**Note that generally, document based systems have different usage patterns, which impact on conversion cycles and time frames. Key questions in this area are:
-When does document access begin?

- Within one week of creation/receipt?
- Within two weeks of creation/receipt?
- Within one month of creation/receipt?

During their active stage, how often are the documents referenced – i.e., how many times are the documents accessed -- ___ times daily, weekly, monthly, or yearly?

Another useful measurement is the document reference activity ratio. This ratio can be derived by dividing the total number of document accesses (daily, monthly, or annually) by the total number of documents in the document base. This ratio is useful for determining appropriate alternatives. For example, high activity ratios coupled with large document volumes point to the need for automated retrieval systems, while large volume-low activity systems point to the feasibility of inactive records center alternatives.

1.2.11 Describe any relevant data processing/office automation interfaces in detail:

1.2.11.1 Host computer make, operating system name/version

1.2.11.2 Application system names/versions

1.2.11.3 Database base system names/versions

1.2.11.4 Office system names/versions

1.2.11.5 Programming languages

1.2.11.6 Communication network environment -- e.g., teleprocessing equipment, local area networks, switches/routers, bandwidth, circuit type, etc.

1.3 Provide details on the costs (monthly or annual) associated with the current records system:

1.3.1 Staff costs

1.3.2 Supply and equipment costs.

For example:

- File/microform related equipment
- Consumables -- various supplies including paper, guides, folders, etc.
- Office automation equipment (terminals, workstations, etc.) Furniture

1.3.3 Maintenance costs

1.3.4 Work/storage space costs

1.2.5 Overhead costs

1.3.6 Total cost based on all of the elements above

2.0 Success Factors/Statement of Needs

2.1 Specify in detail the critical success factors – desired outcomes and performance parameters – for an alternate records system. Whenever possible, quantify the parameters for the success factors. Based upon this listing, provide a narrative statement of needs.

3.0 Preliminary Evaluation Matrix

3.1 List the mandatory criteria for alternative records systems based on the success factors identified in 2.0 above. Also include budgetary constraints and any mandatory longevity and legality requirements specified by the Division of Archives and Records Management.

3.2 Indicate the desirable criteria based on identified success factors and budgetary constraints.

3.3 Develop a weighting/scoring scheme 8.

4.0 Alternate System Specification

Specify alternative system solutions. Potential areas of emphasis are listed below.

4.1 Manual (paper-based) alternatives.

For example:

- Vertical filing
- Lateral filing
- Open shelf filing with color-coding and/or bar coding
- Off-site storage
- Indexing/procedural adjustments

4.2 Microfilm alternatives.

For example:

- Roll film, standard
- Roll film, computer-assisted-retrieval Unitized film, standard
- Jackets Aperture cards
- Hybrid systems
- Unitized film, computer-assisted-retrieval

4.3 Electronic imaging.

For example:

- Engineering and oversized drawings
- Customer contact/support transactions
- System design and project management processes
- Remittance processing (for payment transactions)
- OCR/ICR for text/data capture, indexing and/or full text searching
- Bar-coding (1D/2D)
- Computer output microfilm/optical disk for report management

4.4 Data-oriented alternatives.

For example:

- Database Development
- Internet filing
- E-Commerce (electronic payment vehicles such as credit cards, electronic checks, and electronic funds transfer)
- Bulk electronic filing
- Software based filing/payment systems
- Integrated voice response
- Customer relationship management
- Hybrids

5.0 Analysis of Alternatives

5.1 Conduct a functional/technical analysis of each alternative. Seek to answer the following questions: Do the specified alternatives meet organizational requirements that are identified as success factors -- e.g., simultaneous access, security, integrity controls, storage compaction, permanent retention requirement, etc.?

5.2 Conduct an operational analysis. In light of existing and/or planned organizational capacities, seek to determine if identified alternatives can be successfully implemented. If an evaluation matrix is being used, generate weighted scores for operational features. Factors may include:

- Level of effort required for conversion to new system
- Level of maintenance required
- Inconveniences associated with conversion and new system implementation
- Time required for backlog conversion
- Extent of procedural/staffing changes
- Required facility upgrades
- Top management commitment to prolonged effort
- Staff perspectives on need for changing current system
- Staff skills

5.3 Conduct a cost analysis. Utilizing data from current contracts and recent system development efforts, detail projected costs for identified alternatives. Basic costs include:

5.3.1 One-time costs.

For example:

- Development/programming (consultants and/or OIT)
- Packaged software
- Training
- Staff time or full time equivalents for conversion/indexing
- Supplies

- Supervision
- Main configuration (equipment)
- Maintenance (hardware and software)
- Facility upgrades

5.3.2 Recurring costs (3-5 year horizon).

For example:

- Staff time or full time equivalents for conversion/indexing
- Supplies
- Supervision
- Equipment, lease/rental
- Depreciation
- Maintenance (hardware/software)
- Training
- Facility upgrades

5.4 List and analyze the benefits of each identified alternative.

5.4.1 List the intangible and/or non-monetary benefits.

For example, improved:

- Accuracy
- Integrity Access speed Security Availability Preservation
- Customer service
- Accountability/transparency

5.4.2 Quantify the tangible benefits -- e.g., dollar benefits from labor savings, increased revenue flow, space savings etc., or increases in transaction processing capacity- e.g., x more transactions processed in a given time frame.

5.4.3 Conduct a cost/benefit analysis. Compare the costs of alternatives with those of the current system or adopt a standard methodology such as net present value, payback, or return on investment to assess the desirability of the alternatives. If an evaluation matrix is being used, generate weighted scores for overall cost/benefit performance.9 (It should be noted that in some cases, policy and/or operational exigencies may require investment in system alternatives that address critical intangible and/or non-monetary benefits. In such cases, traditional cost/benefit analyses may not apply.)

6.0 Final Evaluation and Choice

6.1 Eliminate alternatives that fail to meet mandatory criteria.

6.2 Rank the remaining alternatives.

If an evaluation matrix is being used, complete the following steps:

6.2.1 Sum the weighted scores

6.2.2 Produce an overall ranking based upon aggregate weighted scores

6.2.3 If applicable, for the highest ranked alternative, consider additional factors. Additional factors may include the following:

- Availability of product
- Support issues (maintenance and software)
- Market and vendor stability
- Lack of standardization (risk of technical obsolescence)

***If the analysis reveals previously unidentified weaknesses in the highest ranked alternative, reject that alternative, record the reason for rejection, and consider the next highest alternative in light of the additional factors. Continue until an acceptable alternative is found.

6.2.4 Based upon the analyses above, choose the most desirable alternative.

End Notes

Following is a simple example of an evaluation matrix with a weighting and scoring scheme. It lists some basic features that might be used to assess the feasibility of records system alternatives. The listing is not intended to be inclusive. Also note that the matrix encompasses desirable features. Hence, it should be used after alternatives are analyzed for compliance with mandatory criteria.

Feature	Weight (Ascending scale, 1-5; 1 signifies lowest weight and 5 the highest)	Score (Ascending scale 1- 10; 1 signifies the lowest score and10 the highest)	Weighted Score (Weight times score)	Comment
Document Access Speed	3			Seconds required to retrieve and display first page of a requested document
System Integrity	4			Safeguards against lost/misfiled documents
Longevity	4			Ability to retain reproducible

				images for a minimum of 10 years and allow for migration of images to upgraded or new storage platforms
Workflow Management Capability	5			Ability to construct and maintain rules-based transaction processing
Ability to Interface with the State of New Jersey's Shared IT Architecture	4			
Compatibility With Agency's IT Architecture	5			Ability to interface with agency's legacy transaction database, and e-mail and calendaring systems
Ease of Installation/Implementation	3			
Ease of Operation/Administration	5			

The three approaches to cost/benefit analysis are based upon detailed specification and quantification of alternative system costs and benefits (also measured in monetary terms).

Net Present Value

Based upon the concept of the time value of money, NPV is a comparison of the present values of current and future cash inflows/outflows associated with identified alternatives. Present values are derived via the discounting of cash flows at a predetermined rate. NPV analyses consist of the following elements:

- Useful life of the system alternative
- Discount factor
- Discounted cash flows over the useful life of the system (annuities or single inflows/outflows; for State government purposes, cost savings/avoidance may also be considered as inflows in NPV analysis)
- Net Present Value (discounted cash inflows versus outflows); alternatives with the highest positive NPV are the most attractive

Return on Investment

In simplest terms, ROI is expressed as a ratio between benefits and costs: Total Projected Benefits/Total Projected Costs = ROI

ROI is a good tool for ranking alternatives and could be used in conjunction with present value (discounted cash flow) calculations. As the ratio between benefits and costs (ROI) increases, the attractiveness of the alternative increases.

Payback

Payback measures the amount of time required to recoup original investment amounts through the accrual of benefits. The equation for payback is: Total Projected Costs (Investments)/Projected Benefits = Payback Period

Alternatives with short (1 - 3 years) payback periods are most desirable.

Chapter 12

Conceptual Design Guideline Overview

This Conceptual Design Guideline provides a format for documenting automated record image processing and service requirements. The guideline is presented in a self-study (question/answer) format for documenting automated record image processing system/service requirements in a structured and comprehensive fashion.

Agencies may use this Guideline to develop general designs for automated record image processing systems and service contracts. Information gathered through use of this Guideline may also be incorporated into procurement documents such as Requests for Proposals (RFP).

The Guideline does not touch upon equipment configurations. Rather, it is designed for identifying operational/capacity requirements and performance levels. Properly documented requirements and performance levels will provide prospective system vendors and service providers with sufficient information to size proposed equipment configurations and service arrangements.

Certain sections of the Guideline may not be applicable to agency initiatives. For example, detailed specification of transaction work steps may not be needed if a proposed system only involves storage and retrieval of electronic images. In cases where agencies believe that specific Guideline questions are not applicable, they may mark the question as such, and provide a brief explanation of why the question is not applicable to the proposed system/service.

1.0 Document Base

The following questions are designed to gather information regarding the functional orientation and general scope (capacity) of the planned system.

1.1 What types of documents will the system involve? (Provide the name(s) of the record series involved.)

1.2 Are these documents on a state records retention schedule?

1.3 Does the agency intend to dispose of the documents after they have been scanned, indexed and committed to storage? If so, then the system must be certified by the Division of Revenue and Enterprise Services

1.4 Which retrieval mode is desired?

- Real time
- Batch (pre-fetch)
- Combinations

1.5 User Profile

- How many workstations (viewing stations, scanning stations, indexing printing stations for batch image output, etc.) must the system support?
- Where will these workstations be located?
- How are the workstations networked? (cabling-cat5/6, 100mb Ethernet, other?)

1.6 Image Volume

- How many page images will be scanned and stored over the next 5 to 7 years? (Include estimates for each document type if possible)
- If benchmark-scanning tests have been completed, what is the average byte density of a scanned page image? (Include estimates for each document type if possible)

1.7 Alpha-Numeric Data Storage (Meta-Data)

- How many fields (data elements) will be used to index a scanned image? How many fields per index record?
- How many bytes per field/index record?
- How many images will be indexed (back file, current and future volumes)?
- What is a reasonable storage overhead factor for program storage, etc.?

1.8 Modularity

- What types of upgrades must be supported?

1.9 Compatibility

- Must the system interface with existing data processing/office automation frameworks? (Specify frameworks. Also indicate whether there are electronic data records that must be incorporated into the system – word processing documents, spreadsheets, data tables, etc.)

2.0 Performance Factors (Outcomes)

The following questions are designed to assist the agency in identifying relevant performance levels for the targeted system. The list is not inclusive.

Specification of performance factors will assist system vendors and service providers in structuring equipment frameworks that are sufficient to meet the identified performance levels.

2.1 What are the relevant quantifiable performance factors for the system? (Increased throughput/productivity, quicker turnaround time, reduced error rate, enhanced revenue collection, reduced processing costs, etc.)

2.2 What are the relevant qualitative performance factors for the system? (Improved customer service, enhanced compliance with state/federal laws, improved security, enhanced quality of life for constituents, etc. Provide as much detail as possible for each factor listed.)

3.0 Index Data Structure,

Image File Composition/Arrangement and Data Management

The following questions are intended to guide the agency through the process of developing a preliminary index data structure and in delineating desired data management approaches.

3.1 Index Data Structure (Meta-Data)

- Which data elements will be used to identify document types? (These would be document type identifiers such as “correspondence”, “judgments”, “reports”, etc.)
- Which data elements will be used to identify key document contents? (These would be elements that allow for structured searching such document number, date, client name/address, etc.)
- How will the data elements be formatted --length, data type? (Provide flat file views.)

- Will code tables be used for any of the identified data elements? (Specify coding schemes if possible.)
- How will the free-text/full-text searching feature be employed?

3.2 Image File Composition/Arrangement (New System)

- What will be the general physical composition of the image file?

3.3 How must the paper files be arranged/organized for scanning? (Document-Prep)

3.4 Are the files self-contained upon receipt or must images be added to the files throughout their processing and retention life cycles? Specify.

3.5 Are there any special features required of the data management package?

- Ad-hoc report/query (specify retrieval scenarios if possible)
- Secure data import/export
- Other – Specify

4.0 Procedural Flow Analysis

The following questions are designed to assist agencies in specifying procedural flows involved in active records processing applications and identifying programming tasks for procedural flows to be automated. Note that this section does not address the procedural flows involved in converting (scanning, indexing and storing) documents.

4.1 Application Specific Work Steps

Which automated work steps will occur during the processing of individual transactions? (List and describe all work steps involved with each transaction if possible.)

- Receipt/generation
- Conversion (covered in following section)
- Review/processing/annotation
- Storage
- Retrieval/Transfer
- Printing
- Disposal
- Where will the work steps occur?
- How many times will individual steps be completed in a week, month, year (frequency)?
- Which document types will be used in the identified steps?
- Will manual work steps be involved? How will they relate to automated work steps?
- Will the procedural flow involve structured decision points? (Provide decision trees or other devices to illustrate decision logic and associated action sets.)

4.2 General Work Steps

- What steps will be taken to provide for image and index data back up? Frequency of back-ups? Off-site storage location?
- What will be done with hard copy documents subsequent to their conversion to digital format?
- Immediate request for disposition? Off-site storage?
- What maintenance steps will be taken for back-up media?
- Periodic media inspection (schedule for retrieval and inspection)
- Periodic facility inspections
- Full back-up/disaster recovery plan
- What steps will be taken to manage on-line document stores?
- Retention scheduling/purge cycles (including requests for disposal when applicable)
- Data/image reorganization schedules

5.0 Procedural Flow for Document Conversion

The following questions are designed to assist agencies in specifying procedural flows and basic functional/performance parameters for document conversion (scanning, indexing and storing documents). It should be noted that document conversion flows for back file and current operations (updates) may have to be handled differently.

Special emphasis should be placed on document conversion. System integrity and performance are dependent upon effective and efficient conversion operations.

The questions below are divided into distinct task categories. Agencies should note that in reality, the tasks are closely related. In certain cases, tasks overlap -- e.g., image and index verification. Hence, when specifying conversion sub-systems, agencies should carefully plan the sequencing and integration of individual conversion tasks.

5.1 Preparation

- How many documents (or pages) will be prepared per shift?
- Where will preparation operations take place?
- Will preparation operations be located in a separate location from scanning operations?
- If so, will document transfer procedures be required?
- What steps will be taken to insure that documents are scanner ready? (List steps in sequence.)
- Removal of extraneous material
- Removal of duplicate/unnecessary documents
- Unfolding documents
- Repairing damaged documents
- Mounting undersized documents
- Arranging documents in batches
- Placing documents in folders/containers

- Placing documents in order
- Placing document/batch break targets in document containers
- Labeling document containers
- Which document control points will be instituted?
- File/document inventories
- File/document totals/cross totals
- Verification/authorization sign-offs
- Will hard copy document purging be involved? (If so, provide for purge instructions and requests for disposition when applicable.)

5.2 Scanning

- How many documents will be scanned per shift?
- Will the physical characteristics of the document base affect scanner operations?
- Size
- Weight
- Color
- Recording technique (hand written, typed graphics, mixed)
- Dense print
- Contrast
- Condition (good, poor/in need of repair)
- Single/double sided
- Will documents be scanned randomly or in prepared batches?
- Will specific throughput rates be required for scanners?
- Which scanning density is required? Will variable settings be necessary?
- Will a specific compression algorithm be required?
- Will document stampers (audit trail) be necessary?
- Will scanning be done manually or via use of document stackers? (Stackers help speed throughput.)
- Will an off-line scanning service bureau be used? If so, what interface requirements apply?
- Document transfer procedures
- Transfer media specifications (for tapes, disks, etc.)
- Secure data communications link

5.3 Document Indexing

- Drawing upon the previously defined index data structure, which validation criteria should apply?
- When should indexing occur -- prior to or subsequent to scanning?
- Will index data be drawn from hard copy documents or from scanned images?
- Where are the index fields located on the documents?
- Are they always located in the same place?
- Are they all on the first page of the document?
- How is the document filled out – hand print, machine-print, both?

- Is information on the document color-coded?
- Will index data be entered via keyboard or OCR/ICR?
- Will bar coding be utilized? (1D/2D)
- If automated data capture is anticipated, are the forms designed for OCR/ICR? (Constrained Hand Print/Registration Marks/Document Control Barcodes?)

5.4 Quality Control - Image Inspection

When will images be inspected?

- Immediately following scanning
- During indexing/data capture
- Prior to or after storage on optical/magnetic disk

Will inspectors be separated from scanner operators? (Recommended)

What will the level of inspection be?

- Image by image
- Lead images (first page of documents) only
- Random sampling of batches

Will scanned images be cross-verified with original hard copy documents?

Which acceptance/rejection criteria will apply?

- Legibility
- Completeness of coverage
- Scanning density
- Presentation (absence of skews or other problems that cause the loss of detail)

Which rework procedures (for rejected images) will be applied?

Will images be recorded to optical/magnetic disk prior to or following image inspection? (The latter is recommended.)

5.5 Index Verification

How will index values be verified (in addition to on-line validation)?

Simple visual check

Double keying

Software algorithm – Specify approach (Edit/Validation Rules)

5.6 Conversion Process Monitoring

Which management control elements will be necessary?

Batches in process reports

Exception reports on throughput/accuracy performance

Operator statistics

Activity counts by agency/document type

Charge-back data for billing conversion services

6.0 System Management

The following questions are designed to assist agencies in developing specifications for system management functions. (System management may be integrated with standard procedural flows.)

6.1 Management Control

- Will audit trails be necessary for tracking system transactions?
- Will detailed resource monitoring be necessary?
  - Disk usage
  - Input/output activity
  - Device status
  - Application program status
  - Data file/image base status
  - Retrieval/access/print volumes
  - OCR/ICR read rates
  - Employee Productivity
- Which types of error management are necessary?

6.2 Document Management

- Will document version tracking be necessary?
- Will work-in-progress/open activity control be required?
- Would exception reporting (on data synchronization, missed turnaround, etc.) be helpful?

6.3 Security (Software-Controlled)

What security scheme will be implemented?

- User profiles
- User groups
- Functional restrictions on data/image classes/program function

6.4 Document and Content Preservation Strategy

- How will documents and digital content be preserved if retention requirements call for long term storage (10 years or more)?
  - Microfilming paper documents
  - Migration of documents and other content to new technological platforms Technology preservation or Technology emulation

**Microfilming and migration, or a combination of the two approaches is recommended.

7.0 Output Specification/Screen Layouts

The following questions are designed to assist agencies in gathering information concerning image output and screen requirements.

7.1 Retrieval Routines/General Screen Layouts

- Will there be pre-formatted retrieval screens for report programs?
- Will there be specific requirements for other screen layouts?
  - Index screen presentations
  - Menus

7.2 Image Display Requirements

- Will there be specific requirements for image presentation?
  - Screen size
  - Resolution (for retrieval screens/quality control screens) Windowing
  - Zoom/pan/scroll
  - Image rotation
  - Reverse video

7.3 Image Printing

- Will there be any priority schemes?
- Will printing be done on demand or in batch mode?
- Will a batch window be necessary?
- Will customized batch separator sheets for different output streams be required?
- Will specific features be desirable?
  - Output resolution
  - Frame up/down
  - Collation
  - Paper type
- How many prints will be required per month/year?

8.0 Integration Requirements

The following questions are designed to assist agencies in documenting requirements for interfacing the record image processing system with other information processing and management frameworks.

8.1 Computer/Network Interfaces

- Will the system have to interface with an external server(s)?
- If so, what are the relevant base hardware and software elements?
  - CPU Make/model number

    - Operating system name and version (release)
    - Communication protocol
    - Physical connections
- Will the system have to interface with an internal/external network (GSN) or other data communications network? If so, what are the relevant protocols, speed of the network, and physical connections? What are the firewall rules? Are secure sessions required?
- What protocols apply to security/encryption? Will the route between the users and the servers be audited to ensure adequate bandwidth for image traffic?

8.2 Data Processing (Legacy) Application Interfaces

- Which existing data processing applications will be used?
- Will the system require emulation software or batch transfer programs?
- If batch transfer programs will be required, which screens or data elements (from the existing system) will be involved?

8.3 Office Automation Application Interfaces

Which applications will be used?

- Word processing
- Electronic mail
- Forms processing
- Facsimile transmission

8.4 Microfilm/Long Term Storage Interfaces

- Will image and/or index data be output to a microform (film reels and/or fiche)?
- Will there be a need to output computer data to a separate optical/magnetic disk facility for long-term storage?

9.0 Facilities

The following questions highlight key factors in the establishment of facilities to house the new system components.

9.1 Space Requirements

- What is the total space requirement for the new system?
    - Work area
    - Access area
    - Staging/receiving area
    - Main configuration area
    - User workstation area, including furniture
    - Vault storage/shelving area
- Where will the various areas be located?
- How will they be arranged?
- Which wiring/cabling/connector types are required?

- How will wires/cables be run? To where?
- Is special or upgraded lighting required?
- Are specific forms of physical security/protection necessary?
  - Locks/intrusion alarms
  - Fire detection/suppression
  - Water detection
  - Climate control
  - Power conditioning/supply

10.0 Operational Support Elements

The following questions point to key operational support elements that will facilitate system implementation and maintenance.

10.1 Human Resources

- What level of staffing will be necessary for the new system? Is a staffing plan necessary?
  - System operators (scanner operators)
  - Programmer/analysts
  - Scanning/indexing staff
  - Production supervisors
  - System administrators
- What types of training are required?
  - System operators (Scanner Operators)
  - Programmer/analysts
  - Scanning/indexing staff
  - Production supervisors
  - System administrator
  - Management
  - End users
- How many sessions will be held?
- Where will the sessions be held?

10.2 Documentation

- What types of application documentation will be required?
  - Flowcharts
  - Data/process/procedural flow diagrams
  - Procedural flow descriptions
  - File/record layouts
  - Report screen/specifications
  - Forms specifications
  - Scanner settings
  - Compression algorithms
  - Compliable source code

11.0 Technical Support and Maintenance

The following questions point to key technical support elements that also facilitate system implementation and maintenance.

11.1 Will on-site contractor support be required subsequent to equipment installation and system implementation? If so, how long will this support be required?

11.2 Which on-site personnel will be responsible for:

- Hardware
- Application software functions
- System software functions
- Data communications
- All of the above

11.3 Which elements must the hardware maintenance agreement cover?

- Hardware components
- Parts availability
- Response time/escalation schemes
- Remote diagnostics

11.4 Which elements must the software maintenance agreement cover?

- Automatic software updates/software update installation
- Consultations regarding impact of software updates
- On-site/remote diagnostics

11.5 Detail the Consumables Needed

- Magnetic Media
- Disks
- Tapes
- Tape Cartridges
- Optical Disks
- Other Media (CD/DVD)
- Cabling
- Twisted Pair
- Coaxial Cable Fiber Optic Cable Other
- Paper/printing/filing
- Printout Paper Forms Belts/Drums Toner Envelopes Labels
- File Folders
- Guides
- Record Containers
- Cubic foot boxes

- File Drawers/cabinets
- Microform cabinets/containers
- Document Handling equipment
- Staple Removers
- Scissors Rubber Bands Tape
- Pens
- Note Pads
- Carts
- Step Stools
- Pallets

12.0 Operational Budget

Is there a budget for all of the support elements for the new system? Please provide the details – amounts and expenditure categories (minimum of 3-5 year time period).

Chapter 13

Service Package

Planning Service Package			
Consultative Services	**Strategic** Guidance with regard to assessing the feasibility of automated records systems and services Assistance with completing DORES/RMS Feasibility Study Outline Consultation on aligning records systems planning overall information technology and budgetary planning Guidance with regard to incorporating records management practices into automated systems	**Tactical** Guidance with regard to effectively structuring procurement system development/service program initiatives Assistance with completing DORES/RMS Feasibility Study Outline Assistance with completing DORES/RMS Conceptual Design Document	**Operational** Guidance with regard to the roll of out of approved initiatives Direct consultation, and where applicable, development of Memoranda of Understanding outlining service levels for any in-house services to be provided by DORES/RMS

Remittance Processing Service Package				
Consultative Services	**Design Transaction Documents** Consultation on the design of stub and check transactions Verification of retention	**Design Outbound Processes** Consultation on the design of processes that create billing/remittance processing items (involves extracting and generating bills	**Design and Execute In-bound Processes** Design and programing of applications that convert inbound paper transactions to electronic data	**Configure and Implement Data/Image Export and Storage** Configuration and implementation of software and hardware needed to: populate agency databases

	scheduling for transactions	from the agency's production system and then producing the remittance transactions)	and image streams *DORES/RMS manages development and implementation projects in this category directly.	with information about completed transactions; post electronic images to storage/ access platforms; and provide input to revenue deposit and NJCFS processes (State agencies only)
Implementation Services, Remittance Processing	• Mail In-take • Transaction Preparation • Filming/Scanning/Data Capture (Including Indexing) • Image/Data Export and/or Film Delivery • Revenue Deposit/Reconciliation • Electronic Image Storage/Access and Security Copy Storage • Image Processing System Certification • Paper Records Disposition (Storage and/or Authorized Destruction) • Project Management, Implementation Assistance and Service Desk			
Costs	• Charge-back (Cost to Agency) *One-time development costs and inclusive per transaction charge-back costs are negotiated with the customer agency on a case by case basis and incorporated into MOUs.			

Active Document Processing Service Package				
Consultative Services	**Assist in Specifying Functional Requirements** Guidance on development of application specifications and construction of implementation strategies (may involve	**Assist in Producing Design for Automated System** Assistance with completing DORES/RMS Conceptual Design Document	**Provide Project Management Support** Guidance on specifying schedule/deliverable/test elements for planned projects	**Configure and Implement Data and Image Export/Storage (In-House Services)** Configuration of software and hardware needed to: populate agency databases; post electronic

	contractor and/or in-house developer resources)	Assistance with planning for process reengineering, workflow automation, and cross-agency integration where appropriate Verification of retention scheduling for transactions involved		images to image access platforms; provide input to revenue deposit/NJCFS processes; and microfilm for long term storage; if applicable
Implementation Services	• Mail In-take • Transaction Preparation • Filming/Scanning/Data Capture (Including Indexing) • Image/Data Export and/or Film Delivery • Revenue Deposit/Reconciliation • Electronic Image Storage/Access and Security Copy Storage • Image Processing System Certification • Paper Records Disposition (Storage and/or Authorized Destruction) • Project Management Support, Implementation Assistance and Service Desk			
Costs	• Charge-back (Cost to Agency) *One-time development costs and inclusive per transaction charge-back costs are negotiated with the customer agency on a case by case basis and incorporated into MOUs.			

Back File Conversion Service Package				
Consultative Services	**Specify Functional Requirements** Guidance on the development of back file application specification and construction of	**Assist in Designing Application** Assistance with completing DORES/RMS Conceptual	**Provide Project Management Support** Guidance on specifying schedule/deliverable/test development elements for planned projects	**Configure and Implement Data and Image Export/Storage (In-House Services)** Configuration of software and hardware

	and implementation strategy (may involve contractor and/or in-house developer resources)	Design Document Verification of retention scheduling for transactions involved		needed to: populate agency databases; post electronic images to image access platforms; provide input to revenue deposit/NJCFS processes; and microfilm for long term storage; if applicable
Implementation Services	• Back file Document Preparation • Filming/Scanning/Data Capture (Including Indexing) • Image/Data Export and/or Film Delivery • Electronic Image Storage/Access and Security Copy Storage • Image Processing System Certification • Paper Records Disposition (Storage and/or Authorized Destruction) • Project Management Support, Implementation Assistance and Service Desk			
Costs	• Charge-back (Cost to Agency) *One-time development costs and inclusive per transaction charge-back costs are negotiated with the customer agency on a case by case basis and incorporated into MOUs.			

Electronic Records Systems Service Package				
Consultative Services	**Specify Functional Requirements** Assistance with completing DORES/RMS Conceptual Design Document Assistance with planning for process reengineering, workflow	**Assist in Designing Application** Guidance on the development of application specifications and construction and implementation strategy (may involve contractor and/or in-house	**Provide Project Management Support** Guidance on specifying schedules, deliverables and tests for planned projects	**Configure and Implement Data and Image Export/Storage (In-House Services)** Configuration of software and hardware needed to: populate agency databases; post electronic images to image access platforms;

	automation and cross-agency integration where appropriate Verification of retention scheduling for transactions involved	developer resources) In cases involving automated PDF submissions, development of configuration specifications for Enterprise Forms Processing and Records Management Platform		provide input to revenue deposit/NJCFS processes (State agencies only); and microfilm for long term storage; if applicable
Implementation Services	• Secure Web Application Development (Done in Conjunction with OIT) • Secure Bulk Electronic Filing • Application Hosting for PDF-based Forms Processing (In-house and/or Third Party with Back-up/Recovery) **In-house Disaster Recovery Program Being Developed • Electronic Funds Transfer, Electronic Check and Credit Card Payments • Data Capture/Export • Online Reporting/Certification • Revenue Deposit/Reconciliation • Project Management Support and Service Desk • Contract Management for all Electronic Payments, and Where Applicable, Electronic Government Applications Secured Through State Contract # -- (E-Government Contract)			
Costs	• Charge-back (Cost to Agency) One-time development costs and potentially, on-going maintenance costs are negotiated with the customer agency on a case by case basis and incorporated into and MOU			

Chapter 14

Guidelines and Examples

Example Operational Continuity/Disaster Recovery Plan

State of New Jersey
Agency Name
System Name

Operational Continuity and Disaster Recovery Plan

Introduction

1.1 Purpose:

The _____ operational continuity and disaster recovery plan establishes procedures to recover the _____ environment following a complete loss of any of its image storage and retrieval platforms.

The following objectives of the plan are to:

- Implement contingency operations through an established plan that consists of the following phases:
  - Notification/activation to detect and assess areas impacted and to activate the plan
  - Implementation of temporary operations and recovery from impact until normal operations can be restored
  - Recover storage and retrieval operations fully*
- Identify the critical activities, resources, and procedures needed to carry out operations during prolonged interruptions to normal operations
- Assign responsibilities to designated personnel
- Provide guidance for recovering operations during prolonged periods of interruption to normal operations
- Ensure coordination contingency planning stakeholders and staff

1.2 Applicability:

The _____ plan applies to the functions, operations, and resources necessary to restore and resume normal _____ image storage and retrieval operations located at _____.

Scope:

_____ manages various _____ image processing platforms at the facility above. The platforms house over _____ page images and service agencies such as _____

_____

_____ will back-up complete images of all systems, including all custom applications, on a weekly basis, and store the same at a secure and environmentally controlled off-site facility (currently provided by contractor ___). ____ will maintain up-to-date configuration documentation that can be quickly converted to an emergency equipment replacement order and share the same with the Fiscal office.

_____ will also maintain a rigorous back-up regime for all content (see attached schedules).

Should there be a complete loss of one of the platforms, _____will proceed as follows:

- Activate an emergency procurement for the affected platform(s) and place an emergency order for the replacement equipment and base software, if applicable.
- Continue day-forward processing on <scanning and indexing> platform.
- Increase cache storage on <scanning and indexing> platform if required to hold day forward content.
- Working with user agencies, shift as much retrieval activity as possible to back-up content sources (e.g., databases, shares, e-mail, collaboration sites, paper or microfilm).
- Install and configure the replacement platform(s) using back-up images.
- Restore day-forward storage and retrieval operations.
- Restore content from back-up's and thereby reach full recovery.

*Note: Overall, during an outage, ___ will retain paper documents through some combination of storage on site, storage at the client agency and/or retention at the_____ Records Center in _____. Upon resumption of image services, returns will be scanned and indexed based on a priority scheme to be determined by _____ in conjunction with senior management.

1.3 Implementation

In the event of a project delay or general disruption of services, _____ will:

- Alert the <senior management>'s Office as to the nature of any concerns that may become imminent, leading to a processing system failure or disruption.
- Activate the plan outlined in 1.2 with Fiscal via its internal chain of command (see attached organization chart).
- Alert client agencies to disruptions. This notification will include a description of the issue, summary of the activated contingency processing plan and an estimate relative

to recovery time. _____ will set up an emergency contact number and will provide updates to client agencies as required. The alert will also notify the agency that it will be necessary to use alternate sources of informational content if available (e.g., databases, shares, e-mail, collaboration sites, paper or microfilm).

- For affected business registry systems, develop and post, in multiple channels, an advisory for the public indicating that image retrieval may be delayed for a period of time and point potential customers to alternatives such as online abstracts and certificates.

Escalation Scheme/Responsibilities:

- Initial alert and issue assessment – Assistant Director Technology Services
- Notification of <senior management>'s Office – Director (Chief of Staff as alternate)
- Notification of Client Agencies – Chief of Staff (Director as alternate) with support from ____
- Notification of Public – Assistant Director, Application Design (Chief of Staff as alternate) with support from ____ web master and Assistant Director for Business Services
- Notification of ___ Fiscal – Director and Chief of Staff (Assistant Directors of Technology Services and Application Design as alternates)

· Management of Contingency Operations – _____ chain of command (see attached organizations chart)

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

[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.

professionals may wish to use these guidelines when developing or managing contractual engagements with Cloud system/service providers.

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

New Jersey Division of Revenue and Enterprise Services Records Management Guidelines for Remote Work Settings

11/2020

As government agencies strive to address the challenges posed by the COVID-19 pandemic, social distancing continues to be a prominent factor in combating the spread of the virus. In this connection, many agencies promote expanded remote work programs -- working from home and other off-site locations, to reduce the number of employees in traditional office spaces. This increases the number of remote locations in which public records are received, produced, stored, distributed and used.

By way of background, State law defines a public record as being any information that a public agency generates or receives in the transaction of its official duties. This is true **regardless of the medium** used to store the information (for example, electronic devices, paper or microfilm).

Public employees who receive, generate or store public records while working in remote settings have an obligation to manage these records properly. This means that they must be attentive to records retention requirements, basic information security measures, public records access provisions like the Open Public Records Act (OPRA) and any applicable access restrictions in the case of records that are classified as sensitive, confidential or private.

This document is designed to provide government employees with quick and practical guidelines for managing public records in remote settings. While not comprehensive, the guidelines touch upon practical actions that employees can take to ensure they are following a basic records management regime in remote work settings.

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.

Organizational Sources of Support and Guidance

Employees should look to their executive management teams for overall guidance on records management responsibilities. In addition, depending upon the structure of the government agency, the following functions may be able to provide guidance on records management and related topics:

- Information technology office
- Legal department
- Risk management professionals
- Agency records management staff

- Internal audit staff

GUIDELINES

1. Be aware of records retention and disposition requirements.
   State law (N.J.S.A. 47:3 et seq.) requires public agencies to obtain approval before they destroy public records. Accordingly, you may not delete or destroy public records in your possession – no matter where or how they are stored, without approval. Contact RMS for more information on the *Request and Authorization for Records Disposition* process. For a fuller explanation of the State's records retention and disposition program and the legal and operational authorities involved, consult the State Records Manual.

2. Only use the official, agency-approved electronic mail system.
   Use of the official system helps to ensure that email records will be properly managed and preserved.

   If there is a circumstance that **compels** you to use your personal email account to create/store a public record, report the matter to your supervisor and ensure that you forward the record to the official electronic mail system as soon as possible. DO NOT delete public records stored in your personal electronic mail system until they have been forwarded to your agency's official system. Contact RMS for guidance on deleting records from your personal system after they have been properly forwarded.

3. Use only agency-owned/approved (official) computer storage facilities to house electronic public records.
   Use of the official system assures that electronic records will be properly managed and preserved.

   Avoid storing public records on mobile devices like laptops, tablets, cell phones or removable storage devices unless it is necessary to do so. Use agency-owned/approved storage facilities instead. Examples of these storage facilities include your agency's share files and collaboration sites, agency-designated personal storage spaces, content management/electronic image repositories and official data base systems. These facilities may be on-premises (facilities owned and operated by the agency) or reside in agency-approved, vendor- managed Cloud or hosted computer complexes. In remote locations, you will connect with these facilities via the Internet through secure log-in routines, specialized secure communication channels like Virtual Private Networks or other remote-control software applications.

   If you must use a mobile computing device to store public records, ensure that you forward the stored records to the appropriate official storage facility as soon as possible. DO NOT delete public records stored on mobile devices until they have been forwarded to the appropriate official facility. Contact RMS for guidance on deleting records from your personal system after they have been properly forwarded.

4. DO NOT store sensitive, confidential or private electronic public records in Cloud or hosted storage facilities **unless cleared to do so by your agency**.
   Examples of these records include tax records and records containing personally identifiable information, personal health information and/or proprietary information. Such records may be subject to statutory access restrictions, as well as strict security compliance regimes like IRS' SafeGuard and the requirements set forth by the Health Insurance Portability and Accountability Act (HIPPA).

5. For official business, use only approved social media sites and follow your agency's policies and procedures.
   Social media platforms like Facebook, Twitter and YouTube enable government and its constituents to collaboratively produce and share information and content. As such they can be powerful communicative tools. If you use social media to communicate official information about your agency's programs and/or to interact with the public in the course of official government business, **use only the platforms approved and controlled by your agency in accordance with official policies and procedures.** If you transacted public business via your personal social media account, ensure that you copy and forward the content you posted to the appropriate official agency storage facility as soon as possible. DO NOT delete the content until you forward a copy of it to the appropriate official storage facility. Contact RMS for guidance on copying and forwarding social media content and on deleting the content after it has properly forwarded.

6. Avoid creating or storing paper public records in home settings unless authorized to do so by your agency.
   If you do create/store paper records at home, make sure they are kept separate from your personal files in a secure location that prevents others from accessing them. Transfer paper records to your agency's paper storage area or your own office files as soon as possible.

7. Employ basic security measures to protect personal home computing facilities that connect to work systems.
   Protecting home computing facilities (for example, lap top computers and routers) helps to keep both your private information and public records safe from unauthorized access, use, dissemination and/or destruction. The National Security Agency (NSA) publishes useful guidelines for protecting your home computing facilities. Some of the NSA's recommended actions include:
   a. Keeping your operating system up to date.
   b. Using up to date security software including firewall, anti-malware, anti-virus, anti-phishing and safe browsing software.
   c. Disconnecting external storage and printing devices when not in use.
   d. Turning off computing devices when not in use.
   e. Using strong, unique and hard-to-guess passwords on your computing devices and Internet router.
   f. Keeping your browser software up to date.
   g. Limiting the use of the *Administrator* account on your home computer(s) by creating

and using a non-Administrator account for daily activities (the Administrator account gives elevated privileges to system resources and malware can use these privileges to compromise your computer).

h. Practicing safe online behavior – for example:
    i. Do not use open, unprotected networks such as those found in hotels and public spaces.
    ii. Do not log in from overseas locations without the express approval ofyour agency.
    iii. Do not open attachments or links in unsolicited emails;
    iv. Do not open emails from unknown sources or emails that look suspicious;
    v. Verify unfamiliar web sites by searching for them via an Internet search engine (before visiting them); and
    vi. Do not visit sites with known security or reputational issues.

8. Be aware that public records are subject to the Open Public Records Act (OPRA) and must also be made available in response to subpoenas and investigations.
   If you have public records in your possession, you must be prepared to produce them in response to OPRA requests, subpoenas and other investigatory processes conducted by your agency or other authorized governmental agency. For more information on OPRA, see the State's Reference Material.

Selected Links

Links to Content Relating to Electronic Records Management Guidelines, Policies and Procedures

Alaska

http://doa.alaska.gov/ets/messaging/Archiving/policy.html

http://www.azlibrary.gov/records/documents/pdf/GuidanceAndRelatedResources/email_management.pdf

Arizona

http://www.azlibrary.gov/records/documents/pdf/GuidanceAndRelatedResources/Min_Standards_Scanning.pdf

Arkansas

http://www.dfa.arkansas.gov/offices/intergovernmentalServices/Documents/erecord_guidelines.pdf

Connecticut

http://www.cslib.org/publicrecords/GL2009-2Email.pdf

Florida

http://dlis.dos.state.fl.us/barm/handbooks/electronic.pdf

Georgia

http://www.sos.ga.gov/archives/InformationForGovernmentAgencies/Records_advice/TechnicalLeaflets/ ElectronicRecords/Checklist_v3.pdf

http://www.sos.ga.gov/archives/InformationForGovernmentAgencies/Records_advice/TechnicalLeaflets/ElectronicRecords/ArchivesAdvice1.pdf

http://www.sos.ga.gov/archives/InformationForGovernmentAgencies/Records_advice/TechnicalLeaflets/ElectronicRecords/Email_retention_guidelines.pdf

http://www.sos.ga.gov/archives/InformationForGovernmentAgencies/Records_advice/TechnicalLeaflets/ElectronicRecords/ArchivesAdvice13.pdf

Hawaii

http://ags.hawaii.gov/wp-content/uploads/2012/09/Comp-Cir-2001-021.pdf

Idaho

http://history.idaho.gov/sites/default/files/uploads/RecordRetentionBook_2.pdf

Indiana

http://www.in.gov/icpr/files/policyelectronicrecords.pdf

Iowa

http://www.iowahistory.org/archives/assets/GuidelineonElectronicRecords.doc

Kansas

http://www.kshs.org/portal_records_management

Louisiana

http://www.sos.la.gov/Portals/0/archives/pdf/la_archives_e-mail_policy.pdf

Maine

http://www.maine.gov/sos/arc/records/state/rmmanual0712.pdf

http://www.maine.gov/sos/arc/records/state/emailguide0712.pdf

Massachusetts

http://www.sec.state.ma.us/pre/preerecords/E-Discovery%20Presentation.pdf

Michigan

http://www.michigan.gov/dmb/1,1607,7-150-9131_9347---,00.html#900PRESERVATION

Minnesota

http://www.mnhs.org/preserve/records/electronicrecords/erintro.html

http://www.mnhs.org/preserve/records/electronicrecords/ermetadata.html#Minnesota%20Recordkeeping%20Metadata%20Standard (meta data discussion)

Missouri

http://www.sos.mo.gov/records/recmgmt/E-MailGuidelines.pdf

Montana

http://www.sos.mt.gov/Records/forms/MT_Email_Guidelines_06.pdf

Nebraska

http://www.sos.ne.gov/records-management/pdf/Electronic%20Records%20Guidelines.pdf

http://www.sos.ne.gov/records-management/pdf/Electronic%20Records%20Guidelines.pdf

http://www.sos.ne.gov/records-management/pdf/guideline_web_pages_march_2003.pdf (web pages guidelines)

Nevada

http://nsla.nevadaculture.org/index.php?option=com_content&view=article&id=514&Itemid=503

New Hampshire

http://www.sos.nh.gov/archives/PDF/ELECTRONIC%20RECORDS%20ISSUES.pdf

New Mexico

http://www.nmcpr.state.nm.us/records/email.htm

New York

http://www.archives.nysed.gov/a/records/mr_erecords.shtml

North Carolina

http://www.records.ncdcr.gov/erecords/default.htm

North Dakota

http://www.nd.gov/itd/standards/records-management/electronic-records-management-guidelines

Ohio

http://ohsweb.ohiohistory.org/ohioerc/images/1/18/ERMguidelines.pdf

Oregon

http://arcweb.sos.state.or.us/doc/recmgmt/train/erm/emailman806.pdf

http://arcweb.sos.state.or.us/doc/recmgmt/train/erm/stateemail.pdf

Pennsylvania

http://www.portal.state.pa.us/portal/server.pt/gateway/PTARGS_0_77473_823079_0_0_18/EmailMgmt.pdf

http://www.portal.state.pa.us/portal/server.pt/gateway/PTARGS_0_77473_823080_0_0_18/FileNameERecords.pdf

Rhode Island

http://sos.ri.gov/documents/archives/Bulletin_1.pdf

Tennessee

http://www.state.tn.us/generalserv/ba17r/ElectronicRecordsPolicy.pdf

Texas

https://www.tsl.state.tx.us/slrm/recordspubs/stbull01.html

Utah

http://archives.utah.gov/recordsmanagement/ERM/electronic-records-links.html

Vermont

http://vermont-archives.org/records/iSTART/standards/

Virginia

http://www.lva.virginia.gov/agencies/records/electronic/electronic-records-guidelines.pdf

http://www.lva.virginia.gov/agencies/records/electronic/index.htm

Washington

http://www.sos.wa.gov/archives/RecordsManagement/ElectronicRecordsManagementAdviceandResources.aspx

West Virginia

http://www.wvculture.org/history/rmpb/crmmanual11.html

Wisconsin

http://www.doa.state.wi.us/facts_view.asp?factid=15&locid=2

http://www.doa.state.wi.us/facts_view.asp?factid=11&locid=2

Wyoming

http://wyoarchives.state.wy.us/RM/Guidelines.aspx

http://wyoarchives.state.wy.us/pdf/ar-9e.pdf

http://wyoarchives.state.wy.us/pdf/requirements.pdf

Example Litigation Hold Order and Acknowledgement

For Discussion Purposes Only

Consult With Legal Advisors When Dealing With Litigation Hold Orders

<date>

TO: <individual and/or custodian>

FROM: <issuing office>

SUBJECT: <subject or nature of the matter>

Please be advised that you are required to immediately preserve all documents and electronic data related to the above-noted matter. Your failure to do so could result in significant penalties.

<Agency> has received the above-captioned complaint and a copy is attached. We have identified you as a <custodian or individual> who may have potentially relevant paper records (e. g. memoranda, letters, pictures) or electronically stored information (e. g. e-mails, other electronic communications such as word processing documents, spreadsheets, databases, calendars. telephone logs, Internet usage files and network access information) or authority over such records.

You must immediately take every reasonable step to preserve this information until further notice.

Your failure to do so could result in significant penalties against us.

While your obligation to preserve all forms of information is the same, we specifically bring to your attention the need to take action to preserve e-mail and other electronic communications, because there may be automated processes which will delete your e-mail if you take no action and for many individuals the deletion of e-mail is a routine practice. You should take immediate action to store any relevant e-mails in a separate folder or storage area for this potential litigation.

For paper documents and other types of electronically stored information, to the extent that it will not interfere with your ongoing work, you should take action to segregate those materials. In the case of electronically stored information, you should leave it in its current location, but may make a copy for a separate folder or storage area related to the potential litigation. In the case of paper records, you may either move them to a separate location, noting the files from which each record was retrieved, or make copies of the records.

This is a continuing obligation. So if you discover, create or receive relevant documents or electronically stored information in the future you should similarly take action to preserve those materials. You should preserve all relevant documents and electronically stored information in accordance with these instructions until you are affirmatively advised that you are no longer obligated to do so.

Attached is an acknowledgement that you have received this memorandum. You should return it to me within five days of your receipt.

If you have any questions regarding these instructions please call <contact> immediately at (___) ___-____. Again, it is imperative that you take immediate action in accordance with these directions.

Acknowledgement of Receipt of "Litigation Hold" Instructions

RE: <subject or matter>

I, <individual or custodian>, acknowledge that I have received the <date of notice> notice regarding the above-captioned matter from <representative> advising me of my obligation to conduct a reasonable search for any documents, whether stored in hard copy or electronically, that may be relevant to the matter and to take reasonable steps to ensure the preservation of those documents.

I understand the instructions contained in the memorandum.

_____.

Signature

_____ . Date: _____

Name

Note: If you do not understand the instructions, prior to completing this acknowledgement, you should contact <representative> at <___>-<___-____> with any questions you may have regarding either 1) what documents might be relevant to the above matter or 2) what actions you are reasonably expected to take in order to conduct a reasonable search for and preserve any documents, whether stored in hard copy or electronically, that may be relevant to the above matter.

Guidelines on Retention Scheduling Public Records Stored on Social Media Platforms

Updated 12/20/2024

Introduction

These guidelines include suggested action steps for creating retention/disposition policies for public records created and stored via social media services like Meta/Facebook, X, LinkedIn, YouTube, wikis and other Internet-based platforms. Social media services involve various forms of content, including text, images, audio and video recordings. Usually, private firms provide and manage the platforms used to deliver social media services. This factor, combined with the dynamic, rich and complex make-up of the records involved, makes retention scheduling of social media a challenge. Nonetheless, public agencies can begin to deal with the retention scheduling challenge by executing the recommended action steps.

Applicability of Public Records Law

The foundation for this document is the legal imperative expressed in the State's public records law (N.J.S.A. 47:3 et seq.). That is, irrespective of medium, all records that are generated and received during governmental operations in New Jersey are public records and subject to the State's records management and archival requirements. Records generated and received via social media services and stored on social media platforms are therefore subject to the State's public records law.

Audience

Generally, these guidelines are designed for professionals who work in records and information management capacities and who have some familiarity with the State's records management program as described in the State Records Manual. However, generalist managers and administrative support staff may also find the guidelines useful.

Note on Scope

This document covers retention scheduling only[5]. It does not cover the more encompassing topic of social media policies and procedures. The New Jersey Records Manual contains an outline on how the State's Department of the Treasury approached the development of an encompassing social media policy/procedural regime. Readers interested in developing similar regimes for their agencies may find the outline helpful.

[5] The approaches to retention scheduling, storage and disposition of social media discussed in this document are largely based on guidelines and standards published by the National Archives and Records Administration *(*Best Practices for the Capture of Social Media Records) and the New South Wales Archives and Records agency (Strategies for Managing Social Media Records).

NARA issued more recent guidance on Managing Social Media, which includes a listing of software products that may be useful in programs that call for the export of social media records from vendor platforms to agency-controlled storage facilities (Appendix F in the NARA publication).

Be aware that some of the technical references in these publications may be dated or can become so quickly. However, the core concepts about value assessments and content capture, storage and retention/disposition are likely to be valid for the foreseeable future. Finally, The Sedona Conference provides invaluable information on this topic. It guided this document's commentary on the legal context of social media use/management (*Primer on Social Media, Second Edition*. (2018). The Sedona Conference: Phoenix, AZ.)

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.

Action Steps

1. Inventory Social Media

   Start the retention scheduling process by inventorying and documenting all the services and platforms employed by the agency – for example, accounts/sites using Facebook, Twitter, Tumblr, YouTube, Snapchat, Instagram, etc. Describe the content that resides on each platform and the organizational functions that each one addresses – for instance, dissemination of program-related information, constituent service channel, ideation and communal program development, etc.

2. Conduct a Value Assessment(s)

   Based on the descriptions and functional purposes of the social media platforms, assign values to the content (records) they contain. Following are value dimensions that could be assigned to records stored on social media platforms. The value dimensions are tied to a simple range: low (records with little or no lasting retention value); medium (records with some short-term – less than 10 years, retention value); and high (records with greater than 10 years retention value).

   Note that records may bridge or overlap the value dimensions. For example, a particular social media site may contain content that has both informational and planning and decision support/knowledge management values. If this occurs and the overlapping dimensions have different (higher/lower) values with respect to retention and disposition, the recommended policy decision would be to assign the higher value to the content.

   Value dimensions a and b below are likely to be the two most common dimensions that agencies encounter.

   a. Informational **(retention value – low)**. Social media platforms can be used for broadcasting and one-way (organization to stakeholder) communications on routine matters. Content generated for such purposes would likely not have any lasting value, and therefore be classified as routine/non-sensitive in nature. Usually, the original, official broadcast messages are kept in separate storage areas (paper files, file shares, collaboration sites and/or agencies records/content management systems).

   b. General Information Exchange **(retention value - low to medium)**. Social media can augment informational postings by opening channels for two-way constituent service and communications. For instance, social media may serve as conduits for constituent commentary and information sharing (posts and tags) regarding information broadcast by the agency. Content produced in this category can include exchanges such as general feedback, question/answer streams, ratings, voting, likes/dislikes, etc. Such content may

also have secondary uses such as operational research on the effectiveness and efficiency of communications campaigns.

c. Transactional **(retention value - low to medium)**. Social media can be parts of an agency's business processes and service delivery models. While perhaps not a significant use case at this juncture of social media's technical and operational evolution, one could envision potential applications here – for example, delivery of digital content such as reports and other public documents and work order entry and tracking.

d. Operational/Management Control **(retention value - low to medium)**. This form of content relates to various internal (intra-agency) activities such as employee feedback/suggestions, information exchange/knowledge building, policy/procedure dissemination, publication of performance levels, etc. This type of content can correspond with and complement management control by carrying messages and commentary about program outcomes, operational controls and organizational service levels. Management control-related content is likely to have some enduring value beyond its immediate uses, principally as input for the next category, planning and decision support/knowledge management.

e. Planning and Decision Support/Knowledge Management **(retention value - medium to high)**. Here, content aids executives and specialized staff (technologists, public information officers, legal advisors, budget analysts, etc.) who develop plans and rules that guide the actions of the entire organization from a long term or strategic perspective. In this context, social media can contain valuable information including intra-agency and external discussions and information on a wide range of topics including: economic trends; policy research; constituent sentiment; legal issue; evolving products/technologies that impact agency operations; prevailing political trends; and changes in societal perspectives. Social media also may support collaborative efforts aimed at idea development and product or service innovations via feedback from individual citizens, organizational actors and various other stakeholders.

f. Legal/Compliance **(retention value – high)**. This is an encompassing category which, *depending on the agency's mission*, may envelope all the prior categories. It relates to the management of content, in all forms, for adherence to statutory and regulatory record-keeping requirements. Agencies that employ social media platforms in tightly regulated contexts should be aware that legal, contractual and rules-based requirements may attach to the contents generated by and stored on the platforms. Agencies may be compelled to produce this social media content in discovery processes associated with litigation, audits and internal investigations.

g. Historical **(retention value - high)**. This dimension is likely to grow in importance as time progresses, especially in governmental contexts. Historical content holds long-term or permanent research value. It serves to preserve our intellectual heritage and to document important social, political, economic and cultural developments, and thus has enduring relevance. Over time, some portion of the social media content space will document

significant events, developments and/or trends in aspect of human development, and/or record time- and context-bound perceptions and attitudes about significant human endeavors. This may be especially true in relation to the current COVID-19 pandemic.

3. Assign Retention and Disposition Policies to Social Media Records

   Based on the value assessments conducted in Action Step 2, assign retention and disposition polices to all social media records that the agency generates and stores. This may be done by creating new agency-specific records retention schedule items (record series) or using existing records series.

   For information on how to create new agency specific record series, consult the State Records Manual, pages 10 – 13. Note that RMS can assist in establishing on-going authorizations for disposition, which will enable agencies to dispose of low value content routinely for renewable time periods (6 months or year) without having to submit requests for individual disposition actions. Contact RMS for assistance in setting up on-going disposition authorizations.

   For county and local agencies and authorities, Table 1 lists suggestions for use of existing general record series and disposition policies that align with the value dimensions discussed in Action Step 2. State agencies must follow the State General Records Retention Schedule.

   State agencies should follow the General Schedule items listed in Table 2.

   All agencies should bear in mind that litigation hold requirements may apply to social media records. As with all public records, hold orders will have the effect of tolling disposition actions on responsive social media records.

Table 1

Record's Value	Examples Existing Record Series	Retention/Disposition
Informational (Low)	*News Releases (copies);* **official (original) versions maintained on the agency's internal systems permanently**** **If the social media site contains the official versions, treat as Historical (see last row)	Periodic review/destroy (copies)

General Information Exchange (Low-Medium)	For low value, *Correspondence – Internal* For medium value: *Electronic Administrative Resource Files* *OR* *Administrative Subject File*	Periodic review/destroy Retain until no longer needed for Administrative purposes/destroy 3 Years
Transactional (Low-Medium)	For low value, *Correspondence – Internal*	Periodic review/destroy
	For medium value: *Electronic Administrative Resource Files* *OR* *Administrative Subject File*	Retain until no longer needed for Administrative purposes/destroy 3 Years
Operational/Management Control (Low to Medium)	For low value, *Correspondence – Internal* For medium value: *Electronic Administrative Resource Files* *OR* *Administrative Subject File*	Periodic review/destroy Retain until no longer needed for Administrative purposes/destroy 3 Years
Planning and Decision Support/Knowledge Management (High)	*Correspondence – Policy*	25 years with archival review (use of data migration and long-term repositories indicated; see next Action Step)

Legal/Compliance (High)	*Correspondence – Policy*	25 years with archival review (use of data migration and long-term repositories indicated; see next Action Step)
Historical (High)	Permanent	Permanent with archival review (use of data migration and long-term repositories indicated; see next Action Step)

Table 2

Record Series	Examples Existing Records that Can be Included in this Series	Retention/Disposition
Schedule G100000-014-2900-0001 Social Media Records, Informational Postings	These types of records include routine postings of information for public information purposes.	1 Year/Destroy
Schedule G100000-014,-2900-0002 Social Media Records, General Information Exchange	These types of records include routine interactions between the public and agency.	1 Year/Destroy
Schedule G100000-014,-2900-0003 Social Media Records - Service Transactions	These types of records involve service transactions such as delivery of digital content in the form of reports and other public documents, and work order entry and tracking information.	3 years/Destroy
Schedule G100000-014,-2900-0004 Social Media Records, Planning, Decision Support And Knowledge Management 25 Years/Archival review	These records relate to collaborative exchanges specifically targeted for the planning and development of new or substantially modified public programs. The series does not include exchanges or information derived therefrom used for adjusting or enhancing routine public services.	25 Years/Archival Review

4. Choose Modes of Storage for Social Media Records

   It is most common for agencies to use third party social media services and platforms that are publicly facing and that use a variety of electronic storage formats that can evolve rapidly. Also, third party service providers may offer varying levels of quality and storage capacities that could change over time. This can make the underlying storage technologies and service levels for the agency's social media program uncertain and unstable. In this connection, consider the following storage options.

   a. Implement an *archiving* tool that allows for the scheduled extraction and migration of

social media content to an agency-owned or controlled trusted digital repository. This is the preferred approach. A trusted digital repository enables the agency to store digital records, including social media records, in formats that assure access, use and analysis of the records for the entire length of their retention periods. [6] This functionality is critical for long-term and permanent records. **However, for ease of administration, agencies may wish to include short-term records in these repositories as well.**

The trusted digital repository can be an agency owned computer storage facility and/or a Cloud-based platform, either of which meets or exceeds the requirements listed in the RMS Cloud storage guidelines (State Records Manual, page 145). [7] For long-term or permanent storage requirements, the repository should use file formats that are compatible with long-term/permanent storage.[8] Once records are **successfully migrated** to the trusted digital repository, the agency may delete the migrated content from the site.

b. If the agency's social media site(s) contain records with medium to long-term value (for purposes of this guideline, retention for 2 to 10 years), and the procurement of an archiving tool is not possible, migrate the content periodically to a trusted digital repository via importation of tested back-ups or through the use of data export/ import applications. Otherwise, copy (cut and paste) content to the repository. This *snippet* approach is not a best practice but may be used if there are no other options available to the agency.

   If it is not possible to procure an archiving tool, **and the agency's records need to be retained for short time frames (for purposes of these guidelines, no more than 2 years)**, consider relying on the platform used by the social media service provider exclusively. Ensure that the provider has back-up/recovery tools in place to guard against data loss, or that there are data import/export applications that can be used to make accessible copies of the records. Be sure to test the back-up/recovery tools and export/import applications to ensure that lost or damaged content can be restored.

5. Implement the Retention and Disposition Program

   Choose to conduct the program by:
   a. The standard disposition authorization process (State Records Manual, pages 10 – 13)
   b. The on-going disposition authorization process (contact RMS for assistance in setting up an on-going authorization)
   c. A combination of the processes for different sites

---

[6] The Research Library Group/Online Computer Library Center (RLG/OCLC) provides a formal, encompassing definition of trusted digital repository in its publication entitled Trusted Digital Repositories: Attributes and Responsibilities. As noted in the narrative, while trusted digital repositories focus on long-term and permanent storage, for purposes of this guideline, short-term records may also be included for ease of administration.

[7] The Cloud storage guidelines are relevant to this discussion because many of the requirements listed for Cloud platforms center on capabilities that go to the ability of *any* repository to address long-term records storage and access. The RLG/OCLC publication cited in the previous footnote also provides valuable information on these and other key characteristics, as does the OCLC's publication entitled Trustworthy Repositories Audit & Certification: Criteria and Checklist.

[8] The National Archives' guidelines on file formats for transfer of permanent records and metadata for transferred files may prove helpful in determining file format and meta data requirements for trusted digital repositories.

SUMMARY OF ACTION STEPS

1. Inventory All Social Media Sites and Accounts	2. Conduct Value Assessments	3. Assign Retention and Disposition Policies to Social Media Records	4. Choose Modes of Storage for Social Media Records	5. Implement the Retention and Disposition Program
Describe the Functions and Contents of Each	Assign Retention Values to Records Stored in Each Account/Site • Low – Little or No Lasting Value • Medium – Some Short-term Value (up to 10 years) • High – Lasting Value (25 years or More)	Match Values to Existing Record Series or Request Creation of New Records Series through RMS	Select Tools and Platforms for Storage • Trusted Digital Repository Used in Conjunction with Archiving Tool, for **All Value Dimensions** – Low, Medium and High **(preferred approach)** • Periodic Importation of Records to Trusted Digital Repository Via Tested Back-up or Export/Import Applications – **Medium to High Value Dimensions** • Service Provider's Platform Exclusively – **Low Value Only**	Choose Among Available Options • Use Standard Disposition Authorization Process • Use On-going Disposition Authorization Process • Use Combination of the Standard and On-going Processes

File and Folder Naming Conventions

04/2021

Introduction

Public agencies throughout New Jersey rely on computer technology to create, store, manage, access, distribute and dispose of public records of all kinds, including correspondence, fiscal, personnel and budget records, evidentiary documents like minutes, system documentation, drawings, images and audio/video recordings. These records are stored in desk top computers, mobile devices such as tablets and notebooks, centralized electronic file shares, collaboration platforms, video/teleconferencing sites and more. Further, these computer-based records may be stored in a variety of locations encompassing, office and home settings, alternate remote work sites and sites hosted in the Cloud.

Given the variety/volume of and speed at which public records are created in this complex, heterogeneous environment, it is important to adopt practices that foster consistency and clarity with respect to how computer-based public records are named. Doing this helps to ensure that these records can be identified and used for their intended purposes effectively and efficiently over the course of time, by both the initial and subsequent creators/users, and then properly disposed of once their usefulness and retention periods have expired. In turn, this capability fosters improved transparency and accountability in governmental operations and enhanced defensibility of records disposition actions.

The following guidelines set forth basic conventions for naming computer-based files and folders. The term file is analogous with individual records managed by public agencies, while the term folder connotes collections of related files. **Individuals and agencies may apply these conventions to files and folders residing on personal computing devices, centralized file shares, collaboration sites, video conferencing platforms, social media accounts and general Cloud-based storage facilities. Relative to collaboration sites, the conventions can be applied to chat streams, meeting titles, discussion groups and teams and files of all types shared on the sites.**

Like many efforts that involve computing technology, implementation of naming conventions is likely to require the involvement of diverse stakeholders such as:

- Information and records management professionals
- Legal advisors
- Information technology staff (for example, Chief Technology and Chief Information Officers)
- Information security staff
- Agency managers

Notes on Sources, Exceptions and Implementation Options

There appears to be broad consensus on naming conventions among the records management, academic and library science communities. The materials that form the basis for this presentation are drawn from institutions within these three communities (see References below).

Regarding exceptions, not all situations are amenable to the application of the conventions below. For example, some custom-designed and centrally controlled assets like legacy mainframe and client-server

applications and database systems may dictate how files are named. From another perspective, newer forms of technology may provide for greater flexibility in locating and retrieving files, thereby reducing the number of controls required for naming them. At base then, public agencies and employees can adopt variations of any file/folder naming convention, provided they apply it **consistently** over time.

Finally, in connection with implementation, the ideal would be to adopt a comprehensive approach and work to bring all names – for existing and newly received/generated files and folders, into compliance. Achieving the ideal may prove onerous, however, as it simply may not be feasible to rename existing, non-conforming files and folders. If this is the case, several implementation options are available.

It may be best to implement the convention on a day-forward basis and name only newly generated/received computer-based records in accordance with the convention. Alternately, agencies can adopt a hybrid approach by using the convention to rename selected high value records from existing stores and then apply the convention to all newly generated/received records going forward. Lastly, agencies could consider applying the convention to selected high value records only on a day-forward basis.

Key Contacts

The contact for assistance with naming convention 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.

File Name Guidelines

- Use simple, clear and descriptive terms that all members of your organization can understand and that will identify the files uniquely no matter where they are stored. Terms should include descriptors like constituent names and project/event names combined, where indicated, with other parameters such as dates and numeric identifiers. Other useful terms could include the type of communication (newsletter, status report, annual report, constituent response, minutes, agenda, etc.), version number and organizational unit.

  Examples:

  Contituent_Response_Smith_Jane_20210804.doc.

  Project01_Charter_Final.ppt

  News_Release_Program_Alpha_20210301.docx

  Revenue_Report_20210415.xlsx

  Password_Use_Policy_Final_20210201.pdf

  Contract_01234_Office_Supplies.doc

  Processing_Bureau_Status_Report_0802021

  Safety_Committee_Meeting_Minutes_03062021.docx

  Safety_Committee_Meeting_Minutes_03062021.docx

- **If possible, do not use default names** (names automatically assigned by the system). This is important because, over the course of time, files may be moved to other storage platforms and default names may not provide enough information on the content and context of the files being moved.
- **<u>Be consistent</u> in the way you name files.** Apply your naming conventions consistently over time.
- **Ensure that each file name is unique.**
- **Be concise.** Try not to exceed 50 characters per file name. Do not use words that *do not help* to identify the file such as articles (the, a and an) and conjunctions (and, or, but, nor, etc.). Where appropriate, use abbreviations that are clear and understandable **to all staff** who may need to retrieve and view the file. If possible, develop a control list of abbreviated terms and use it consistently.

  Avoid using special characters in file names – for example, *\ / : * ? " < > | [ ] & $,* because computer operating systems may use these characters to physically organize and store files. In many cases, the system software will prohibit the use of these character. Also, *only use periods to separate the file name from the extension*. The extension indicates the file type or format (.doc, .docx, .pdf, .xlxs, .ppt, etc.) thus – Filename***.Extension***.*

  To separate principal terms within a name, consider using *underscores* or *capital letters* (the latter is called *Title Case*) instead of periods and spaces. This practice will help ensure accurate identification and retrieval of files, especially if they are moved to new/different storage platforms that interpret spaces and periods differently than the system originally used to create and store the files. The examples in the first guideline above use underscores as separators. The following examples show the same names using capital letters as separators. The use of capital letters may be preferred because the practice helps shorten file names and may facilitate/speed file retrieval.

  Examples:

  ContituentResponseSmithJane20210804.doc.

  Project01CharterFinal.ppt

  NewsReleaseProgramAlpha20210301.docx

  RevenueReport20210415.xlsx

  PasswordUsePolicyFinal20210201.pdf

  Contract01234OfficeSupplies.doc

  ProcessingBureauStatusReport0802021.docx

  SafetyCommitteeMeetingMinutes03062021.docx

- **Use dates in a consistent manner**. The preferred date format follows the International Standards Organization (ISO) standard date notation (ISO 8601) of year, month, day - YYYY_MM_DD or YYYYMMDD. If the date is a key retrieval element, place it either at the front or end of the file name consistently:

Examples (without separating segments of the date):

News_Release_ProgramA_**20210301**.docx

News_Release_ProgramB_**20210420**.docx

News_Release_ProgramY_**20211020**.docx

Examples (with underscores separating the segments of the date):

2021_05_01_ Revenue_Report.xlsx

2021_05_02_ Revenue_Report.xlsx

2021_05_03_ Revenue_Report.xlsx

- **Where applicable, use a consistent versioning format.** If you store drafts or versions of documents, presentations, reports or other content, use a consistent format to name the versions. Consider using the letter ***v*** to indicate draft version and numbering succeeding versions sequentially. Label the final product as ***Final***.

  Examples:

  Password_Use_Policy_**v01**_20210301.pdf

  Password_Use_Policy_**v02**_20210302.pdf

  Password_Use_Policy_**v03**_20210303.pdf

  Password_Use_Policy_**Final**_20210302.pdf

- If you use sequential numbering, pad the numbers in the series with leading zeros.

  Examples:

  Contract_ Office_Supplies _**01234**_.doc

  Contract_PPE_**01235**.doc

  Contract_Copier_Maintenace_**01236**.doc

- **Document your naming conventions** in a document or plain text file and give the file a descriptive name -- for example, in Title Case, FileNamingConventionsSmithWilliam.txt. Store the file in a conspicuous space such as your desktop or notebook Documents folder, or on a shared network drive or Cloud storage area allotted to you.

- **If appropriate, consider harmonizing your computer file names with related manual (paper) file names.**

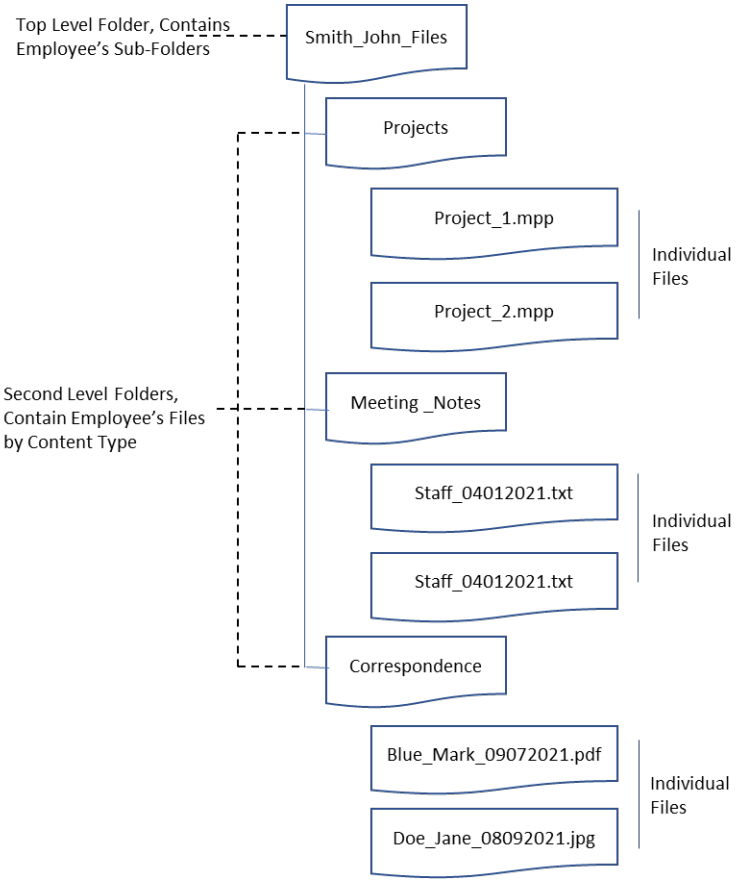
Folder Name Guidelines

Folders are collections of related files. Folders may also contain multiple subfolders. Arranging related files in electronic folders aids in organizing, accessing, managing and disposing of your electronic content.

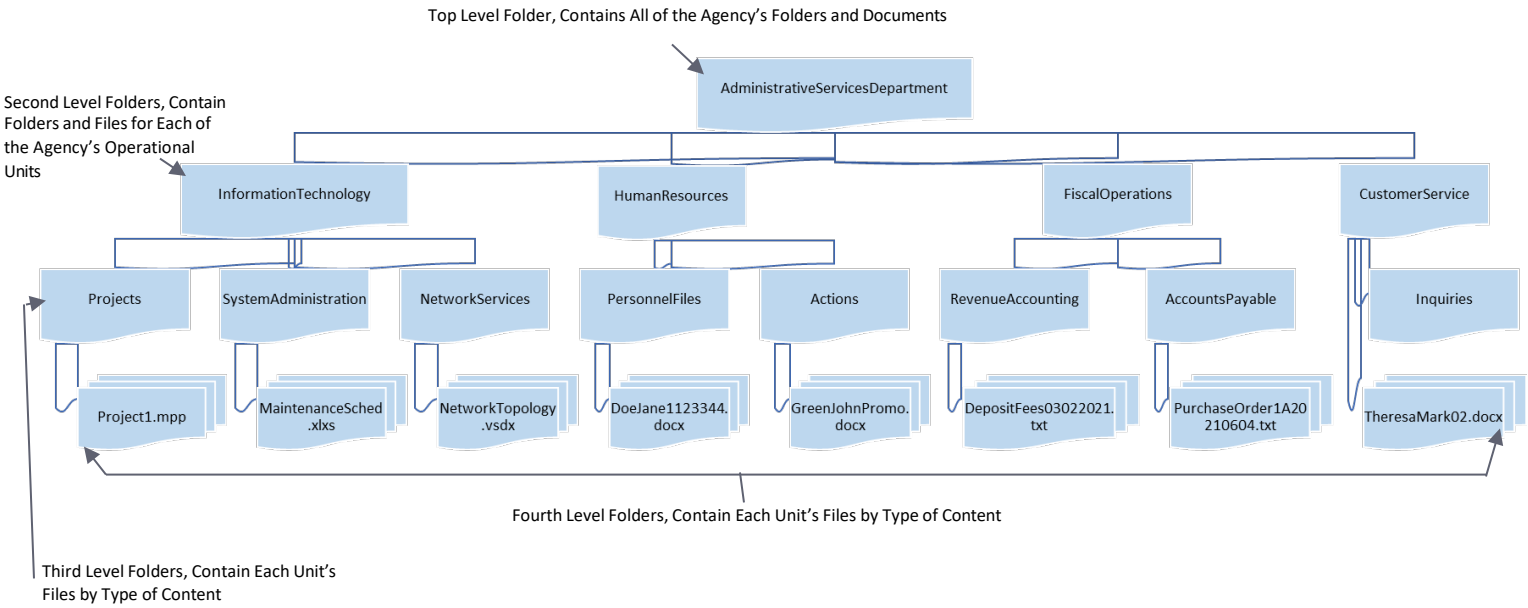
- **Use a hierarchical structure to organize folders.** The structure can be based on an organizational hierarchy or hierarchies based on functions, events, activities or other criteria. Hierarchical structures work well for individuals and can be applied effectively on an organization-wide basis. For instance, folder structures can be applied to centrally controlled file shares, collaboration sites, video conferencing platforms and Cloud-based storage areas.

- **Use the file naming conventions** outlined in the preceding section when naming folders.

  Example of a simplified folder structure for an individual employee (underscores used to separate terms in the folder and file names):



Example of a simplified folder structure for an organization using Title Case (capital letters used to separate terms in the folder and file names):



References

Harvard Medical School. (2021). *File naming conventions.* **https://datamanagement.hms.harvard.edu/collect/file-naming-conventions**

Maguire, L. (2017, July). *File naming conventions: Simple rules save time and effort.* **https://www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/File%20Naming%20Conventions%20July%202017.pdf**

Minnesota Historical Society. (2012, March 1). *Electronic records management guidelines, file naming, Version 5*. **https://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/FileNaming-V5-march2012.pdf**

National Institute of Standards and Technology. (2016, March). *Electronic file organization tips.* **https://www.nist.gov/system/files/documents/pml/wmd/labmetrology/ElectronicFileOrganizationTips-2016-03.pdf**

North Carolina Department of Natural and Cultural Resources. (2019). *Best practices for file naming, version 2.0.* **https://files.nc.gov/dncr-archives/documents/files/filenaming.pdf**

Princeton University Library. (2020, October 21. *Research data management at Princeton, file naming.* **https://libguides.princeton.edu/c.php?g=102546&p=930626#:~:text=File%20naming%20best%20practices%3A&text=File%20names%20should%20be%20short,periods%20or%20spaces%20or%20slashes**

Smithsonian Libraries. (2018, February 28). *Research data management best practices, naming and organizing your files*. **https://library.si.edu/sites/default/files/pdf/rdm_best_practices.pdf**

Stanford Libraries. (n.d.). *Best practices for file naming*. **https://library.stanford.edu/research/data-management-services/data-best-practices/best-practices-file-naming**

Wisconsin Historical Society. (2017, October). *Best practices for naming electronic records.* **https://www.wisconsinhistory.org/pdfs/la/FileNaming-Final.pdf.**

York University. (n.d.). *Tip Sheet 6 - Naming conventions for electronic files and folders.* **https://ipo.info.yorku.ca/tool-and-tips/tip-sheet-6-naming-conventions-for-electronic-files-and-folders/**

Guidelines on Retention Scheduling Public Records Stored on Electronic Messaging Platforms

Updated 12/20/2024

Introduction

These guidelines include suggested action steps for creating retention and disposition policies for public records created via electronic messaging systems in formats such as text, chat, instant messages and voice messages. Electronic messaging allows for real time exchange of digital information and for storage of the information for later use. Various providers, such as Google, Zoom and Microsoft include chat and instant messaging resources in their collaboration platforms. Chat and instant messaging are available via social medial platforms like Facebook. Also, Internet service providers, telecommunications firms and information technology businesses offer text messaging for users of mobile devices such as smart phones and tablets, as well as facilities to record and store voice messages.[1]

Applicability of Public Records Law

The foundation for this document is the legal imperative expressed in the State's public records law (N.J.S.A. 47:3 et seq.). That is, irrespective of medium, all records that are generated and received during governmental operations in New Jersey are public records and subject to the State's records management and archival requirements. Records generated and received via electronic messaging platforms are therefore subject to the State's public records law.

Audience

Generally, these guidelines are designed for professionals who work in records and information management capacities and who have some familiarity with the State's records management program as described in the State Records Manual. However, generalist managers and administrative support staff may also find the guidelines useful.

Notes on Scope and Foundation for this Document

This document covers retention scheduling for electronic messaging. It does not cover the management of electronic mail or social media.

Guidance on managing email may be found in the State Records Manual (pages 39-48).

The State's Guidelines on Retention Scheduling Public Records Stored on Social Media Platforms address social media. **The social media guidelines form the foundation for dealing with electronic messaging as well. The reader will note that the processes and methods set forth in this document track those found in the social media guidelines.**

[1] See the National Archives and Records Services' Guidance on Managing Electronic Messages and Electronic Messages White Paper. While now somewhat dated, they still provide useful insights into defining and managing electronic records. The State of North Carolina also provides helpful guidance in this area in its publication Best Practices for Electronic Communications Usage in North Carolina.

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.

Action Steps

1. Inventory Electronic Messaging Platforms

   Start the retention scheduling process by inventorying and documenting all the electronic messaging services and platforms employed by the agency – for example, accounts/sites using Facebook, TEAMS, Zoom, Google Workspace, mobile telephone and other voice communication services that include voice recording, etc. Describe the content that resides on each platform and the organizational functions that each one addresses – for instance, dissemination of scheduling information, emergency notices, constituent services, ideation, meeting dialogues, etc.

2. Conduct a Value Assessment(s)

   Based on the descriptions and functional purposes of the platforms, assign values to the content (records) they contain. Following are value dimensions that could be assigned. The value dimensions are tied to a simple range: low (records with little or no lasting retention value); medium (records with some short-term – less than 10 years, retention value); and high (records with greater than 10 years retention value).

   Note that records may bridge or overlap the value dimensions. For example, a particular electronic messaging service/platform may contain content that has both informational and planning and decision support/knowledge management values. If this occurs and the overlapping dimensions have different (higher/lower) values with respect to retention and disposition, the recommended policy decision would be to assign the higher value to the content.

   Value dimensions a and b below are likely to be the two most common dimensions that agencies encounter.

   a. General Information **(retention value – low)**. Electronic messaging services are frequently used for the exchange routine information such as meeting reminders, general questions/answers shared among staff on technical matters or simple requests for the return of a telephone or online call. Content generated for such purposes likely has no lasting value, and can therefore be classified as routine/non-sensitive in nature.

   b. Operational Information Exchange **(retention value - low to medium)**. Electronic messaging can augment dialogue among agency staff, service providers and constituents. For instance, chats may serve to enhance information exchange among participants in online meetings and as a customer support channel for an agency contact center. Records

produced in this category can include exchanges such as general feedback, question/answer streams, ratings, voting, likes/dislikes, etc. These records may also have secondary uses such as operational research on the effectiveness and efficiency of customer support programs and online service offerings.

c. Transactional and Operations Management **(retention value - low to medium)**. Electronic messaging may connect with an agency's service delivery processes. For example, agencies may use texts and chats to deliver tailored electronic content or private links (links to content directed to a specific individual) in response to document filing or information access requests.

d. Planning and Decision Support/Knowledge Management **(retention value - medium to high)**. Electronic messaging may aid executives and specialized staff (technologists, public information officers, legal advisors, budget analysts, etc.) who develop plans and rules that guide the actions of the entire organization from a long term or strategic perspective. In this context, electronic messaging can contain valuable information including intra-agency and external discussions and information on a wide range of topics including: economic trends; policy research; constituent sentiment; legal issues; evolving products/technologies that impact agency operations; prevailing political trends; and changes in societal perspectives. Electronic messages may also support collaborative efforts aimed at idea development and product or service innovations via feedback from individual citizens, organizational actors and various other stakeholders.

e. Legal/Compliance **(retention value – high)**. This is an encompassing category which, *depending on the agency's mission*, may envelope all the prior categories. It relates to the management of records, in all forms, for adherence to statutory and regulatory record-keeping requirements. Agencies that employ electronic messaging in tightly regulated contexts should be aware that legal, contractual and rules-based requirements may attach to the records generated/stored by the electronic messaging service/platform. Agencies may be compelled to produce records in this category in discovery processes associated with litigation, audits and internal investigations.

f. Historical **(retention value - high)**. Historical records hold long-term or permanent research value. They serve to preserve our intellectual heritage and to document important social, political, economic and cultural developments. Thus, they have enduring relevance. Over time, some portion of electronic messaging will document significant events, and/or trends in an aspect of human development, and/or record time- and context-bound perceptions/attitudes about significant human endeavors.

3. Assign Retention and Disposition Policies to the Records

Based on the value assessments conducted in Action Step 2, assign retention and disposition polices to all electronic messages that the agency generates and stores. This may be done by creating new agency-specific records retention schedule items (record series) or using existing

records series.

For information on how to create new agency specific record series, consult the State Records Manual, pages 10 – 13. Note that RMS can assist in establishing on-going authorizations for disposition, which will enable agencies to dispose of low value content routinely for renewable time periods (6 months or year) without having to submit requests for individual disposition actions. Contact RMS for assistance in setting up on-going disposition authorizations.

Following are suggestions for use of existing general record series and disposition policies that align with the value dimensions discussed in Action Step 2.

For county and local agencies and authorities, Table 1 lists suggestions for use of existing general record series and disposition policies that align with the value dimensions discussed in Action Step 2. State agencies must follow the State General Records Retention Schedule.

State agencies should follow the General Schedule items listed in Table 2.

All agencies should bear in mind that litigation hold requirements may apply to electronic messaging. As with all public records, hold orders will have the effect of tolling disposition actions on responsive electronic messaging records.

Table 1

Record's Value	Examples Existing Record Series	Disposition
General Information (Low)	*Electronic Administrative Resource Files* – for example, meeting reminders, exchange of web links (URLs) on technical topics, routine announcements about agency events or relevant news articles, etc.	Retain until no longer needed for administrative purposes/destroy
Routine Information Exchange (Low-Medium)	For low value, *Electronic Administrative Resource Files* -- for example, chat logs and dialogues associated with routine operational meetings For medium value: *Correspondence, Internal* – for example, routine exchanges relative to the processing and disposition of routine customer service issues *OR*	Retain until no longer needed for administrative purposes/destroy 1 year/destroy

		3 years/destroy **(use of data migration recommended; see next action step)
Transactional and Operations Management(Low-Medium)	For low value*, Electronic Administrative Resource Files*, for example, confirmations of receipt and completion of document/application filings or information access service requests For medium value*:* *Correspondence, External* -- for example, customer feedback relative to public programs or service quality *OR* *Administrative Subject File*	Retain until no longer needed for administrative purposes/destroy 3 years/destroy **(use of data migration recommended; see next action step) 3 years/destroy **(use of data migration recommended; see next action step)
Planning and Decision (High)	*Correspondence, Policy* -- for example, exchanges among mid to senior level staff regarding the development, progress or status of a public program or function	25 years with archival review **(use of data migration and long-term repositories required; see next action step)
Legal/Compliance (High)	*Correspondence, Policy* -- for example, exchanges regarding decisions to award of contracts and directives relative to compliance with regulatory and/or compliance regimes	25 years with archival review **(use of data migration and long-term repositories required; see next action step)
Historical (High)	Permanent based content and context – for example, exchanges between top level administrators regarding key issues affecting the State, including State-wide emergencies, sensitive investigations, executive staff appointments, etc.	Permanent with archival review **(use of data migration and long-term repositories required; see next action step)

Table 2

Record Series	Examples Existing Records that Can be Included in this Series	Retention/Disposition
Schedule G100000-014-3000-0001 Electronic Communications Records General/Routine Information Communications	Records in this series include the exchange of routine information such as meeting reminders, general questions/answers shared among staff on technical matters pertaining to operations or projects, or simple requests for the return of a telephone or online call. Records in this series can also include general feedback, question/answer streams, ratings, voting, likes/dislikes, etc.	1 Year/Destroy
Schedule G100000-014-3000-0002 Electronic Communications Records Operational Information Exchanges	Records produced in this series encompass the same types of communications listed under 3000-0001, but in this case, the records are specifically targeted for secondary uses such as operational research on the effectiveness and efficiency of customer support programs and online service offerings.	3 Years/Destroy
Schedule G100000-014-3000-0003 Electronic Communications Records Service Transactions	These types of records involve service transactions such as delivery of digital content in the form of reports and other public documents, and work order entry and tracking information.	3 Years/Destroy
Schedule G100000-014-3000-0004 Electronic Communications Records Electronic Communications Records - Planning, Decision Support And Knowledge Management	These records relate to collaborative exchanges specifically targeted for the planning and development of new or substantially modified public programs. The series does not include exchanges or information derived therefrom used for adjusting or enhancing routine public services.	25 Years/Archival Review

4. Choose Modes of Storage for Electronic Messages with Consideration of Policies Controlling Use of Platforms and Devices

   By way of background, it is common for agencies to use third party contractors, including cloud and cellular service providers, for electronic message storage. Also, depending on the nature of the messaging system and service, individual employees may store messages on their agency-assigned devices and/or possibly on their own devices.

   Contractors may offer varying levels of service, quality and storage capacities that could change over time. This can make the underlying storage technologies and service levels for the agency's electronic messaging program uncertain and unstable. Likewise, use of privately owned devices

is fraught with complications, ranging from exposure to records loss to challenges with responding to access requests associated with discovery, audits, investigations and Open Public Records (OPRA).

a. Given the backdrop above, when addressing storage solutions for electronic messaging, agencies should consider the following policies:

- Prohibit use of private devices for the exchange of public records (any message dealing with official agency business).
- Prohibit or at least strongly discourage use of electronic messaging for public records with retention periods greater than three (3) years or generally, any messaging that involves investigations, audits, the formulation of public policy and/or administration of legal processes such as contracts.
- For all electronic messaging contractors, including those who provide voice message recording services, employ contractual provisions that address public records retention and disposition requirements. (See example language for Cloud-based platforms listed in the RMS Cloud storage guidelines, State Records Manual, page 115).

b. Choose appropriate storage solutions or mix of solutions.

- Trusted Digital Repository (Preferred). Implement a collection tool that allows the agency's centralized information technology and/or records management program to perform scheduled extraction and migration of electronic messages from all sources to an agency-owned or controlled trusted digital repository.[2] A trusted digital repository enables the agency to store digital records, including electronic messages, in formats that assure access, use and analysis of the records for the entire length of their retention periods.[3] Such functionality is critical for long-term and permanent records and recommended for records that must be maintained for three (3) years or more.

  The trusted digital repository can be an agency owned computer storage facility and/or a Cloud-based platform, either of which meets or exceeds the requirements listed in the RMS Cloud storage guidelines (State Records Manual, page 115).[4]7 For long-term or permanent storage requirements, the repository should use file formats that are compatible with long-term/permanent storage. After records are successfully migrated to the trusted digital repository, the agency may delete the migrated content from the source platform.

[2] The Sedona Conference published an accessible discussion of collection software in the context of small case discovery efforts. See The Sedona Conference. (2022). *Primer on Managing Electronic Discovery in Small Cases*, The Sedona Conference, Phoenix, AZ. The publication includes references to the Sedona Conference's more expansive guidance on the discovery life-cycle and resources used to support it.

[3] The Research Library Group/Online Computer Library Center (RLG/OCLC) provides a formal, encompassing definition of trusted digital repository in its publication entitled Trusted Digital Repositories: Attributes and Responsibilities. As noted in the narrative, while trusted digital repositories focus on long-term and permanent storage, for purposes of this guideline, short-term records may also be included for ease of administration.

[4] The Cloud storage guidelines are useful because they address many requirements for long-term records storage and access. The RLG/OCLC publication cited in the previous footnote also provides valuable information on these and other key characteristics, as does the OCLC's publication entitled Trustworthy Repositories Audit & Certification: Criteria and Checklist.

Also, use collection tools that extract/archive metadata associated with each targeted electronic message. As defined by the National Archives and Records Service (NARA), *metadata* are data elements that "provide administrative, descriptive, and technical information that describe the structure and content of electronic records."[5] Examples of metadata for electronic messages include authors name, cellular phone number, organizational affiliation, recipient names/cellular phone numbers, subject line, date created/sent, etc.

With regard to file formats used for long term storage, use standards and guidelines published by the New Jersey State Archives. As of the publication of these guidelines, the Archives had drafted a table of preferred and acceptable formats, but had yet to publish it. Check with the Archives on the status of the table (609-633-8304 or 609-292-6260).

- Centralized Agency Collaboration Platform. Agency collaboration platforms such as Office 365/TEAMS and Google Workspace provide tools that enable agencies to set enterprise, organization-wide retention/disposition policies for messaging streams like chats and other digital communications. Use these tools whenever possible. Also consider moving messaging streams with long-term retention values to a trusted digital repository as described above.

- Back-ups and Data Export/Import. If the agency's electronic messaging platform contains records with medium to long-term value, and does not accommodate retention/disposition management or collection tools, migrate the content periodically to a trusted digital repository via importation of back-ups or through the use of data export/ import applications. Be sure to test the back-up/recovery tools and export/import applications.

- Service Provider Platforms. If the agency uses a platform that operates separate from its centralized collaboration and storage facilities and it is not possible to set up a trusted digital repository, consider relying on the messaging service provider exclusively. This approach is viable only if the records involved do not have long term retention value. Ensure that the provider has back-up/recovery tools in place to guard against data loss, or that there are data import/export applications that can be used to make accessible copies of the records.

[5] See NARA Bulletin 2015-04, Metadata Guidance for the Transfer of Permanent Electronic Records. NARA's guidelines on file formats for transfer of permanent records and metadata for transferred files may also prove helpful in determining file format and metadata requirements for trusted digital repositories.

- Individual Devices. In cases where employees are creating and storing message streams on individual devices that are not automatically synchronized with an agency-controlled repository, institute a policy that highlights the need for employees to attend to retention and disposition directly. As part of the policy, require periodic copying of messages that have longer term retention value (for purposes of this presentation, two years or more) to a designated repository. Ideally, this would be accomplished through the use of a collection tool made available to employees (see discussion under (Trusted Digital Repository). If it is not possible to employ a collection tool, cutting and pasting message streams is a possibly, but be aware that this approach is limited and may not allow for the capture of metadata that is critical for access, discovery and research purposes.[6]

5. Implement the Retention and Disposition Program

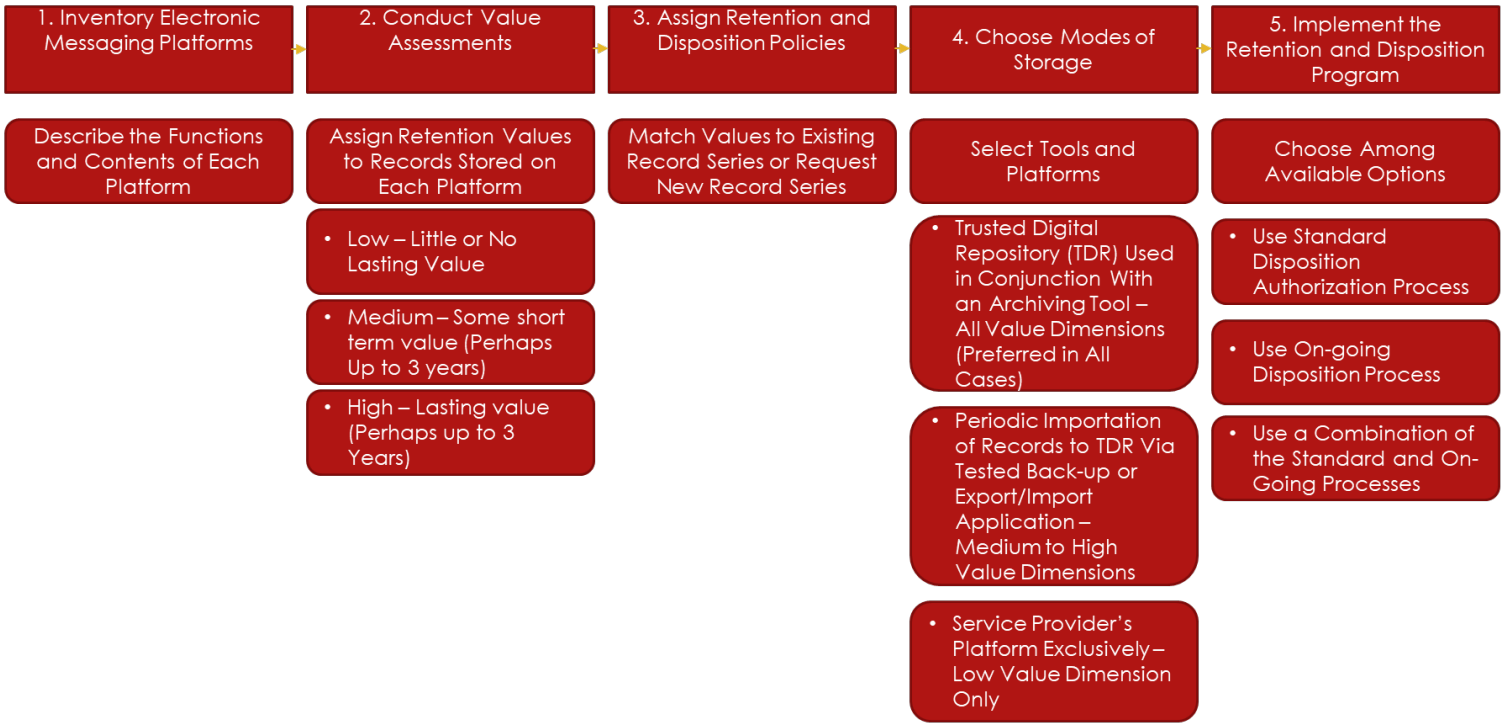
   After completing the four preceding steps, choose to conduct the retention and disposition program via:

   a. The standard disposition authorization process (State Records Manual, pages 10 – 13);
   b. The on-going disposition authorization process (contact RMS for assistance in setting up an on-going authorization); or
   c. A combination of the processes for different sites.

[6] Internet searches will surface examples of these policies. Some examples include policies promulgated by New York City, The State of Washington and the University of Oregon.

SUMMARY OF ACTION STEPS

The Action Steps Contained in the Guidelines
(Conceptual Approach to the Retention and Disposition Program)



Chapter 15

General E-mail Retention and Disposition Program Frameworks

1.0 Introduction

Electronic mail systems, commonly called e-mail, are the communications method of choice for many public officials and public employees in New Jersey. Public employees use e-mail for mundane administrative communications, as well as for communications involving substantive information or records previously committed to paper. This nexus of communications and record creation/keeping compels public agencies to treat e-mail messages as records.

The management of e-mail systems touches on many important operational concerns including privacy, business administration, vital records management, security, auditing and public access. Therefore, the need to manage e-mail messages and systems in a structured fashion, on an ongoing basis, is clear. In this connection, e-mail retention scheduling and disposition programs are important parts of a structured and sustainable e-mail management platform.

2.0 Purpose

This chapter contains descriptions of two conceptual frameworks that county and local public agencies may use to manage retention and disposition of electronic mail (e-mail) produced, received and/or stored by their offices.* Agencies are encouraged, but not required, to consider them. Agencies may consider adopting the frameworks in whole or in part. They may also consider employing hybrids that incorporate aspects of both frameworks.

By applying the concepts included in these frameworks, agencies will augment their ability to manage e-mail messages and attachments as public records per the Destruction of Public Records Act, P.L. 1953, c. 410 (N.J.S. 47:3-16). This, in turn, will enhance their capacity to capture, retain and dispose of all electronic records uniformly. Likewise, application of concepts from the frameworks will improve their ability to meet the requirements of New Jersey's Open Public Records Act (OPRA) efficiently. Keys to success in this area include the ability to establish procedures that set forth how long e-mail and attachments must be maintained, and how and when to dispose of the content in an orderly, documented and accountable manner. Storage and operational efficiencies will result from timely disposition of e-mail and attachments as well.

Note that the frameworks relate to systems maintained by public agencies or by third party service providers on behalf of any agency, whether on the agency's premises or on the service provider's premises. E-mail retention and disposition requirements apply to all e-mail systems and content – current and any legacy (decommissioned) systems. Finally, the guidelines assume agencies are managing their e-mail in electronic format --

that is, they are not printing out and storing e-mail on paper or other hardcopy media for retention purposes.

Agencies are encouraged to contact the Department of the Treasury's Records Management Services (RMS) unit at 609-530-3201 before implementing e-mail retention and disposition programs. RMS will offer feedback with respect to agency programs, along with suggestions on how to apply the frameworks covered herein. Further, RMS will facilitate the authorization of disposition actions implemented under these frameworks or under other approaches that meet the basic requirements of the public records laws of this state.

*(State agencies are currently required to follow Circular Letter 14-2 DORES/OIT for their e-mail programs.)

3.0 Definitions

For purposes of this presentation, the following definitions apply:

"Records series" means a group of records that is stored together because the included records relate to a common function, topic, purpose, transaction or other unifying feature associated with their creation, access or use.

"Individual records series" means any record series that appears on an approved Records Retention Schedule (general schedule or agency specific) that is not a broadband or general records series.

"Long-term record series" means any records series that must be maintained for longer than seven years.

"Permanent record series" means any records series that must be maintained indefinitely.

"Broadband/general records series or broadband/general e-mail records series" means a record series that encompasses a group of individual records series, categorized by a common retention period or common range of retention periods, which facilitates retention and disposition management. The National Archives and Records Administration developed a program (Capstone) for Federal agencies that uses this scheduling method.

"E-mail records and e-mail content" means any e-mail message, attachment to an e-mail message and associated information or meta-data, such as dates and times sent/received, sender/receiver addresses, message format, etc.

"E-mail systems" means computer-based systems that transport messages from one computer user to another. E-mail systems range in scope and size. They may be local platforms that move messages to users within an agency or office over a local area network (LAN) or enterprise-wide e-mail systems that carry messages to various users in various physical locations over a wide area network. The latter may include systems that send and receive message around the world over the Internet. Often the same e-mail system serves all three functions.

"Record copy or record copies" means the original, official version(s) of a record or records.

"Traditional records disposition procedures" means listing individual records series on Records Disposition Requests through the system known as ARTEMIS and executing disposition actions based on the use of individual records series.

4.0 Frameworks

The following frameworks relate to the two approaches highlighted in Chapter 7, Electronic Mail . The first connects with Approach 1, and centers on the adoption of traditional records retention schedules and procedures. The second connects with Approach 2 and involves the use of a broadband/general e-mail records retention schedule coupled with centralized management of e-mail retention and disposition.

**Note: Due to the still-evolving nature of e-mail technologies and processes, RMS anticipates that new and improved approaches to e-mail management (including retention and disposition regimes) will emerge as time goes on. Accordingly, agencies are encouraged to share with RMS their experiences in applying the two approaches in Chapter 7 and associated frameworks discussed here, or indeed, to propose alternative retention/disposition regimes designed to meet the legal requirements of the public records law. Such feedback will help RMS develop and post responsive guidance in this manual on a continual basis.

4.1 General Discussion

Like any other form of record-keeping technology, public agency e-mail systems contain public records that can be classified and matched to individual record series that are listed within approved records retention schedules. Accordingly, if agencies are able to reliably, consistently and accurately identify e-mail content by individual record series, they can apply traditional records disposition procedures, as per Framework 1, to their e-mail systems. In this regard, a word of caution is in order. In practical terms, given the current state of e-mail technology, agencies may indeed find it difficult to achieve the levels of reliability, consistency and accuracy required for successful implementation of Framework 1. Agencies that lack the ability to automatically apply centrally controlled classification, retention and disposition rules will likely be exposed to risks of general end-user noncompliance, inconsistent application of agency rules and/or proliferation of uncontrolled offline/near-line e-mail content.

In contrast, using Framework 2 with centralized vaulting/journaling provides a number of significant benefits, including: efficient centralized management of most all e-mail communications under a single State Records Committee-approved records series, while also allowing for the identification, segregation and management of long-term and permanent e-mail records; uniformity and greater transparency in e-mail retention scheduling and disposition; efficient system administration; and provision of a platform that facilitates the future adoption of more advanced records and electronic content management techniques/technologies that encompass all forms of electronic records.

4.2 Framework 1

This framework is based on the use of traditional records retention schedules and procedures.

4.2.1 Prerequisites (Foundational Elements)

In advance of adopting this framework, address the following foundational elements.

4.2.1.1 Governance

Governance includes the formal institutional structures through which agencies implement and maintain the policies, procedures, techniques and technologies that will support the e-mail retention and disposition framework. Governance structures will vary from jurisdiction to jurisdiction but, in general, they include executive leadership and sponsorship (provided through the endorsement of the governing body), along with legal advice given by counsel. Active involvement by the agency's lead records management and technology officers, human resources representatives and line-of-business managers is also required.

Ensure there is executive sponsorship for and approval of the framework, and that key actors are involved in the implementation process. Assign responsibility for administering the framework to the lead technology and records management officers.

4.2.1.2 Electronic file plan

Electronic file plans encompass classification schemes for electronic records. For purposes of this framework, file plans should include:

- Titles for each type of record maintained in the e-mail system – for example, internal correspondence, external correspondence, administrative case files, etc.
- Brief descriptions of the e-mail titles. (Describe the content and function of each title.)
- Custodians (List the offices or functions responsible for maintaining the e-mail titles or indicate that the titles are received/generated and stored at the Enterprise or organization-wide level. If possible, designate the custodians responsible for record copies of specific titles.)
- Record series designations. (Match each title with an approved records schedule and item number.)
- Storage locations. (Indicate all electronic storage facilities in which the content is stored – for example, end-user mailboxes, vault/journal, network drives, separate content management system, etc.)
- Back-up information. (Indicate back-up cycles for the e-mail content and retention timeframes for content contained in each back-up cycle.)
- Disposition instructions. (Per the approved records schedules, for each title, list the actions to be taken after the records retention periods have expired. For titles involving long-term and permanent record series, list the actions to be taken after the records are no longer needed by the agency or office custodians for administrative, legal or fiscal purposes – for example, retain in end-user mailbox (feasible, but not recommended), transfer to network folder, transfer to content management system, etc.)

Publish the file plan and distribute it to each employee who uses the agency's e-mail system, along with instructions on how to set up electronic folders in each storage area that enable employees and technical staff to use the file plan. For example, organize the folder structure by office and then by the title/record series within the office folder. In turn, title and record series folders can be broken down by topics and dates that are meaningful to the office staff.

Other viable methods of folder organization include use of key words, process names, account designations (for high level decision-makers) and case/project names.

Train all staff on how to use the file plan and records disposition process.

Audit for and/or evaluate levels of compliance with the file plan and retention/disposition program on a regular basis.

4.2.1.3 Acceptable use policies covering e-mail and the Internet

Acceptable use policies describe the permissible uses of e-mail and the Internet (a resource aligned with e-mail usage), employees' responsibility with respect to these permitted uses and the potential sanctions for noncompliance. For reference, see the State of New Jersey's policies (Internet and E-mail).

Ensure each employee receives and reviews these policies.

4.2.1.4 Litigation hold process

This process covers the agency's obligation to identify and preserve records, including e-mail and attachments, which are relevant to civil and criminal proceedings, as well as audits and internal agency investigations. Broadly, it encompasses the technical and operational requirements for identification, preservation and, ultimately, production and presentation of relevant records. Litigation hold orders supersede retention and disposition policies. See Chapter 7 of the manual for background information on the litigation hold process.

Ensure all e-mail system administrators, records custodians and legal advisors are aware of and can respond effectively to litigation hold requests.

4.2.1.5 OPRA response/tracking process

E-mail messages and attachments that serve to document organizational functions, policies, decisions, procedures, operations or other official activities, meet the definition of a government record under OPRA. Such content must therefore be made available for public access for the length of its designated retention period, unless it falls under one of the exceptions enumerated in the law and/or administrative regulations.

Ensure all e-mail system administrators, records custodians and legal advisors are aware of and can respond effectively to OPRA requests. See the Government Records Council's guidance to records custodians for more information.

4.2.1.6 E-mail back-up/recovery and disaster recovery/continuity of operations programs

Develop, implement and document a back-up and recovery program for both real time e-mail and vault/journal content, if applicable. Also institute a fail-over disaster recovery/continuity of operations capability for the e-mail system. Generally, these tasks are the responsibility of the information technology officer and, if applicable, third party service providers.

4.1.2.7 System security

Develop the technical, procedural and physical controls required to prevent unauthorized or unintended access, use, distribution, modification or destruction of e-mail records. Also develop controls that assure message authenticity, integrity, accessibility and usability over time. Generally, these tasks are the responsibility of the information technology officer and, if applicable, any third party service providers.

For more background information on the nature and scope of security programs in networked computing environments, see the research paper entitled Security for the Networked Enterprise, Elements of a Holistic Approach in the Appendix.

4.1.2.8 Employee separation procedure

Implement a process that ensures that, upon notification of a separation, all of the former employee's e-mail is vaulted or otherwise preserved and retained for the length of the longest retention period associated with the e-mail content stored by that employee.

4.1.2.9 Other best practice points

End-user awareness and training programs are essential to the success of e-mail retention and disposition programs.

E-mail retention and disposition requirements apply to all e-mail systems – current and any legacy systems. Therefore, if agencies are updating to new e-mail systems, they should arrange to have the e-mail from the legacy system migrated to and managed by the replacement system. Alternately, they should manage the legacy content by storing it on accessible, readable and secure media for the length of the latest retention period of any record series included in the system.

Finally, agencies should also direct their internal and/or third party audit teams to include checks for compliance with general records management requirements, including compliance with the e-mail retention/disposition program.

4.2.2 Adopting Framework 1

After addressing the fundamental elements above, take the following steps to adopt the framework.

4.2.2.1 Issue an e-mail records management directive to all employees

Include the following requirements in the directive.

- Any e-mail produced or received in the course of official business is a public record and may not be disposed of unless permission is granted through procedures

established by the State Records Committee under the authority of N.J.S.A. 47:3 et seq.

- Employees must follow the Electronic File Plan and procedures for implementing storage areas that complement the File Plan.
- If appropriate, indicate that non-record e-mail is not covered by the directive, and may be deleted at the employee's discretion.
- E-mail retention periods are set forth in approved records retention schedules and must be followed.
- Designate the officer authorized to submit e-mail disposition requests on behalf of the agency.
- Point out that State's process for records disposition actions must be followed (see information on the State's process on the ARTEMIS site).

4.2.2.2 Adopt and administer the e-mail records retention and disposition program

Formally assign responsibility for administering the framework to the agency's chief information technology manager, lead records management authority or chief administrative officer. The officer assigned this responsibility should work to ensure the agency:

- Has in place all of the foundational elements listed in 4.2.1 above.
- Manages all e-mail content produced, received and/or stored by agency employees during the course of official business as public records, encompassing all content -- messages, attachments and system-produced information that describes the content (meta-data).
- Makes e-mail records available for public inspection in accordance with OPRA.
- Adheres to the e-mail records disposition process as set forth in ARTEMIS.

4.2.3 Implement the e-mail records disposition process

The agency's chief information technology manager, lead records management authority or chief administrative officer should execute or oversee the execution of the steps below at least once per year.

- Identify e-mail records that match individual records series on the agency's retention schedules and/or general retention schedule that are eligible for disposition.
- Document the impending disposition action(s) in an ARTEMIS request(s); ARTEMIS is the State's online records disposition tracking system.
- Upon clearance to proceed, segregate and securely delete the aged e-mail content from all storage facilities – for example, central storage (agency's e-mail vault/journal or archive), end-users' mailboxes, file shares, collaboration sites, electronic content management platforms, back-up media, etc.
- Document the destruction actions as required by ARTEMIS.

For permanent records that are no longer needed by the agency or office custodians for administrative, legal or fiscal purposes, move the content to a designated folder(s) in

accordance with the file plan for the records involved and that resides on a network storage device or content management system.

4.2.4 Implement and administer an annual e-mail system sustainability assessment

The agency's chief information technology manager, lead records management authority or chief administrative officer should conduct a sustainability assessment each year to review the ongoing viability of the agency's e-mail system and, if applicable, the vault/journal platform and content management facility. When applicable, review upgrade options. Consideration of content migration strategies is also part of the assessment. The baseline requirements for the assessment can be found in the New Jersey Records Manual, Chapter 10.

4.3 Framework 2

This framework is based on the use of a broadband/general e-mail records series with a seven- year timeframe, coupled with centralized management of e-mail retention and disposition. It also entails the development of a file plan for electronic mail content that must be retained for more than seven years.

Note that certain key exceptions, many of Framework 2's elements are identical to those found in Framework 1.

4.3.1 Prerequisites (foundational elements)

In advance of adopting Framework 2, address all of the following foundational elements.

4.3.1.1 Governance

Adopt the same elements listed in 4.2.1.1 above.

4.3.1.2 Electronic file plan

Follow the guidelines listed in 4.2.1.2 above, but focus your efforts solely on classifying any e-mail records with greater than seven year retention periods, including permanent e-mail records if applicable.

Management of all other e-mail content will be covered under the broadband/general retention schedule (seven years).

4.3.1.3 Acceptable use policies covering e-mail and the Internet

Adopt the same elements as listed in 4.2.1.3 above. Ensure each employee receives and reviews these policies.

4.3.1.4 Litigation hold process

Adopt the same elements listed in 4.2.1.4 above.

4.3.1.5 OPRA response/tracking process

Adopt the same elements listed in 4.2.1.5 above.

4.3.1.6 E-mail vaulting/journaling with central management of end-user e-mailboxes

Institute an e-mail vaulting/journaling platform that makes copies of all content flowing from/to individual e-mail boxes, across the agency, to a separate, secure and centrally-controlled repository. Also ensure that the platform addresses all end-user mailbox content. Ideally, the latter will be done via a centralized console. In this context, centralized management includes the ability to copy, move/transfer and delete end-user e-mailboxes, or selected content from the e-mail boxes, by an authorized system administrator.

If agencies are unable to manage end-user e-mailbox content centrally, they will have to establish a procedure that allows end-users to copy their e-mailboxes to alternate file formats -- for example, Microsoft's pst format, for storage in a central electronic storage facility, for the length of the seven year period highlighted below or for long-term/permanent retention as applicable. Agencies should note, however, that this type of arrangement may be difficult to manage effectively on a sustained basis. Consequently, agencies that adopt this approach are at greater risk of end-user noncompliance and proliferation of uncontrolled offline/near-line records content.

4.3.1.7 E-mail back-up/recovery and disaster recovery/continuity of operations programs

Adopt the same elements listed in 4.2.1.6 above.

4.3.1.8 System security

Adopt the same elements listed in 4.2.1.7 above.

4.3.1.9 Employee separation procedure

Adopt the same elements listed in 4.2.1.8 above.

4.3.1.10 Other best practice points

Adopt the same elements listed in 4.2.1.9 above.

4.3.2 Adopting Framework 2

Take the following steps to adopt the framework.

4.3.2.1 Issue an e-mail records management directive to all employees

Include all of the requirements listed in 4.2.2.1, plus the following:

- The broadband retention period for e-mail is seven (7) years.
- Employees will be responsible for complying with any subsequent directives for retaining and disposing of any electronic content including, where applicable, e-mail content that is not covered by the seven year broadband period.
- In accordance with the Electronic File Plan, outline the procedure for declaring and moving long-term and permanent e-mail records to designated long-term/permanent storage areas. Long-term and permanent content should be classified and indexed within the vaulting /journaling platform and either managed in place on the platform or migrated to a designated long-term/permanent storage

area within an agency-wide electronic content management system at intervals determined by lead information technology and records management staff.

4.3.2.2 Adopt and administer the e-mail records retention and disposition program

Formally assign responsibility for administering the framework to the agency's chief information technology manager, lead records management authority or chief administrative officer. The officer assigned this responsibility should work to ensure the agency:

- Has in place all of the foundational elements listed in 4.2.1 above.
- Manages all e-mail content produced, received and/or stored by agency employees during the course of official business as public records, encompassing all content -- messages, attachments and system-produced information that describes the content (meta-data).
- Makes e-mail records available for public inspection in accordance with OPRA.
- Adopts the broadband/general e-mail retention period of seven (7) years. Generally, the broadband/general record series will encompass any record that must be kept seven (7) years or less.
- Manages e-mail records subject to the seven year retention period centrally via a vaulting/journaling system with automated management of end-user mailboxes, or via coordinated action between the information technology officer and end-users. (See next item on electronic records cumulative retention periods exceeding seven years.)
- Will, within a timeframe set by the agency's chief information technology manager, lead records management authority or chief administrative officer, identify all electronic records, including e-mail, with retention periods exceeding seven years.
- Adheres to the e-mail records disposition process as set forth in ARTEMIS.

4.3.2.3 Implement the e-mail records disposition process

The agency's chief technology officer or lead records management authority should execute the steps below at least once per year.

- Identify centrally-stored end-user e-mail content that is covered by the broadband retention period and aged to seven years or more and any long-term e-mail content that has reached or exceeding its long-term retention period.
- Document the impending disposition action(s) in an ARTEMIS request(s); ARTEMIS is the State's online records disposition tracking system.
- Upon clearance to proceed, segregate and securely delete the aged e-mail content from all storage facilities – for example, central storage (agency's e-mail vault/journal or archive), end-users' mailboxes, file shares, collaboration sites, electronic content management platforms, back-up media, etc.
- Document the destruction actions as required by ARTEMIS.

For permanent records that are no longer needed by the agency or office custodians for administrative, legal or fiscal purposes, move the content to a designated folder(s) in

accordance with the file plan for the records involved and that resides on a network storage device or content management system.

4.3.2.4 Implement and administer an annual e-mail system sustainability assessment

The agency's chief information technology manager, lead records management authority or chief administrative officer should conduct a sustainability assessment each year to review the ongoing viability of the agency's e-mail system, including its vault/journal platform and content management facility. When applicable, review of upgrade options. Consideration of content migration strategies is also part of the assessment. The baseline requirements for the assessment can be found in the New Jersey Records Manual, Chapter 10.

Under Framework 2, success in handling e-mail records with long-term and permanent retention periods includes procedures and preferably, an automated system, which collectively enable the agency to use Electronic File plan classifications to flag in-bound and out-bound communications for segregation and long-term/permanent retention/management on the vault/journal platform, a network drive or more advanced content management system.

In all cases, the long-term/permanent storage platform should allow the agency to search and retrieve all stored content by multiple tags or indexes – e.g., sender/receiver, subject, date sent/received, message body (searchable text in message body), etc. The platform should also have sufficient security features to prevent unauthorized access, use or modification of stored content. The platform must allow access to authorized end-users and support searching/retrieval for OPRA and litigation hold purposes.

If the agency opts for less than real time vaulting/journaling, it should develop and distribute a directive that prohibits the deletion of any e-mail content prior to the last completed vaulting/journaling job run, and establish a communications plan that ensures all employees are aware of the last completed archive job run date.

To mitigate storage costs, agencies may opt to implement tiered storage arrangements for their e-mail vault/journal platform – moving content from online storage, to secondary disk storage and then to tape or other off-line media.

References

This section covered the basic nature of social media and social media content. It highlighted how these items are becoming increasingly important assets in public information and records system architectures, and provided tentative guidelines for retaining, preserving and disposing of these assets in accordance with the State's records management requirements. Agencies are advised that this is an evolving practice space and that changes in these guidelines are likely to occur. In this connection, agencies are encouraged to provide their feedback to the Division relative to their experiences and perspectives, so that our staff may stay current with developments and successful approaches being applied by our records custodians State-wide.

Bullas, J. (2015). 12 major business benefits of the social media revolution. Retrieved from http://www.jeffbullas.com/2011/02/14/12-major-benefits-of-the-social-media-revolution/

Cavazza, F. (2012, March 12). An overview of the social media ecosystem. Retrieved from http://www.forbes.com/sites/fredcavazza/2012/03/12/an-overview-of-the-social-media-ecosystem/

Comer, D. E. (2015). Computer networks and internets. (6th ed.). Upper Saddle River, NJ: Laudon, K.C. & Laudon, J.P. (2014). Management information systems: Managing the digital firm. (13th ed.). New York, NY: Pearson.

Layton, T.P. (2007). Information security: Implementation, measurement and compliance. (2nd ed.). Boca Raton, FL: Auerbach Publications Taylor& Francis Group.

National Archives and Records Administration. (2013). Best practices for the capture of social media records. Retrieved from http://www.archives.gov/records-mgmt/resources/socialmediacapture.pdf

National Institute of Standards and Technology. (2014, February 12). Framework for improving critical infrastructure cybersecurity. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

New South Wales Government. (2012). Social media policy and guidelines. Retrieved from http://www.finance.nsw.gov.au/ict/sites/default/files/NSW%20Government%20Social%20Media%20Policy%20and%20Guidelines.pdf

New South Wales Government. (2014). Management strategies for social media information. Retrieved from https://www.records.nsw.gov.au/recordkeeping/advice/designing-implementing-and-managing-systems/strategies-for-managing-social-media-information/management-strategies-for-social-media-information

Office of the Auditor General. (2013). Learning from public entities use of social media. Retrieved from http://www.oag.govt.nz/2013/social-media/docs/social-media.pdf

Peltier, T. R. (2014). Information security fundamentals. (2nd ed.). Boca Raton, FL: CRC Press.

Richman, J. (2010, February 3). The seven uses of social media in business -- the 7 “C”s. Retrieved from http://www.doseofdigital.com/2010/02/the-seven-uses-social-media-business/

Saxena S. (2013, August 11). 7 key characteristics of social media. Retrieved from http://www.easymedia.in/7-key-characteristics-of-social-media/

The Sedona Conference. (2012). Primer on social media. https://the Sedonaconference.org/download- pub/1751

Guidelines for Developing Retention and Disposition Policies for Artificial Intelligence/Machine Learning Systems

Background and Action Steps

Published by:

New Jersey Division of Revenue and Enterprise Services
James J. Fruscione, Director
February 2025

TABLE OF CONTENTS

Introduction

These guidelines include suggested action steps for creating retention and disposition policies for public records associated with or created by systems using artificial intelligence/machine learning (AI/ML).[1]

AI/ML offers government agencies opportunities to innovate and greatly improve their services and productive capacities. In this connection, the potential applications for AI/ML touch upon a broad range of institutional activities and can give shape to initiatives that influence our social, economic, political, cultural, health, academic, scientific and environmental sectors. Accordingly, as government agencies work to implement and leverage the technology, the development of pathways to effective governance of AI/ML, including the institution of retention and disposition policies, is in order.

Applicability of Public Records Law

As with all public records management publications, the foundation for this document is the legal imperative expressed in New Jersey's public records law (N.J.S.A. 47:3 et seq.). That is, irrespective of medium, all records that are generated and received during governmental operations are public records and subject to the State's records management and archival requirements. Records associated with or created by governmental systems using AI/ML are therefore subject to the State's public records law.

Audience

These guidelines are primarily for professionals who work in records and information management capacities and who have some familiarity with the State's records management program as described in the New Jersey State Records Manual (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2024c). In addition, generalist managers, administrative support staff, technologists, cybersecurity exerts, procurement officials, auditors, human resources officers, legal advisors and ethics liaisons may find the guidelines useful.

Background

While AI/ML itself is not new, the recent emphasis on expanded experimentation with and use of the technology, including new governmental initiatives and applications, represents an important trend.

The background discussion that follows helps set the general context in which the guidelines may be applied. The assumption here is that use of AI/ML is a relatively new concept for many State and local records managers and public officials, so the discussion goes into greater depth than is typical for records management guidelines. Notwithstanding, this is not intended to be an exhaustive or authoritative treatment of the technological dimensions of AI/ML systems.

Definition and Uses

The Organization of Economic Cooperation and Development (OECD) defines an Artificial Intelligence system as:

> "…a machine-based system that can, for a given set of human defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments (OECD, 2019, p.1)."

Thus defined, use cases for AI/ML technology may encompass a variety purposes. For example, in the public sector, AI/ML may be used to augment or directly execute informational searches and text retrieval. Similarly, it may summarize meetings and text from a collection of works or be used to personalize a citizen's on-line interactions with public agencies based on prior patterns of on-line behavior and/or demographical data. It may be used to predict outcomes or render diagnoses/decisions in topical spaces like computer security, health care, finances, benefits eligibility, environmental controls and public safety/defense. Moreover, it can recognize objects and biological traits, generate media presentations, handle language translations, drive robotic operations and more. (Glasscock, 2019; State of New Jersey, 2023; OECD, 2024)

Predictive forms of AI activity center on ML and revolve around pre-defined rules and data sets. More advanced applications focus on the generative capabilities of AI, or GenAI. GenAI goes beyond the predictive thrust of ML. It uses

[1] ML is a subset of AI technology. For purposes of this presentation, the acronyms AI and AI/ML are used interchangeably.

massive computing power to derive relationships, patterns and inferences from data sources to create new outputs or contents.

Such generative outputs can be new written works, formulas for planning or problem resolution, fully automated decisions, computer code/controls, graphics/pictures, cyber/physical security controls, audio/visual works, etc. Increasingly, AI/ML systems leverage aligned technologies such as natural language processing and customer-centered interfaces like chatbots to facilitate end-user interactions (Lawton, 2024).

Typical Components AI/ML Systems

Industry observers (Fleming, 2024; Lawton, 2024; Run:ai, 2024) note that AI/ML systems operate within infrastructures that feature data, software processing, hardware/network architectures and user interface tools.

Data can come from structured data bases, semi-structured data like electronic documents and spread sheets and unstructured data such as images, video and audio compilations. It can be owned by the end user organization and/or be supplied by third parties. Data can be stored within in-house facilities, Cloud-based platforms or hybrid (Cloud/in-house) complexes.

Software processing tools operate on source data to yield desired outputs. These tools can be based on traditional business rules-processing software. However, increasingly, language models, including so-called large language models (LLMs) like OpenAI's GPT-3 and Google's Palm 2, are rising to prominence. Language models leverage technologies and processes such as neural networks and deep learning and operate with natural language processing to yield answers and predictions to end users (Barney and Lutkevich, 2024). Other types of software tools include data transport, cleansing and access programs that supply usable data to the AI/ML system and end-users. Generally, software tools can be owned by the user organization and/or be obtained via licensure from vendors. Use of language models will likely entail licensure of a vendor’s product.

Hardware/network architectures provide the resources needed to run AI/ML systems, transport data to/from system nodes and end-users, and train/operate language models. AI/ML systems are likely to require high capacities to handle massive volumes of data and complex, resource-intensive computational work. For the latter consideration, beyond traditional central processing units, AI/ML may require components that are geared to massive and specialized processing operations – for example, GPUs (Graphics Processing Units), TPUs (Tensor Processing Units), FPGAs (Field-Programmable Gate Arrays), etc. (Flipsson, 2024). These systems are also likely to require massive data storage arrays and robust communications networks to move large volumes of data within and across information system platforms. Given the need for specialized hardware/software, it is likely that most organizations will need to procure and/or license significant portions of their AI/ML architectures from third parties.

Finally, user interface tools enable developers, testers and end users to interact with AI/ML systems. Interface tools can be in the form of customized software such as application programming interfaces and increasingly, natural language interfaces connected with chatbots. These tools can be developed in-house by the organization and/or be procured or licensed from a third party.

Potential Benefits of AI/ML

The potential benefits of AI/ML flow logically from the use cases described previously. For example, in its final 2024 report to the Governor, New Jersey’s Artificial Intelligence Task Force (2024) highlights that AI (with specific reference to GenAI) could potentially enhance a range of state government functions, from internal administrative operations to external service delivery.

Likewise, the OECD (2024) investigates the benefits that societies (including their governmental institutions) can derive using AI, with a focus on ten such benefits. Paraphrased, these include: enhanced scientific progress; improved economic growth, productivity and living standards; decreased levels of inequality and poverty; better approaches to complex issues like climate change; more effective forecasting, predictions and analysis; broader and more flexible forms of information production, distribution, access and sharing; advanced healthcare and personalized educational services; improved/safer job experiences; increased citizen engagement and empowerment; and increased institutional

transparency/accountability.

Concerns about the Use AI/ML

The potential for improving human endeavors through use of AI/ML is truly impressive. However, OECD (2024) also cautions that use of the technology engenders many significant risks and potential harms.

Once again, paraphrased, the organization's top ten prioritized risks and potential harms are: providing foundations for sophisticated cyber-attacks (including unauthorized access, use and/or defacement of sensitive information); spreading misinformation/disinformation, with negative outfalls like increased fraud and election interference; implementing rushed and poorly designed AI systems that are not safe or trustworthy; causing unexpected harms through misalignments between AI systems and stakeholders' desires, needs and values; concentrating power in the hands of a few technology companies and/or countries that underwrite the development of the technology; using flawed outputs that cause critical system failures; infringing on privacy (through stepped-up surveillance) or on copyright protections; operating with inadequate governance programs that fail to keep up with rapid technological advances; using technologies that are opaque (not clearly understood), thereby engendering accountability gaps; and through system bias, worsening inequality and poverty and/or threatening employment.

The New Jersey AI Task Force (2024) identifies risks and potential harms that are like OECD's. Further, to counterbalance these risks/potential harms, in a joint circular letter, the State of New Jersey (Office of Information Technology et al., 2023) exhorts agencies using AI/ML to adhere to principles like empowerment, inclusion, transparency, innovation, and risk management, as well as to take measures to protect sensitive information.

State and Federal Actions in the AI/ML Practice Space

State and federal authorities within the executive and legislative branches are taking actions to address the potential risks and harms of AI/ML. The Future of Privacy Forum (2024) points out that state lawmakers are working to enact legislation that regulates AI used in decisions that have significant impacts on peoples' lives and livelihoods, with an eye toward mitigating discrimination and violations of citizens' rights. Hooshidary, Canada and Clark (2024) also highlight various initiatives at the federal and state levels – directives, executive orders, legislation, etc., aimed at creating rules to govern the application of the technology, with emphases on the ethical use of AI/ML and protecting the legal rights of individual citizens.

In all these efforts, either explicitly or implicitly, government authorities point to the need for governance – policies, procedures, rules and staffed administrative functions that determine how and when the technology is to be employed.

AI/ML governance aims at the creation of systems that are fit-for-purpose, understandable (explainable), accountable, safe/secure and as free from bias as possible (Mooradian, 2019; U.S. Department of Homeland Security, 2024; The White House, 2024).[2]

Per force, such governance (and ultimately, the sustained success of AI/ML technology itself) relies on records that document how AI/ML systems are designed, developed, tested, operated, used and managed throughout their life cycles. Therefore, basic records management practices, including retention and disposition policies, are core parts of AI/ML governance. In fact, at the national level, professionals representing state government technology agencies note that strong governance programs, including controls over the public records that GenAI creates, are needed to address the risks posed by the technology (Glasscock, 2024).

Governance Models and Their Relationships with Records Management Practices

Arguably, as of the writing of these guidelines, the two most complete and mature governance models for AI/ML technology in the U.S. can be found in the Government Accounting Office's (GAO) AI accountability framework (2021) and the National Institute of Standards and Technology's (NIST) risk management framework for AI (2023).

[2] Federal government perspectives on AI/ML may be shifting. As of the writing of these guidelines, it is too early to predict how this development will evolve to influence the uses of AI/ML technology.

Both frameworks feature controls that span the life cycles of AI/ML systems and in doing so, highlight documentary resources (records) required to manage the systems' risks and ensure the requisite system qualities – safe, secure/resilient, privacy-enhanced, explainable, fair, accountable/transparent, valid and reliable (National Institute of Standards and Technology, 2023). As will be discussed, these documentary resources can be used to develop a tentative AI/ML record series taxonomy that can be translated into a records retention/disposition policy regime.

Summary of NIST Framework

The NIST framework (2023) includes four functions: 1) govern (a cross-cutting function that defines the values, policies, procedures, rules, roles and responsibilities associated with AI/ML systems); 2) map (determining and documenting the legal and operational context of AI/ML systems and associated risks); 3) measure (collecting and assessing data points – qualitative and quantitative, on system operations and impacts); and 4) manage (assigning resources to run/administer AI/ML systems and directing steps required to address issues and opportunities that result from the operation of the systems). Within the NIST framework, there are requirements for involving diverse stakeholders, managing vendors and determining when to decommission systems.

Summary of GAO Framework

GAO's framework (2021) also includes four functions: 1) govern; 2) data; 3) performance; and 4) monitoring. To a significant degree, these functions overlap NIST's. However, as one might expect, GAO has a stronger orientation toward documentary artifacts that facilitate auditing. So, for example, the governing function requires documentation of technical specifications to ensure AI/ML systems are suited for their intended purposes. The data function calls for documentation of sources and attributes of data used by the systems – for instance, reliability measures, documentation of use of synthetic, imputed and/or augmented data, information about data dependencies, measures of bias, security classifications, etc.

Organizational Structure

Both frameworks pre-suppose organizational structures (governing bodies) within which AI/ML governance is developed, applied and administered. In New Jersey's governmental context, these structures will vary based on the level, size and complexity of specific institutional settings. Broadly, however, one could envision governing bodies consisting of diverse groups of people representing wide ranges of disciplines, including system owners/subject matter experts, legal authorities, procurement officials, records management professionals, information technologists, cyber security authorities, human resources specialists, ethics officers and external/internal stakeholders.

Despite the organizational diversity that exists among governmental agencies in New Jersey, there is a common legal structure through which AI/ML retention and disposition programs can be implemented – approval of retention schedules and disposition actions through the State's Records Management Services Unit and State Records Committee (New Jersey Division of Revenue and Enterprise Management, Records Management Services Unit, 2024c, pp. 10-13). Thus, as will be shown, no matter how agencies constitute their AI/ML governance functions, those functions can be linked with this common legal structure, seamlessly and to good effect, for records management purposes.

Guidelines

With a basic understanding of AI/ML technology, its potential benefits/risks and the governance structures needed to ensure sound and accountable AL/ML system operations, New Jersey governmental officials can develop policies for AI/ML records retention and disposition. Given the rapidly expanding and diversified uses of the technology, such policies must be considered provisional. Nonetheless, it would be best for agencies to plan for retention and disposition controls before implementing AI/ML technology. Organizations that fail to take proactive postures may ultimately find themselves unable to account for their uses of AI/ML in a responsive, legally defensible manner.

In connection with the points above, even if their approaches to records retention/disposition are provisional, proactive agencies will gain better understandings of AI/ML records by taking the actions outlined below. Improved understandings of these records will foster greater intellectual control over the components of AI/ML systems. Through this, agencies will improve their capacity to develop more understandable, fair, secure, reliable, valid and effective systems over the course of time.

Key Contacts

The contact for the records management topics covered in the guidelines is the New Jersey Division of Revenue and

Enterprise Services' Records Management Services Unit (DORES/RMS): 609-777-1020 or 609-292-8711. Guidance on records with permanent and historical value can be obtained from the State Archives: 609-633-8304 or 609-292-6260.

Action Steps

Following are the action steps that agencies can take to create AI/ML records retention and disposition policies. The action steps mirror those reflected in earlier guidelines issued by DORES/RMS (New Jersey Division of Revenue and Enterprise Management, Records Management Services Unit, 2024a, 2024b).

Because many governmental agencies are just beginning to explore and use the technology, the guidelines include the formation of an AI/ML governing board, which can interact with DORES/RMS and the State Records Committee when formulating and administering the agency's AI/ML retention and disposition policies.

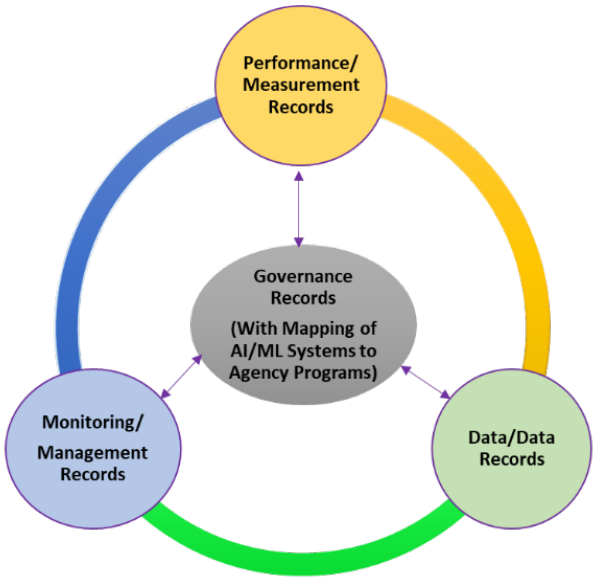
1. **Form an AI/ML Governing Board.** Given the potential benefits and risks of AI/ML technology, it would be wise to form an AI/ML governing board with a mandate to assess, charter and monitor the agency's use of AI/ML systems. This would be especially important if the agency intends to use the technology in settings involving significant societal concerns such as benefits eligibility, health care coverage, education, environmental protection or public safety.

As noted previously, one could envision representatives from a wide range of disciplines and endeavors participating on an AI/ML board – for example, system owners/subject matter experts, legal authorities, records management professionals, information technologists, cyber security experts, procurement officials, human resources authorities, ethics officers, and external/internal stakeholders. Records management professionals would likely be the best candidates to coordinate and lead projects aimed at establishing Ai/ML retention and disposition policies.

Finally, the best practice would be for the governing body to review and approve action steps 2-6 below.

2. **Inventory/Create Categories for Records**. For new systems, agencies may create records categories (series), or for existing systems, conduct inventories of existing series. In both cases, using a scheme such as the example taxonomy depicted below may prove helpful. Note that the example record series in the taxonomy align with functions like those found in the GAO and NIST frameworks discussed previously. Ultimately, building formal records series taxonomies is central to developing intellectual control over the contents and functions of AI/ML system.

Figure 1. Tentative AI/ML Records Series Taxonomy



a. Governance Records. These records pertain to the core organizational, financial/fiscal and technical aspects of the system. They inform, and in turn are informed by, the system as it operates throughout its life cycle. Examples of records in this category may include:
   - Documented goals and objectives of the system
   - Technical specifications and resources – records covering all the technical components of the system, including documentation of system architecture/system design, development, AI model training, testing, implementation, etc.
   - Project management documentation such as plans and status reporting associated with system development and major system upgrades
   - Budget and expenditure records
   - Laws, policies, procedures, rules and regulations that shape and limit system operations, including official records retention and disposition policies
   - Assigned roles and responsibilities (mappings to responsible agency programs and staff) for system design, development, implementation, operation, administration, audit, etc. (See U.S. Department of Homeland Security (2024) for a discussion of AI/ML-related roles.)
   - Communications plans involving stakeholders
   - Risk assessments and recommendations
   - Staff training plans
   - Cybersecurity controls
     *Note: In New Jersey, the Office of Homeland Security and Preparedness' Statewide Information Security Manual (2024) sets forth cybersecurity policies, standards, processes and guidance for the State's information programs.
   - Decisions to migrate a system to another platform or to decommission a system
   - Contractual terms and conditions, including service level agreements, which govern relationships with vendors who provide system platforms, software, services, etc.

b. Data/Data-Records. These records include documentation of the data identified by the governance function, which are used to create, train, test, operate and manage the AI/ML system, **as well as the actual data compilations that serve as the content for the systems**. Data records also include meta-data associated with AI/ML data compilations – for example, names and functional descriptions (purposes for which the data is used), authorship, dates created/updated, dependencies, transformations/augmentations such as changes used to combine or anonymize data elements, create proxy values for data, etc. Examples of data/data records include:
   - System data -- databases, data sets and other compilations, which can be structured (for example, table-oriented databases), semi-structured (for instance, delineated text files, documents, spreadsheets) and unstructured (such as pictures, graphics, chats, audio and video files)
   - Meta-data as described above
   - Web sites and social media link (AI/ML software can crawl and *learn* sites by navigating a set of links)
   - Log files – files reflecting system events including end user interactions, security alerts, performance issues, etc.
   - Prompts (inputs that trigger queries and requests processed by AI/ML systems) and responses/outputs generated by the systems

     *Note: Agencies will need to consider whether it is feasible to store prompts and outputs produced during normal system operations for fixed time periods. The logistics and costs for doing so may prove prohibitive for large-scale systems, particularly those used by government agencies to serve the public. Alternately, for low impact systems, prompts may generate non-sensitive, ephemeral outputs and so may not warrant coverage in the system retention schedule. If the agency decides it cannot accommodate storage of these entities or believes that they are ephemeral, it would still be wise to document how prompts and outputs are produced/used and the reasons for not storing them.

- Classifications that indicate whether the records/data used by the system are public, confidential, private, etc. (Data classifications will inform cyber security controls enacted via governance directives.)

  *Note: AI/ML systems may employ combinations of internal and third-party data resources and combinations of in-house and Cloud-based storage. For Cloud-based storage of agency-owned data, use of the State's suggested controls for Cloud storage would be a best practice (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2019). The guidelines make it clear that decisions about retention and disposition of agency-owned data fall under the exclusive purview of the agency. Handling data provided by third parties is a more complicated consideration, which will likely connect with negotiated contractual provisions established by the governance function.

c. Performance/Measurement Records. Agencies will generate these records as they test, operate and use an AI/ML system in accordance with the goals and objectives set forth by the governance function. Examples of performance/measurement records include:
   - Reports and metrics that plot actual system performance against desired operational capacities and outcomes defined by the governance function (for example, end-user satisfaction ratings, assessments of citizen engagement with the system, transactions handled within a specific timeframe, internal and/or third-party reviews of accuracy, completeness, observed bias(es) and/or usability, evaluations of efficiency measures/cost savings associated with task automation, etc.
   - Readings of a system's transparency and understandability via ad-hoc and/or structured stakeholder feedback, subject matter expert assessments, industry and/or cross agency benchmarks, etc.
   - Quality control and test records that reflect processes used to ensure the accuracy, reliability, validity and integrity of data used by the system
   - Results of cyber security and operational audits
   - Reports of broader consequences for humans (for example, job losses or shifts in responsibilities due to automation, complaints regarding privacy violations stemming from stepped up surveillance, increased denials of benefits due to automated decision-making, etc.)

d. Monitoring/Management Records. In this category, records document the decisions and actions the agency takes to implement, control, adjust, secure, and ultimately, decommission a system in accordance with directives emanating from the governance function and information drawn from performance/measurement records. Examples include records reflecting:
   - Corrective action plans designed to adjust data sources, language models, business rules and related system resources to address issues and/or improvement opportunities surfaced in audits or other evaluations
   - Responses to specific incidents involving breaches or harms caused by the operation of an AI/ML system
   - Configuration control records showing significant adjustments to the system architecture and/or functions
   - Changes to contractual terms and conditions due to evolving circumstances that affect system design or performance
   - Changes (deletion, addition, substitution) of data sources
   - Changes to language models, user interfaces and/or data transmission/transformation software
   - Changes to storage platform(s) (for instance, moving from in-house to Cloud, switching Cloud vendors or adopting a hybrid arrangement)
   - Significant reengineering of prompts (inputs used to interact with language models)
   - Correcting for identified bias(es)
   - Adjustments made for new or modified stakeholders

- Records disposition actions based on approved retention schedules and disposition requests per these guidelines; these actions will be documented in the State's authorized disposition action database, ARTEMIS (See Step 6.).

3. Conduct a Value Assessment(s). Based on the taxonomy, assign values to the AI/ML records. While traditional values -- for example, administrative, fiscal, audit, legal and historical, could apply to AI/ML records, it may be best to emphasize the level of human impact in this space – that is, to emphasize a risk management perspective. This is appropriate because, to a higher degree than previous technologies, AI/ML augments or drives the automatic generation of information that can have direct effects on the well-being of citizens, businesses and society. Indeed, it is for this reason that states and the federal government seek to place restrictions on the technology's use (Hooshidary, Canada and Clark, 2024; The White House, 2024).

As public agencies in New Jersey become more experienced in the use of AI/ML, broader methods of value assessment, including methods that blend traditional and sensitivity values, may surface. Ultimately, some systems may produce outputs of enduring, historical value such as meeting minutes, executive summaries of technical reports used for decision-making and other reports scheduled as permanent. For this reason, agencies should consult with the State Archives both prior to implementing AI/ML systems and before any final decisions to decommission them.

Following are value dimensions that agencies can consider. The value dimensions are tied to a simple sensitivity range that parallels information system categorizations found in cybersecurity/risk management regimes (New Jersey Office of Homeland Security and Preparedness, 2024, pp. 51-52):

a. Low -- System generates/stores records that have limited or no impact on individual citizens, businesses or broader society; examples may include records associated with a system that supports agency employees in answering routine questions about or locating information on agency forms, procedures and policies, summarizing routine meeting dialogues, drafting routine correspondence that employees must review/approve before sending, etc.

b. Moderate -- System generates/stores records that affect individuals and businesses such that inaccurate or misleading outputs may inconvenience end-users or frustration them, but that will entail no- or low-risk of any lasting harm and/or broader societal impacts; examples may include outward facing (public) chatbots regarding routine agency forms, services, procedures and policies, informational guides on general licensing requirements, summaries of public meeting minutes, etc.

c. High -- System generates/stores records that affect individuals, businesses and/or society in substantial, consequential ways; examples may include records associated with a system that generates decisions on citizens' applications for social or medical benefits coverage, produces recommendation for job eligibility, serves as a self-regulating mechanism for critical infrastructure, etc.

*Note: As with many types of governmental records, AI/ML system records may bridge or overlap the value dimensions above. That is, different system records may have varying sensitivity levels -- from *low to moderate*, *moderate to high*, *low to high*. A common approach to assessment in cases involving overlapping values is to assign the highest level to the system as a whole – for example, if the overlapping range is *low to high*, assign the *high* value to all system records. If this approach is not feasible or desirable, then the agency can opt for a more granular approach and assign values to the involved records on a series-by-series basis. The discussion in Step 4 below covers both of these approaches.

4. Assign Retention and Disposition Policies. Based on the value assessments conducted in Action Step 3, assign retention and disposition polices to the AI/ML records. For the steps involved in creating official retention and disposition polices (schedules) in conjunction with DORES/RMS and the State Records Committee, consult the State Records Manual (New Jersey Division of Revenue and Enterprise Services, 2024c, pp. 10-13).

Before proceeding, be aware that there may be use cases that do not require the creation of new AI/ML record series. Specifically, if the agency uses the technology to produce only low sensitivity outputs and all those outputs must be reviewed and approved by designated, responsible employees, then the agency may be able to focus on scheduling those outputs alone and not the entire system. An example use case would be a system that produces routine correspondence, operational meeting summaries or statistics used in an agency's monthly report, all of which are reviewed by designated, responsible employees. Here, general schedule items such as external correspondence, electronic resource files and monthly reports may be used for AI/ML records retention scheduling. Review available general retention schedules for these routine types of records online at the DORES/RMS web site and also review the New Jersey State Records Manual (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2024c). RMS will assist agencies in using existing records series for AI/ML records.

a. Following is an example AI/ML record series taxonomy, along with example retention and disposition policies for each series. Agency retention/disposition scheduling efforts may result in record series like those shown below **or** be different based on the agency's circumstances and the characteristics of its system(s). Work with RMS to settle upon a records retention/disposition scheme.

   The tables show two possible approaches to AI/ML records retention and disposition scheduling: Table 1, system-wide scheduling with a single policy assigned to all records series (easiest to promulgate and administer, but may foster over-retention and/or pre-mature disposition actions); and Table 2, granular scheduling series-by-series (may be cumbersome to administer and maintain, but provides the greatest degree of control).

   *Note: The application of any AI/ML retention/disposition regime pre-supposes that the agency has taken steps to ensure either:
   - The underlying system infrastructure upon which records generation, receipt and storage depends remains active for the length of the longest records retention period involved; or
   - There is an actionable plan to migrate records to a successor system that addresses retention/disposition requirements.

   Because the use of AI/ML likely entails substantial reliance on third-party system infrastructures and potentially, third-party data resources, agencies will need to **align contractual terms to assure system availability for the duration of all retention periods**.

Table 1. Example of System-wide Retention Scheduling

Example Record Series	Retention/Disposition Policy by Sensitivity Level		
	Low	**Moderate**	**Low**
• Governance Records • Data/Data Records • Performance/Management Records • Monitoring/Management Records	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy

Table 2. Series-by-Series Scheduling

Example Record Series	**Retention/Disposition Policy by Sensitivity Level**		
Governance Records	**Low**	**Moderate**	**High**
Organizational (charter) documentation including: feasibility studies; directives to implement system; stake-holder rosters/communications; goals/objectives of system; citations to governing laws and regulations; system policies/procedures; assigned roles/responsibilities; communications plans; status reports; decisions to migrate to another platform or to decommission; and project management files	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Technical specifications including: design/development documentation; bias assessments/reports; test plans/results; and system configuration information	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Budget and expenditure records (Assumes these are copies, with original records kept by budget/fiscal officers)	3 Years/Destroy	3 Years/Destroy	3 Years/Destroy
Risk management records including assessments and recommendations	As updated/Destroy	3 years/Destroy	7 years/Destroy
Staff training plans	As updated/Destroy	As updated/Destroy	As updated/Destroy
Contractual terms and conditions	7 years following termination of contract/Destroy	7 years following termination of contract/Destroy	7 years following termination of contract/Destroy
Example Record Series (Series-by-Series Continued)	**Retention/Disposition Policy by Sensitivity Level**		
Data/Data Records	**Low**	**Moderate**	**High**
Source data and associated meta-data (databases, data sets and other compilations), web sites and social media records used by the system	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Records/data classifications	Retain until business use	1 year following decommissioning	7 years following decommissioning

	ceases/Destroy	or migration to replacement platform/Destroy	or migration to replacement platform/Destroy
Prompts and responses/outputs generated by the systems (As noted previously, it may not be feasible or necessary to retain these records, but to the extent that they are retained, retention/disposition policies are in order.)	Retain until business use ceases/Destroy	1 year/Destroy	7 years/Destroy
Log files – files reflecting system events including end user accesses, tracked changes to databases, security alerts, performance issues, etc.	As updated/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy

Example Record Series (Series-by-Series Continued)	**Retention/Disposition Policy by Sensitivity Level**		
Performance/Measurement Records	**Low**	**Moderate**	**High**
Reports and metrics that plot actual system performance against desired outcomes defined by the governance function; readings of a system's transparency and understandability; and quality control and test records	As updated/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy
Cybersecurity and operational audit reports/evaluations	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Reports of consequences for humans (for example, job losses or shifts in responsibilities due to automation, complaints regarding privacy violations stemming from stepped up surveillance, increased denials of benefits due to automated decision-making, etc.)	N/A	N/A	7 years following decommissioning or migration to replacement platform/Destroy

Example Record Series (continued)	Retention/Disposition Policy by Sensitivity Level		
Monitoring/Management Records	**Low**	**Moderate**	**High**
Corrective action plans (to address audit findings) and status reports	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Responses to specific incidents involving breaches or harms caused by the operation of an AI/ML system or process	7 years following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Change files documenting adjusts and corrections to the system, including: contractual terms and conditions; deletion, addition or substitution of data sources; language models, user interfaces and/or data transmission/transformation software; storage platform(s); reengineering of prompts (inputs used to interact with language models); and identified bias(es)	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Configuration control records showing significant adjustments to the system architecture and/or functions	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Cyber security controls including plans and configurations settings	As updated/Destroy	3 years following update/Destroy	7 years following update/Destroy
Records disposition actions based on approved retention schedules and disposition requests per these guidelines Note: The State's automated records disposition system, ARTEMIS, houses these records. (See Action Step 6.)	Permanent	Permanent	Permanent

5. Choose Modes of Records/Data Storage. As can be seen from the record series taxonomy, AI/ML systems involve both document-based records like feasibility studies, reports and corrective action plans, and data-oriented compilations that serve as the foundational resources for language models and system software. Also, as noted, agencies will likely use third party contractors, including Cloud service providers, for AI/ML, either exclusively or in tandem with in-house storage platforms. With these factors in mind, consider the following for agency AI/ML storage environments:

a. Adopt a digital-only records policy for AI/ML systems so that both documents and data records can be managed in computer-based form.

b. To the extent possible, use a single platform for all AI/ML records, thereby avoiding fragmented, application-by-application approaches to storage. Realistically though, for the foreseeable future, agencies may be faced with the need to manage data across multiple storage platforms – for example, an office software suite including electronic mail (in-house or Cloud-based) for documentary forms of records and a combination of in-house and Cloud-based storage for data.

c. Ensure that the storage platform(s) incorporates features that enable the agency to implement basic records management functions like policy-based retention and disposition, as well as general principles, practices and standards that support these functions. Doing this will not only bolster the agency's posture relative to records management, but also relative to risk management, cybersecurity and overall accountability and transparency. Accordingly, agencies may wish to review the following to develop records management requirements for their AI/ML systems specifications and contracts:

- Through its Federal Electronic Records Modernization Initiative, the National Archives and Records Administration (2024) provides a model that covers the basic functions that federal agencies must implement to support their records management programs. These requirements, which broadly apply to New Jersey's government sector as well, cover the life cycle of records: capture (including creating/declaring a record); maintenance and use; disposal; transfer; metadata; and reporting. While not all of the requirements here relate to AI/ML, the overall model does touch upon key functions that undergird records retention scheduling and disposition in all settings, as well overall records system integrity, accountability and transparency.

- Looking to the professional non-profit sector, the Association of Records Managers and Administrators International's Generally Accepted Recordkeeping Principles © (2017) highlights the foundations for information governance, including accountability, transparency, integrity, protection, compliance, availability, retention and disposition. Agencies building AI/ML systems would do well to consult and incorporate these principles in their system specifications. Likewise, The Association for Intelligent Information Management (AIIM) (2024) provides useful guidance on structuring AI/ML systems. The organization stresses the institution of policies and protocols in the areas of access control, data encryption, searching, private data identification, automated data classification and user/intent /context analysis.

- The IT industry offers tools and platforms the agency can employ to manage records used by AI/ML systems, and that facilitate the implementation of retention and disposition policies. The elements included in these tools/platforms may involve: encryption of data in transit and at rest; the ability to identify and inventory AI applications used by the agency; electronic discovery (for legal proceedings); security regime compliance reports (for instance, HIPAA, Criminal Justice Information System (CJIS), Safeguards, etc.); role-based security for data access/manipulation; data loss prevention (via detection, labelling and control of sensitive data); assignment of retention periods to specifically labelled records; centralized review and approval of disposition actions; secure deletion (destruction) of records; and audit trailing of deletion actions.

By way of illustration and not endorsement, Microsoft (2024) is an example of a firm that offers solutions covering elements such as these, as are firms like Gimmal and Preservica and others. In the same illustrative way, firms such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, Oracle Cloud, Snowflake and Databricks are examples of third-party Cloud platforms/services that feature security and compliance features, including data retention management.

- At a minimum, if the agency is dealing with a third party for data storage, ensure the contractual agreement includes controls such as those suggested in the State's records management guidelines for Cloud storage (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2029).

d. When it comes to tracking retention and disposition of AI/ML records, it is important to keep an important distinction in mind. Documentary records like reports and electronic mail can be managed at the item or entity level. That is, it is feasible to manage individual instances of documentary records as discrete entities from the beginning to the end of their respective retention periods. It may also be possible to do this with semi-structured and unstructured records. From a practical perspective, however, it will likely be infeasible to accomplish this with respect to individual entries (fields) in databases. In most cases, retention periods will apply to a database in its entirety. Thus, retention periods will relate to the data

base as a whole or possibly to dated versions (snap shots or copies) of the database taken at pre-defined time intervals.

6. Implement and Monitor/Evaluate the Program. After completing the five preceding steps, work with DORES/RMS to implement and monitor/evaluate the retention and disposition program. In this connection, agencies may use one or two formats for disposition actions following the expiration of AI/ML records retention periods: *single-action* and *phased* disposition. Single-action disposition requests relate to AI/ML records that can be managed at the item or entity level such as reports and electronic mail. For single-action requests, the agency periodically identifies specific records that have met or exceeded their approved retention periods and submits individual requests for each. In contrast, phased disposition is most useful for frequently updated databases and other bulk data compilations. For these requests, the agency obtains authority to dispose of AI/ML records on an on-going basis for renewable time periods (6 months or year) without having to submit requests for individual disposition actions.

Referring to the example retention schedules under Action 4, if the agency adopts for a system-wide approach (single retention/disposition policy assigned to all records series in the system), only the single-action disposition format will be feasible. Agencies that opt for the record series-by-record series format may use both disposition formats. For example, again referring to the example retention schedules under Action 4, use phased disposition for source databases, metadata, log files and prompts/outputs, and use the single action format for the balance of AI/ML records.

*Note: Agencies will obtain authorizations for and maintain records of their disposition actions through use of the online system known as ARTEMIS. Use of ARTEMIS requires the agency to register staff authorized to request and approve disposition actions. Once registered, the agency will be able to submit disposition requests to RMS via ARTEMIS, including the entry of approved schedule/record series numbers, and then receive online authorizations to proceed with disposition actions. ARTEMIS includes automated workflow features that guide the agency through the steps in the authorization process. Using ARTEMIS provides for legally defensible disposition actions.

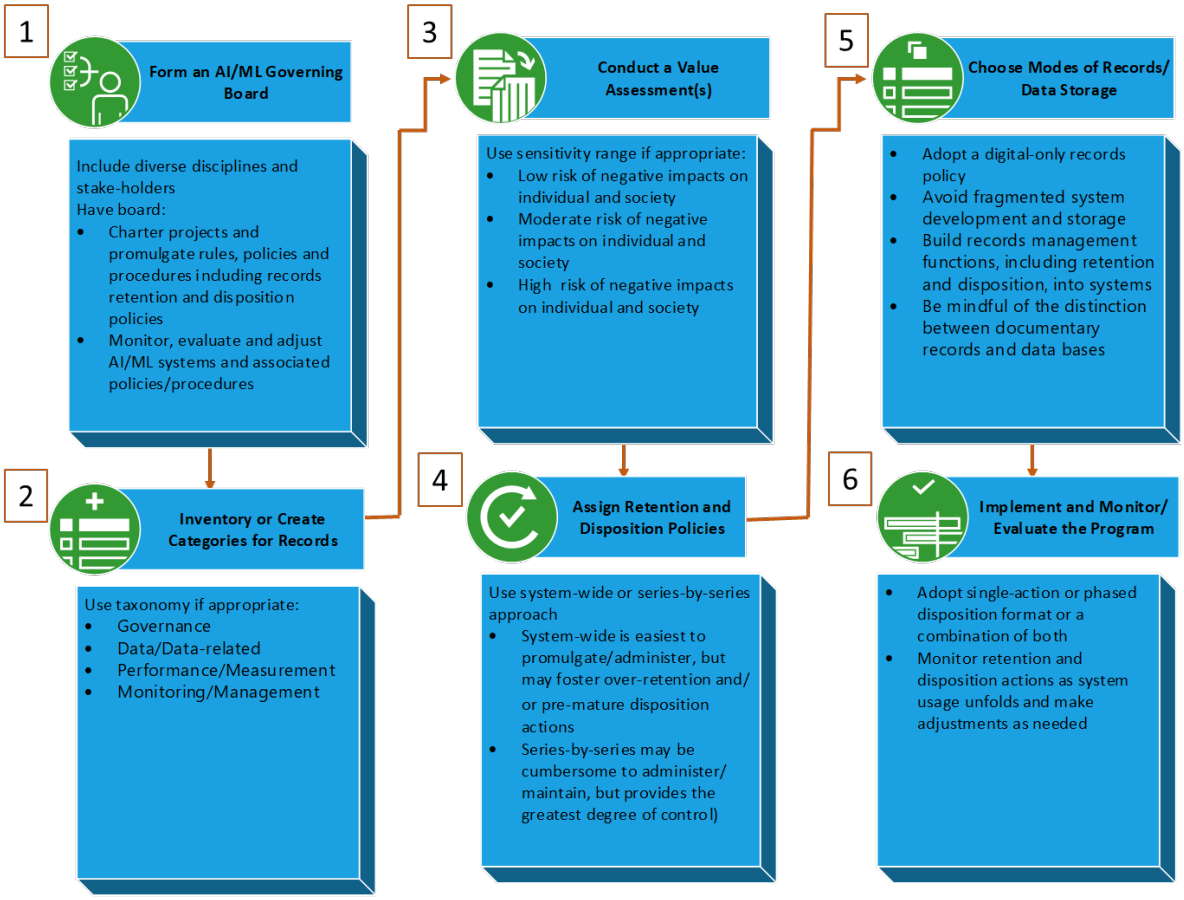
Monitor and evaluate retention and disposition actions as system usage unfolds and make adjustments as required. While the need for monitoring, evaluation and adjustment is implicit in any business system or program, agencies should give these functions particular emphasis given the rapidly evolving and potentially expansive impacts of AI/ML technology.

Conclusion

This presentation provided background on AI/ML technology, its potential use cases and the possible benefits and drawbacks associated with those uses. As summarized in Figure 2 below, it then provided guidelines on how to address AI/ML records retention and disposition within a governance framework based on risk/sensitivity levels. The levels align with the potentially transforming and yet still-uncertain effects of the technology.

The hope is that these guidelines will help New Jersey's governmental officials gain intellectual control over the contents and outcomes of their AI/ML systems and through this, the ability to institute accountable and legally-defensible records retention/disposition policies. From a broader perspective, by implementing governance measures and achieving intellectual control over AI/ML, our public agencies will be better-positioned to realize the transformative potential of the technology.

Figure 2. Summary of Action Steps for Establishing AI/ML retention and Disposition Policies


1
Form an AI/ML Governing Board
Include diverse disciplines and stake-holders
Have board:
• Charter projects and promulgate rules, policies and procedures including records retention and disposition policies
• Monitor, evaluate and adjust AI/ML systems and associated policies/procedures
2
Inventory or Create Categories for Records
Use taxonomy if appropriate:
• Governance
• Data/Data-related
• Performance/Measurement
• Monitoring/Management
3
Conduct a Value Assessment(s)
Use sensitivity range if appropriate:
• Low risk of negative impacts on individual and society
• Moderate risk of negative impacts on individual and society
• High risk of negative impacts on individual and society
4
Assign Retention and Disposition Policies
Use system-wide or series-by-series approach
• System-wide is easiest to promulgate/administer, but may foster over-retention and/ or pre-mature disposition actions
• Series-by-series may be cumbersome to administer/ maintain, but provides the greatest degree of control)
5
Choose Modes of Records/ Data Storage
• Adopt a digital-only records policy
• Avoid fragmented system development and storage
• Build records management functions, including retention and disposition, into systems
• Be mindful of the distinction between documentary records and data bases
6
Implement and Monitor/ Evaluate the Program
• Adopt single-action or phased disposition format or a combination of both
• Monitor retention and disposition actions as system usage unfolds and make adjustments as needed

References

Association for Intelligent Information Management. (2024). “Safeguarding Your Organization’s Data in the Age of AI”, AIIM, Silver Spring Md.

Association of Records Manager and Administrators. (2017). Generally Accepted Recordkeeping Principles. © ARMA International, www.arma.org/principles.

Barney, N. and Lutkevich, B. (2024, August). “What is Language Modeling?” TechTarget, https://www.techtarget.com/searchenterpriseai/definition/language-modeling

Fleming, G. (2024, August). “The Top 10 Key Components to Artificial Intelligence”, https://www.linkedin.com/pulse/top-10-key-components-artificial-intelligence-gerry-fleming-ri0rc

Filipsson, F. (2024, July). “Artificial Intelligence Hardware – What is Required to run AI?”. Redress Compliance, https://redresscompliance.com/artificial-intelligence-hardware-what-is-required-to-run-ai/

Future of Privacy Forum. (2024). *U.S. State AI Legislation, How U.S. Policymakers Are Approaching Artificial Intelligence Regulation*, https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf

Glasscock, A. (2024). “Generating Opportunity: The Risks and Rewards of Generative AI in State Government”. National Association of State Chief Information Officers, https://www.nascio.org/resource-center/resources/generating-opportunity-the-risks-and-rewards-of-generative-ai-in-state-government/

Government Accounting Office. (2021). *Artificial Intelligence, an Accountability Framework for Federal Agencies and Other Entities,* https://www.gao.gov/assets/gao-21-519sp.pdf

Hooshidary, S., Canada, C., Clark, W. (2024). “Artificial Intelligence in Government: The Federal and State Landscape”. National Conference of State Legislatures, https://www.ncsl.org/technology-and-communication/artificial-intelligence-in-government-the-federal-and-state-landscape#:~:text=This%20legislation%20is%20designed%20to,AI%20practices%20across%20government%20agencies

Lawton, G. (2024). “What is GenAI? Everything You Need to Know”. TechTarget, https://www.techtarget.com/searchenterpriseai/definition/generative-AI

Microsoft (2024). Microsoft Purview data security and compliance protections for generative AI apps. Microsoft, https://learn.microsoft.com/en-us/purview/ai-microsoft-purview

Mooradian, N. (2019). “AI, Records, and Accountability”. ARMA International, https://magazine.arma.org/2019/11/ai-records-and-accountability/

National Archives and Records Service. (2024, September). “Federal Electronic Records Modernization Initiative (FERMI)”. NARA, https://www.archives.gov/records-mgmt/policy/fermi

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0),* https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

New Jersey AI Task Force. (2024). *Final Report to the Governor*, https://www.nj.gov/governor/docs/Final-2024-NJ-AI-Task-force-Report-to-Governor.pdf

New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit. (2019). Records Management Guidelines for Cloud-based Records Storage, https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforRecordsManagementintheCloud.pdf

New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit. (2024a). *Guidelines on Retention Scheduling Public Records Stored on Electronic Messaging Platforms,* https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforSchedulingElectronicMessagingRecordsforRetentionandDisposition.pdf

New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit. (2024b). *Guidelines on Retention Scheduling Public Records Stored on Social Media Platforms*. https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforSchedulingSocialMediaRecordsforRetentionandDisposition.pdf

New Jersey Division of Revenue and Enterprise Services. (2024c). New Jersey Records Manual, https://www.nj.gov/treasury/revenue/rms/manual/RMSManual.pdf

New Jersey Office of Homeland Security and Preparedness. (2024). Statewide Information Security Manual, https://www.cyber.nj.gov/home/showpublisheddocument/36/638568130115330000

Office of Information Technology, Office of Homeland Security and Preparedness and NJ Cybersecurity & Communications Integration Cell. (2023). *AI Acceptable Use Joint Circular*, https://www.nj.gov/circulars/23-oit-007.pdf

Organization of Economic Cooperation and Development. (2019). *Artificial Intelligence & Responsible Business Conduct*, https://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf

Organization of Economic Cooperation and Development. (2024). *Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives,* OECD Artificial Intelligence Papers, No. 27, OECD Publishing, Paris, https://doi.org/10.1787/3f4e3dfb-en

Run:ai. (2024). *AI Infrastructure, 5 Key Components to Building Your AI Stack*, https://www.run.ai/guides/machine-learning-engineering/ai-infrastructure

U.S. Department of Homeland Security. (2024). *Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure*,https://www.dhs.gov/sites/default/files/2024-11/24_1114_dhs_ai-roles-and-responsibilities-framework-508.pdf

The White House. (2024). *Framework to Advance AI Governance and Risk Management in National Security*, https://home.treasury.gov/system/files/216/Framework-to-Advance-AI-Governance-and-Risk-Management-in-National-Security.pdf

Appendix

This space is provided for research and discussion papers/presentations on new, emerging and evolving issues that affect the management of public records in this State. It does not set forth Department of the Treasury policies, procedures, requirements or standards, and is not intended to endorse specific solutions, products or services.

A.1 Research Forum

Parties interested in posting papers and/or presentations here may send proposed materials to RMS State Records Center, 2300 Stuyvesant Avenue, Trenton.

Research Papers:

Security for the Networked Enterprise, Elements of a Holistic Approach

Planning for Cloud Procurements

PowerPoint Presentations on the Department of the Treasury's Electronic Records Management Program (Presentations by the Department's Division of Revenue and Enterprise Services to the State Records Committee):

New Jersey Department of the Treasury Records Management Services - March 2017

Update on Electronic Records Management Program - December 2017

Social Media Policy/Procedures - December 2018

References

[1] Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS), AIIM ARP1-2009, (2009), Association for Image and Information Management, Silver Spring, Md.

[2] The National Archives and Records Administration provides useful background information on trustworthy systems and digital signature technology. See "NARA Bulletin 2006-02 Attachment 2 Policy for Effective and Comprehensive Management of Electronic Records," National Archives and Records Administration, December 15, 2005

[3] The OIT items are Information Disposal and Media Sanitization (09-10-NJOIT, 09-10-S-1-NJOIT and 09-10-S-2-NJOIT), Office of Information Technology, April 8, 2011 and Personal Naming Standards for E-Mail Addresses (94-04-NJOIT), Office of Information Technology, October 2, 2008. The NARA bulletins are NARA Bulletin 2000-02, Disposition of Electronic Copies; Suspension of NARA Bulletin 99-04, December 27, 1999. National Archives and Records Administration, 2000 and NARA Bulletin 2008-05 Guidance Concerning the Use of E-mail Archiving to Store E-mail, July 31, 2008. National Archives and Records Administration, 2008.

[4] NARA published a useful discussion on managing public records in the social media context. See NARA Bulletin 2011-02 Guidance on Managing Records in Web 2.0/Social Media Platforms, October 20, 2010. National Archives and Records Administration, 2010.

[5] In-Place Hold, (n.d.), Microsoft Corporation, Redmond Washington, http://technet.microsoft.com/en-us/library/ff637980.aspx.

[6] Mary Mack, Dennis Kiker and Tom Mighell, Effective Management of Litigation Holds and e-Discovery, (May, 2009), Association of Corporate Counsel, Washington, DC, http://www.fiosinc.com/e-discovery-knowledge-center/electronic-discovery-article.aspx?id=583.

[7] See The Search Is On: State CIO Starting Points for E-Discovery, (November 2007), National Association of State Chief Information Officers, Lexington, KY, http://www.nascio.org/publications/documents/NASCIO-TheSearchIsOn.pdf, for the CIOs perspective on approaching e-discovery.

[8] When reviewing NARA's information, remember that only the technical guidance applies. The legal frameworks, policies and procedures apply to Federal agencies.

[9] Jonathan de Boyne Pollard, (2004), "Mbox' is a Family of Several Mutually Incompatible Mailbox Formats," http://homepage.ntlworld.com./jonathan.deboynepollard/FGA/mail-mbox-formats.html . Be aware that the author suggests MBOX is less-than optimal and points to the emergence of format called Maildir.