



THE WONDERFUL
WIZARD of

*Records & Information Management
Back to the Basics*

Karen Anne Perry
Records Analyst I
Department of the Treasury
Division of Revenue and Enterprise Services
Records Management Services
2022

L. FRANK BAUM

Disclaimer: The content of this presentation is designed for educational and informational purposes only.

New Jersey Public Agencies' - Constituency Base

- Federal, State, County/Local, Boards, Authorities
- Parents, Legal Guardians, The General Public
- Unions, Associations & Additional Groups
- Legal Counsel
- Healthcare Facilities & Professionals
- Financial Institutions & Auditors
- Private Sector & Vendors
- The Media – Print, TV/Cable, Radio, etc.
- Internet & Social Media
- The International Arena



The Global Transmission of Information via the Internet is $\frac{2}{3}$ the Speed of Light. This further compounds the concerns for:

- Data Security
- Access
- Regulatory Compliance
- Retention, Preservation & Disposal

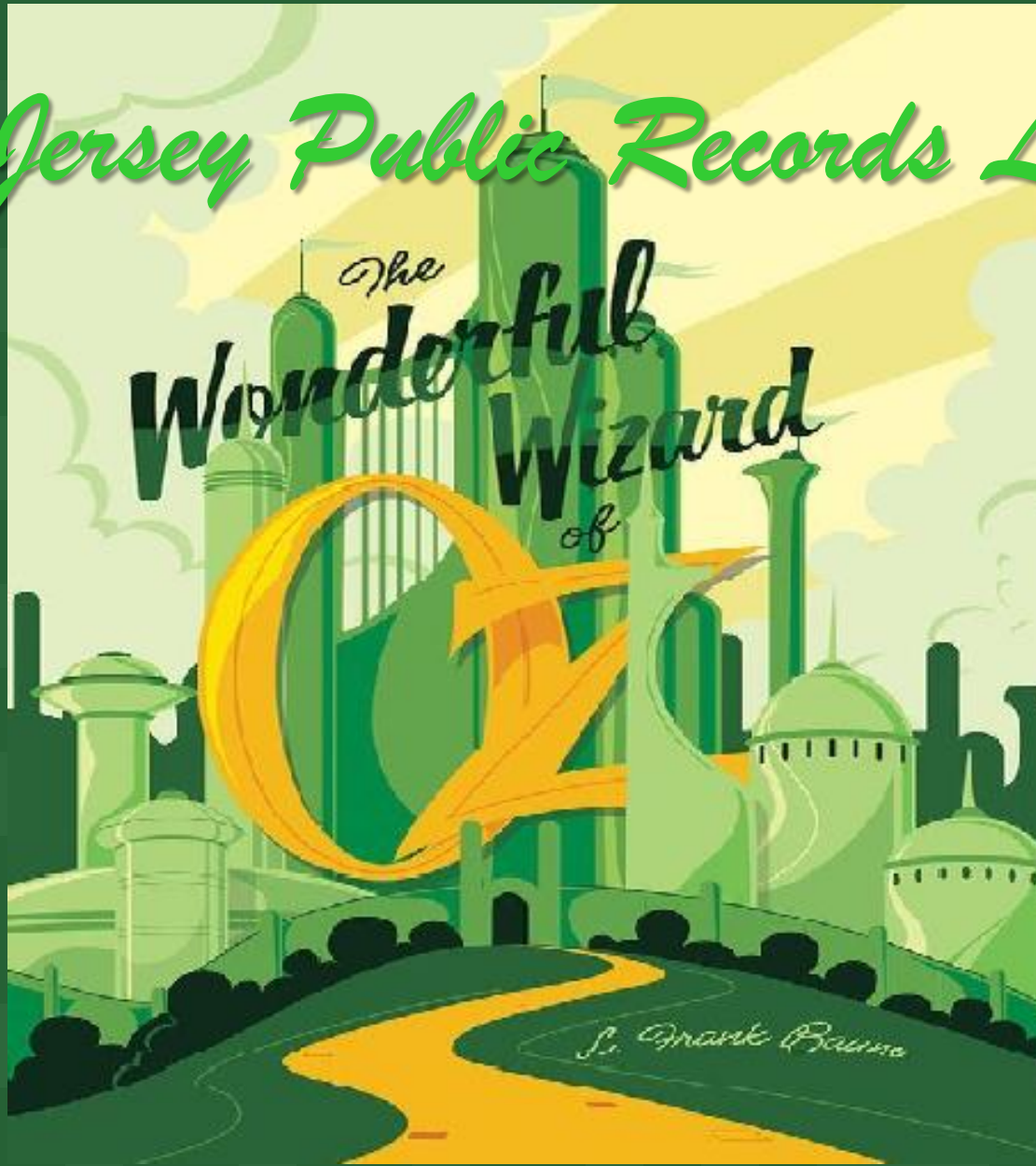


Records and Information Management (RIM)

Why Should You Care?

- It's the Law - Government records & information are Public Records and must be protected from theft, corruption or unlawful access.
- Cost Effective - minimize costs and promotes savings, efficiency and productivity.
- Valuable Asset - Loss, theft or damage can cause financial loss, disrupt business operations and damage an agency's reputation resulting in loss of public confidence.
- Historical/Legacy Information - Irreplaceable loss of intellectual rights, historical records, etc.
- Litigation and e-Discovery Support - International, Federal & State
- Audit Compliance - International, Federal & State
- OPRA Compliance - Promotes Public Records Access, Transparency and Accountability
- Regulatory Compliance - International, Federal & State - the European Union's *General Data Protection Regulation (GDPR)* & Regulation (EU) 2016/679 for privacy and protection of processing of personal data; *Sarbanes-Oxley Act (SOX)* which protects shareholders from accounting errors & financial fraud; *Health Insurance Portability and Accountability Act (HIPAA)* for personal medical information and the NJ Public Records Laws, etc.

New Jersey Public Records Law



The
Wonderful
Wizard
of

S. Frank Baum

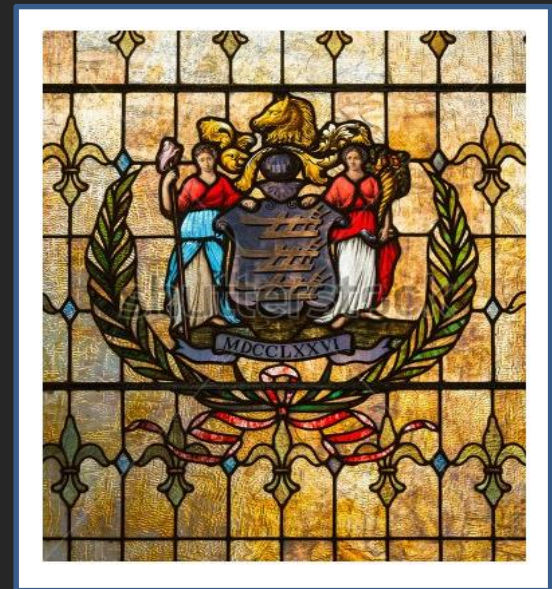
Destruction of Public Records Act

PL 1953, c. 410

State Records Committee

The Destruction of Public Records Act (PL 1953, c. 410) created and entrusted the State Records Committee (SRC) with having *final authority* over the retention and disposition of *all* New Jersey Public Agency records. The SRC consists of representatives from:

- State Treasurer
- State Attorney General
- State Auditor
- State Archives
- Department of Community Affairs,
Local Government Services



Destruction of Public Records Act,

PL 1953, c. 410/NJSA 47



What Actually is a Public Record?

Information, regardless of its medium (hardcopy, microform, digital, electronic, and Internet-based) that is created, received, maintained and distributed by a public agency receiving tax payer dollars and serves as Evidence of the Transactions of its Normal Course of Business.

Destruction of Public Records Act, PL 1953, c. 410/NJSA 47

"Public" Can Have Two (2) Meanings

1. Ownership - A record is Public when it is evidence of the normal course of business of a government agency which receives a substantial contribution of tax dollars to conduct its activities.

2. Access - The Open Public Records Act (OPRA)/PL 2001, c. 404, NJSA 47:1A et seq., provides that public records must be accessible. However, because of issues of *Privacy, Confidentiality and Security*, an agency may restrict access to records - Classified National Defense Records *are* Public Records but due to National Security they are *not* accessible.

Open Public Records Act (OPRA)

PL 2001, c. 404, NJSA 47:1A et seq.

In most instances, agencies were required to allow access to records under *The Right to Know Law*. The Open Public Records Act (OPRA) PL 2001, c. 404, NJSA 47:1A et seq. replaced *The Right to Know Law* regarding public records access:

- Provides that Public Records must be made accessible to the public in *most** cases.
- Established the position of Custodian of Public Record** for all public agency record-keepers.
- Personal Financial & Legal Accountability for intentional denial of public records access.

****NOTE:** When possible, the OPRA Custodian of Public Record should also be the ARTEMIS Public Records Custodian to legally authorize the disposal of their Agency's Public Records for legal compliance and OPRA accountability.

However, the degree of a record's accessibility does *not* determine whether a record is Public or Private.

*An agency may restrict access to records due to considerations of :

- Privacy
- Confidentiality &
- Security

The **Government Records Council** (GRC) is the Government Entity created under OPRA to respond to OPRA inquiries/complaints from the Public & Records Custodians, issue advisory opinions and mediation/resolution of disputes.

New Jersey Government Records Council



New Jersey Government Records Council

P.O. Box 819

Trenton, NJ 08625-0819

Phone: (609) 292-6830

Fax: (609) 633-6337

Toll-Free 1-(866) 850-0511

E-Mail: Government.Records@dca.nj.gov

Website: <http://www.nj.gov/grc>

National Archives and Records Administration (NARA)
Washington DC

It's not just New Jersey...

What Are Federal Records?

Federal Records Act of 1950, United States Code Title 44

NARA defines Federal Records as:

- ✓ All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business.
- ✓ Federal records must be preserved by an agency - as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the United States Government or because of the informational value of the data in them.



Spoliation: The destruction of or failure to preserve evidence relevant to litigation or investigation.

Spoliation: The destruction of or failure to preserve evidence relevant to litigation or investigation.

Litigation Hold Order – Electronic Data

For Discussion Purposes Only

Consult With Legal Advisors When Dealing With Litigation Hold Orders

SAMPLE

<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.

Litigation Hold Order – Electronic Data continued...

- 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.

Litigation Hold Order Acknowledgement of Receipt

For Discussion Purposes Only

Consult With Legal Advisors When Dealing With Litigation Hold Orders

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.



Back to where it all started...



IT WAS SOME TIME BEFORE THE Cowardly Lion awakened, for he had lain among the poppies a long while, breathing in their deadly fragrance; but when he did open his eyes and roll off the truck he was very glad to find himself still alive.

Records Inventory, Retention and Disposition

PL 1953, c. 410/NJSA 47

- Records Retention Schedules must be created for all Public Records maintained by all New Jersey Public Agencies.
- Request and Authorization for Records Disposal must be submitted by the Public Agency of ownership, to DORES-RMS (through Artemis), in order to obtain prior authorization for the disposal of their Public Records whose retention periods have **EXPIRED**.

Records Inventory

A Records Inventory can be invaluable in the event of an OPRA Request, Audit, e-Discovery, Litigation, etc. - it is a complete and accurate listing of all records maintained by an agency (e.g., paper, microform, digital, Web- and Internet-based) that indicates:

- How & Where Physically Stored
- Volume
- Classification
- Retention Periods as per the agency-specific Records Retention Schedule
- Disposition
- Federal & State Regulations, Statutes & Codes

Records Inventory continued...

RECORD SERIES INVENTORY		INSTRUCTIONS: USE ONE FORM PER RECORD SERIES				
DEPARTMENT		DIVISION		OFFICE		
CONTACT PERSON (Name, Title, Phone Number)				DATE INVENTORY COMPLETED		
RECORD SERIES TITLE and DESCRIPTION (How the record functions, what information it contains, form number)						
PAPER	<input type="checkbox"/> LETTER SIZE	<input type="checkbox"/> LEGAL SIZE	<input type="checkbox"/> BOUND BOOK	<input type="checkbox"/> RINGED NOTEBOOK	<input type="checkbox"/> PUNCH CARD	<input type="checkbox"/> CARD FILE: SIZE: ___ X ___
	<input type="checkbox"/> OTHER: _____					
MICROFILM	<input type="checkbox"/> ROLL SIZE: _____ mm	<input type="checkbox"/> FICHE	<input type="checkbox"/> OTHER: _____			
MAGNETIC	<input type="checkbox"/> COMPUTER TAPE SIZE: _____	<input type="checkbox"/> AUDIO TAPE SIZE: _____	<input type="checkbox"/> VIDEO TAPE SIZE: _____			
MEDIA	<input type="checkbox"/> DISC SIZE: _____	<input type="checkbox"/> OTHER: _____				
FILING METHOD	<input type="checkbox"/> ALPHA BY _____	<input type="checkbox"/> NUMERIC BY _____	<input type="checkbox"/> CHRONOLOGICALLY BY: <input type="checkbox"/> CALENDAR YEAR			
	<input type="checkbox"/> FISCAL YEAR					
REFERENCE RATE	<input type="checkbox"/> DAILY	<input type="checkbox"/> WEEKLY	<input type="checkbox"/> MONTHLY	<input type="checkbox"/> YEARLY	<input type="checkbox"/> OTHER: _____	
INCLUSIVE DATES	RECORD SERIES RANGE	RECORDS LOCATION	RECORD TYPE	EQUIPMENT TYPE	VOLUME	
FROM	TO	(e.g., L1-Ru, 300-650)	(Building, Room, Floor Number)		(Cubic Feet)	
LIST OTHER SOURCES AND LOCATIONS OF THIS RECORD SERIES						
ANNUAL ACCUMULATION (In Cubic Feet)	APPLICABLE STATUTES/REGULATIONS	IS AN EXTERNAL AUDIT REQUIRED?		IS RECORD SERIES LISTED ON A RECORDS RETENTION SCHEDULE?		
		<input type="checkbox"/> YES	<input type="checkbox"/> NO	<input type="checkbox"/> YES	<input checked="" type="checkbox"/> NO	
				IF NO, CONTACT DORES RECORDS MANAGEMENT SERVICES.		

Records Retention

Mandated by the New Jersey Public Records Laws PL 1953, c. 410/NJSA 47, Records Retention Schedules are a detailed listing of the records maintained by an agency and the MINIMUM Legal and Fiscal time periods they must be retained.

Records Retention Schedules address:

- Vital Records
- Legal, Fiscal & Administrative Value
- Historical Records
- Confidentiality
- Records Retention
- Final Disposition

Records Retention and Artemis



Records Retention and Disposition Management System (Artemis) Division of Revenue and Enterprise Services Records Management Services

Artemis enables users to:

- Search - General & Agency Records Retention Schedules,
- Create Electronic Records Disposal Requests and Status - Pending, Approved & Denied,
- Produce Authorized Records Disposal Requests for OPRA Requests, and
- Create Reports - Records Retention & Disposal.

Records Retention

Artemis-Generated Records Retention Schedule

Department of the Treasury, Division of Revenue and Enterprise Services, Records Management Services

Records Retention and Disposition Schedule		Agency: S821110	Schedule: 002	Page #: 1 of 4
Department:	Treasury - Supplemental Annuity Collective Trust (SACT)	Agency Representative:		
Division:		Title:		
Bureau:		Phone #:		

SCHEDULE APPROVAL: Unless in litigation, the records covered by this schedule, upon expiration of their retention periods, will be deemed to have no continuing value to the State of New Jersey and will be disposed of as indicated in accordance with the law and regulations of the State Records Committee. This schedule will become effective on the date approved by the State Records Committee.

Status	Last Updated Date/Time	Approved Date	Effective Date
Published	3/18/2015 3:56 PM		

Record Series #	Record Title and Description	Audit	Alternate Media	Archival Review	Vital Record	Confidential	Retention Policy		Disposition	Citation
							Total Retention Period	Minimum Period in Agency		
0001-0000	Authorization of Disbursement --- Form authorizes the disbursement of checks from the SACT section.						7 Years	7 Years	Destroy	
0002-0000	Bank Record File --- Contains: acknowledgements, deposit slips, reconciliations, and bank statements.						7 Years	7 Years	Destroy	
0003-0000	Cash Disbursements Journal - Manual Input --- Contains: payment totals, check dates, and reason for refunds.						7 Years	7 Years	Destroy	
0004-0000	Cash Disbursement List --- List of cash disbursements for various programs types (i.e., retirements, withdrawals, deaths). Serves as a cross-reference of terminations for supplemental annuity cases.						7 Years	7 Years	Destroy	
0005-0000	Cash Receipt File --- Contains cash receipts documents and a listing of contributions from the various pension funds, utilized for monthly journal entries.						7 Years	7 Years	Destroy	

* P - Public, C - Confidential

Records Disposal



Create Disposition Request

Request Id : N/A

Status : Work In Progress

*Agency:

*Schedule #:

Limit Record Series to:

Requester First Name: Requester Last Name:

Custodian Name: Custodian First Name:

Microfilm Present: Digital Image Present:

Location:

Request Date: / /

Requester Title:

Custodian Last Name:

Damaged Records Certificate:

Comments:

Is this request for the Disposition of Emails? Yes No

Would you like to sign this Disposition Request Electronically? Yes No

Does this Disposition Request require a Local Agency Auditor's Signature? Yes No

Disposition Request Details

S.#	Record Series #	Title	Retention Period	From (MM/yyyy)	To (MM/yyyy)	Dispose After (MM/yyyy)	Medium Type	Volume (Cu. ft)
1	0002 - 0000	Annual Financial File (Copy)	7 Years				Paper	.00

[Add New Row](#) [Add Multiple Rows](#)

Requester Approver Auditor eSignature History

[Upload Disposition Form / Supporting Documents](#)

[Save](#) [Submit](#) [Delete](#) [eSign / Reroute](#)

[Print](#)

Records Disposal – Artemis and Email

DISPOSITION: For E-mail to be legally destroyed, an email-defined Artemis Request and Authorization for Records Disposal must be submitted for authorization before disposal can occur.

Artemis
RECORDS RETENTION AND DISPOSITION MANAGEMENT SYSTEM

Home | My Profile | Contact Us | Help | FAQ | Training Video

Disposition Management | Retention Schedule | System Management | Reports

Board of Education
High Bridge Borough School District - jonesc - M700000 | LOGOUT

Create Disposition Request Request Id : N/A Status : Work In Progress

*Agency: M700105 - Financial

*Schedule #: M700105-001-Financial

Limit Record Series to: those not requiring archival review

*Request Date: 06 / 24 / 2019

Requester First Name: Christopher Requester Last Name: Jones Requester Title:

Custodian Name: --Select-- Custodian First Name: Custodian Last Name:

Microfilm Present: Digital Image Present: Damaged Records Certificate:

Location: Comments:

Is this request for the Disposition of Emails? Yes No

Would you like to sign this Disposition Request Electronically? Yes No

Does this Disposition Request require a Local Agency Auditor's Signature? Yes No

Disposition Request Details

S.#	Record Series #	Title	Retention Period	From (MM/yyyy)	To (MM/yyyy)	Dispose After (MM/yyyy)	Medium Type	Volume (Cu. Ft)
1	0002 - 0000	Annual Financial File (Copy)	7 Years				Paper	.00

Add New Row Add Multiple Rows

Requester Approver Auditor eSignature History

Upload Disposition Form / Supporting Documents

Save Submit Delete eSign / Reroute Print

Developed by Sunrise Systems Inc. Artemis (RELEASE) (3.2.1.11)

Email Disposal Request

Records Disposal - Artemis-Generated Request & Authorization for Records Disposal

Request Id: 34274

Status: Authorized

Agency: S821112 - Treasury-Pensions & Benefits-Financial Services

Image Type: Disposition Request Packet



This Disposition Request is selected for Electronic Signature. Disposition Form upload is not required. However, you may upload any supporting documents.

Status:





1



2



3

Department of the Treasury, Division of Revenue and Enterprise Services, Records Management Services

REQUEST AND AUTHORIZATION FOR RECORDS DISPOSAL		Instructions: This request must be submitted prior to the disposition of any public records. Items 1. through 14 must be completed in full and Items 15.A and 15.B signed for fiscal records. NOTE: In the event of an unexpected scanning failure, until the problem is resolved, the form may be sent to: DISPOSAL REQUESTS, Department of the Treasury, Division of Revenue and Enterprise Services, Records Management Services, P.O. Box 661, Trenton, N.J. 08625-0661. Questions, call 800.630.7404.		1. Requesting Agency Name and Address Treasury - Pensions & Benefits 50 West State Street PO Box 295 Trenton NJ 08625			
				1.A Agency Retention Schedule Number S821112 - 002			
2. Request Id/Date 34274 3/8/2016	3. Requested By (Electronically Signed by)	4. Request Approved By (Electronically Signed by)		5. Records Manager			
6. Archival Review Not Required		7. Early Records Disposal (Due to Document Conversion or Damage) Microfilm Digital Image Damaged Records Certificate		8. Comments - Document Conversion or Damage			
Authorization is hereby requested for the disposal of the following public records in accordance with New Jersey P.L. 1953, c. 410 as amended. It is further certified that the record series listed herein have exceeded their respective retention periods and are not involved in any action, such as a pending OPRA request, litigation, or anticipated litigation as per the Federal Rules of Civil Procedure, December 2006; and are not required for a present or a future audit.							
#	9. Record Series #	10. Record Series Title	11. Retention Period	12. Inclusive Dates From (MM/YYYY) To (MM/YYYY)		13. Dispose After	14. Volume (in Cubic Feet)
1	0001-0000	Annual Statement Workpapers	10 Years	01/2004	12/2005		1.00

For Records Management Services Use Only :	Total Volume :	1.00
--	----------------	------

15. Audit Verification		16. Authorization		17. Disposition	
15.A Auditor (Electronically Signed by) <i>William D. Robinson</i> (000)	16.A Authorization Date	16.B Authorization Number			
15.B Date	16.C Authorizing Signature , Records Management Services <i>L. P. ...</i>		17.A Verification Signature	17.B Date	



RECAP

- Submit - Electronic Requests for Authorized Records Disposal
- Search - General & Agency Records Retention Schedules
- Create – Electronic Records Disposal Requests and Status - Pending, Approved & Denied
- Produce – Authorized Records Disposal Request for OPRA Requests, Audits & Litigation
- Create – Customized Records Retention & Disposal Reports

Artemis

Reference Manual



PS: The **HELP** button on the Artemis Home Page is the Artemis Reference Manual.



Records Management Tools to Help Improve Your OPRA Program

The OPRA Custodian of Public Record should also be the ARTEMIS Public Records Custodian to legally authorize the disposal of their Agency's Public Records for legal compliance with the NJ Public Records Laws and to mitigate incoming OPRA requests

Conduct a Records Inventory to identify: Active/Obsolete, Confidential, Historical and Vital Records.

Utilize the Records Retention Schedules to determine when records retention have expired and may be disposed.

Create and Submit Records Disposal Requests for Obsolete Records and ensure the records are destroyed after authorization has been received – otherwise as long as they are in your physical custody, they are **DISCOVERABLE**.

*Records and Information Management Alternatives –
Imaging*



Records and Information Management Alternatives — Imaging



As per PL 1994, c. 140, the State of New Jersey allows for the replacement of hardcopy public records with digital images (e.g., Optical Disk, CD, DVD, Magnetic Tape & Microfilm). The State Records Committee and Records Management Services issues Initial and Annual Renewal Imaging System Certifications to an Agency for an in-house or outsourced imaging application. Documents required for obtaining Imaging Certification from the State Records Committee and Records Management Services include:

➤ Image Processing System Initial Registration Application

- Scanning Policy and Procedures
- Disaster Prevention and Recovery
- Data Migration Path
- Feasibility Study
- RFP/RFI/RFB
- Vendor Detail
- Imaged Records Series List
- Proof of Public Notice

➤ Annual Review/Amendment

- Scanning Policy and Procedures
- Disaster Prevention and Recovery
- Data Migration Path
- Imaged Records Series List

Records and Information Management Alternatives - Imaging continued...





 State of New Jersey
 Division of Revenue and Enterprise Services (DORES)
 Records Management Services - RMS

IMAGE PROCESSING SYSTEM REGISTRATION APPLICATION

[N.J.A.C. 15:3-5et seq.] BEFORE completing this application, please read the [Instructions](#).

AGENCY NAME: _____

This is an application for:

In-house Imaging System
 Service Bureau Imaging
 Special Do

APPLICATION PACKAGE CHECKLIST

Review Form
 Feasibility Study and or RFP/RFI/RFB
 Data Migration Report (replacement s

Imaging Registration
 Annual Review/Amendment Form

Mailing: PO Box 661, Trenton, NJ 08625-0661
 Location: 33 W. State St. 5th Floor Trenton, NJ 08625
 609-292-8711

ANNUAL REVIEW AMENDMENT ANNUAL REVIEW


AGENCY NAME :
CERTIFICATE #:

Primary Contact Name:
 Address:

Phone/fax/email:

Imaging Registration
 Imaged Records Series List

Mailing: PO Box 661, Trenton, NJ 08625-0661
 Location: 33 W. State St. 5th Floor Trenton, NJ 08625
 609-292-8711



Complete this form and email to your Records Analyst.

AGENCY NAME:
CERTIFICATION NUMBER:

RETENTION SCHEDULE AGENCY NUMBER: **SCHEDULE NUMBER:**

Record Series Number	Record Series Name	Retention Time	Inclusive Years	Back-up? (paper, microfilm, or migration path)

The title card for 'The Wonderful Wizard of Oz' features the title in a stylized, maroon-colored font with a gold outline. The words 'The Wonderful Wizard' are in a smaller font, while 'of Oz' is in a larger, more prominent font. The background is a classic illustration of the yellow brick road winding through a lush, green landscape under a warm, golden sky.

The
WONDERFUL
WIZARD *of* OZ

A Picture
Book Adaptation

*Records and Information
Management Alternatives –
The Cloud*

Records and Information Management Alternatives – The Cloud



The Cloud

Cloud Storage – Internet-based of shared resources, software, and data/information for immediate access. Based on a common server site, inexpensive and mobile, low maintenance and Internet-based. The cloud structure consists of:

- Client – Hardware or software dependent upon the cloud to function
- Application – Software downloaded via the Internet to a desktop/laptop
- Platform – Cloud computing structure that houses the applications/software
- Infrastructure – Complete, packaged virtual platform environment per desktop/laptop
- Server – Operating system from simple to complex per client

NOTE: Refer to DORES-RMS Website for guidance pertaining to the Records Management and the Cloud.

<https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforRecordsManagementintheCloud.pdf>

NOTE

Due to the fluid and fragile nature of virtual cloud storage and its data, precautions must be taken when dealing with Database Data, Metadata, Portable Data, Text Messages, and Email.

Records and Information Management Alternatives – The Cloud continued...

Cloud-based computing systems/services enable mobile work forces to access government systems outside of traditional office settings. Whether stored in the Cloud or in agency-owned storage systems, these public records are crucial to the organization of our society and essential to the daily operation(s) of government.

Their value of some records endure beyond their active use, because they provide unique evidence of significant actions and transactions that have affected the public regardless of their medium: 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.

Records and Information Management professionals should work across disciplinary lines to protect these records:

- 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

Records and Information Management Alternatives – The Cloud continued...

Things to Consider When Storing in the Cloud

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.
2. Ensure that Cloud storage facilities allow the agency to classify stored records in accordance with approved State/County/Local records retention schedules.
3. Require the use of controls that prevent unauthorized access, manipulation, distribution, defacement and/or destruction of records stored in the Cloud facility.
4. Be aware of storage 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).
6. Prohibit the contractor from deleting/destroying Cloud-based records unless the agency specifically directs the action.
7. Institute data/content management protections.

Records and Information Management Alternatives — The Cloud continued...

8. To the maximum extent possible, use non-proprietary and/or widely used (de-facto standard) file formats for Cloud records storage.
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.
10. Specify records transfer requirements for contract-exit processes and other operational purposes.
11. Ensure that records are retrievable and reproducible in response to Open Public Records Act (OPRA) requests, audits, subpoenas and investigations.
12. Participate in planning for service levels with your information technology and procurement teams.



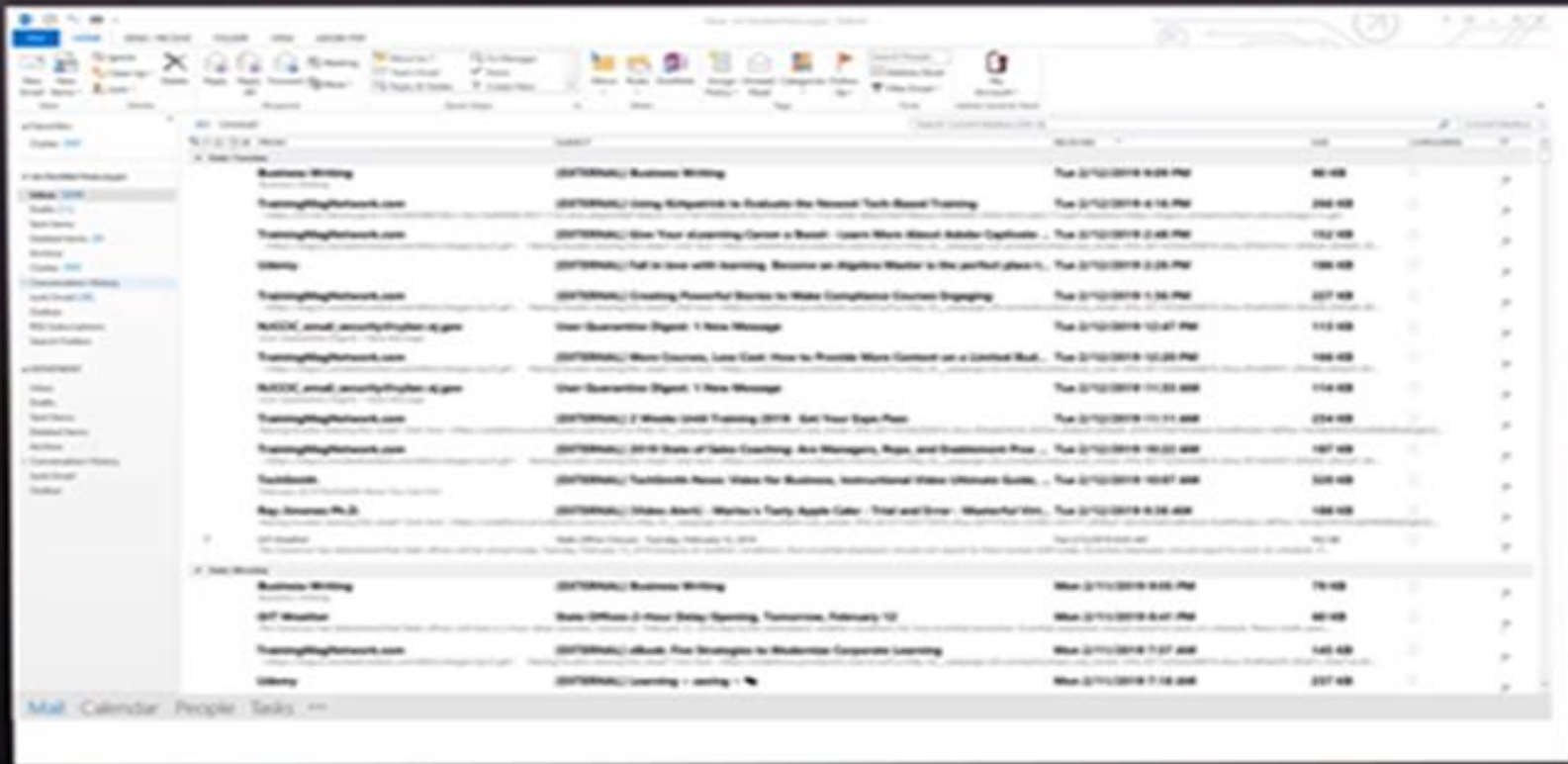


Electronic Records

YOU'VE ALWAYS HAD THE POWER
MY DEAR, YOU JUST HAD TO
LEARN IT FOR YOURSELF.

-GLINDA-

WIZARD OF OZ



Email.....

e-mail

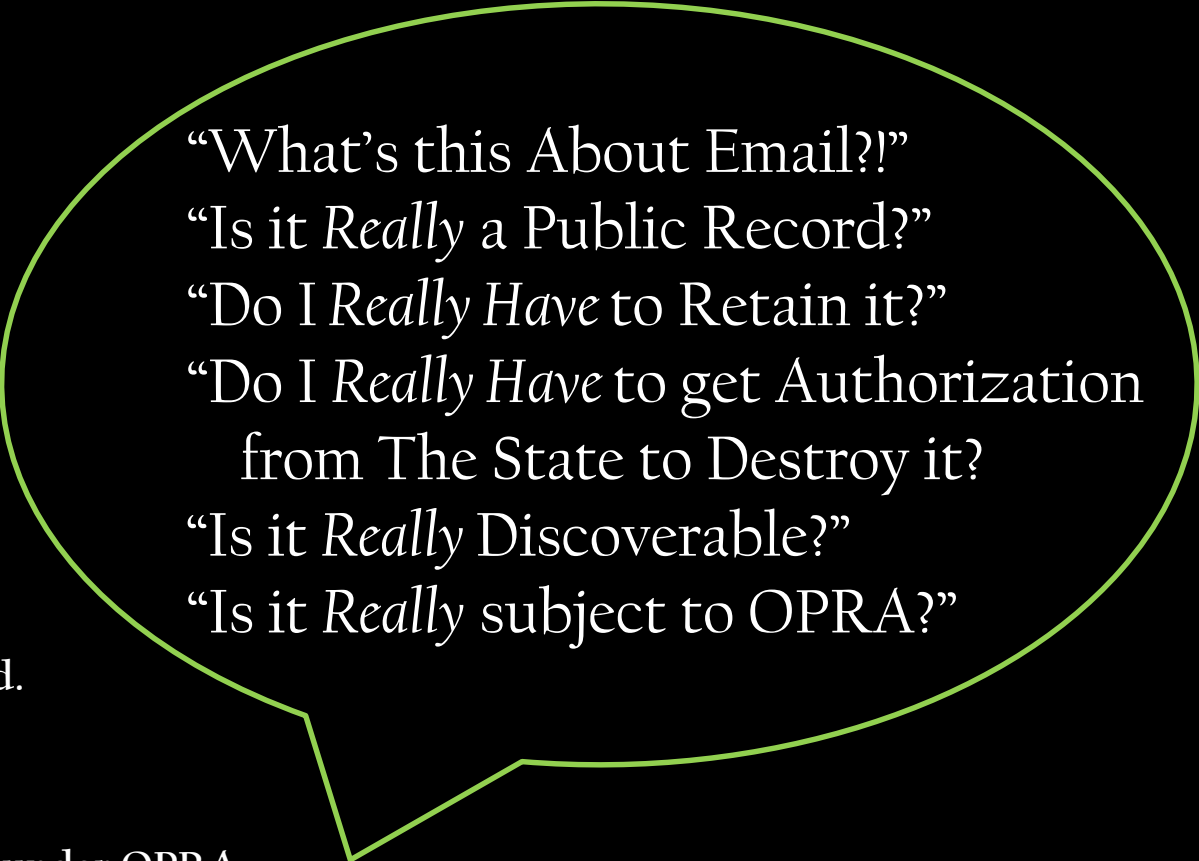
–noun 1. a system for sending messages from one individual to another via telecommunications links between computers or terminals.

2. a message sent by e-mail: Send me an e-mail on the idea.

–verb (used with object) 3. to send a message by e-mail.
Also, E-mail, email.

- Email (including content, metadata, and attachments) are created, sent, or received electronically; therefore they are Public Records with the same Records Retention, Disposition, Access, Intellectual Property, Legal Rules of Evidence and e-Discovery concerns.
- This also includes Email, Instant Messaging, Blogs, Wikis, Pod Casts, Social Media, etc.

Email continued...

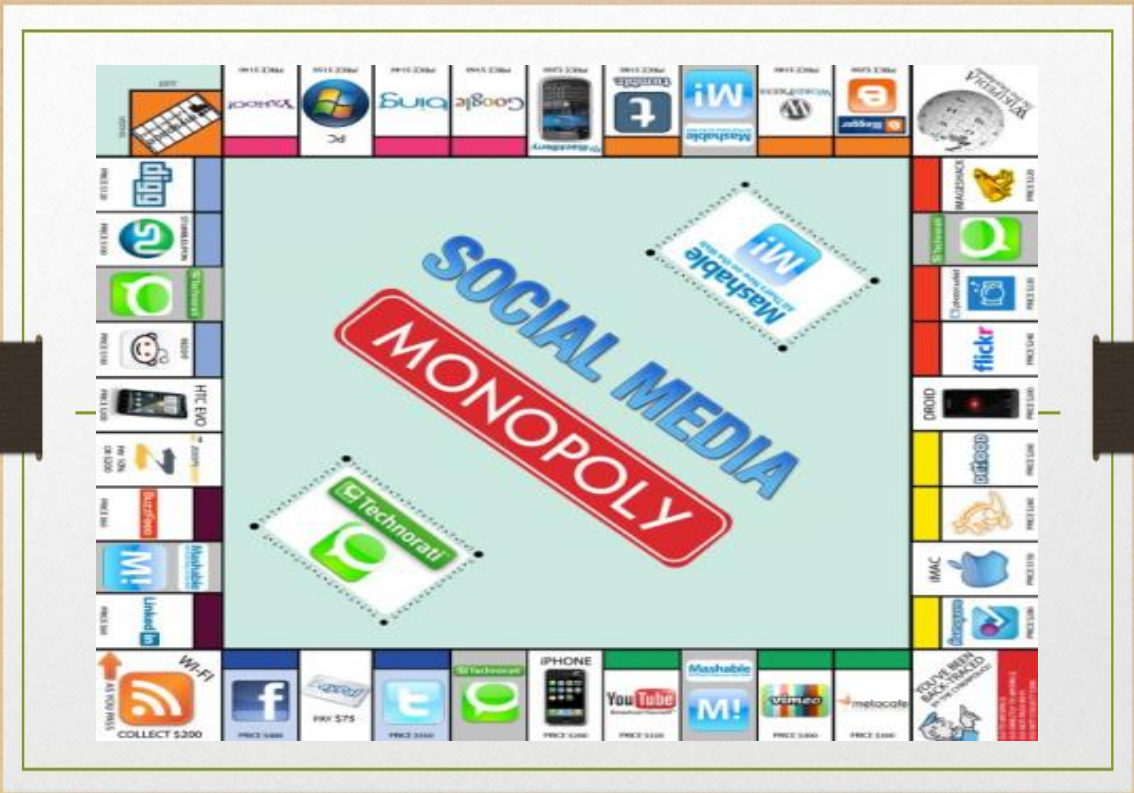


“What’s this About Email?!”
“Is it *Really* a Public Record?”
“Do I *Really Have* to Retain it?”
“Do I *Really Have* to get Authorization
from The State to Destroy it?”
“Is it *Really* Discoverable?”
“Is it *Really* subject to OPRA?”

- ✓ Email is a Public Record.
- ✓ Email is Discoverable.
- ✓ Email may be Accessed under OPRA.
- ✓ Email may be Disclosed in a Court of Law.
- ✓ Email may be Disclosed through e-Discovery.
- ✓ Email must be placed on a Records Retention Schedule.
- ✓ Email may *not* be destroyed without prior Records Management Services’ authorization.

Email Management

- Consult the General Schedule for the **general 7-year retention period** regarding the Retention and Disposition of Email.
- Adopt policies for Email and Internet usage - with **ongoing** Agency-wide training.
- The Email System should have Security Controls that guard against unauthorized access, use, modification, dissemination, disclosure and/or destruction. NOTE: Email is often a phishing target that can lead to an malware attack.
- The Email System should have provisions for the administration of **“Litigation Holds”**.
- The Email System should also include Back-up and Disaster Recovery for the restoration of Email.
- Only *authorized* Agency IT and/or Records Management Staff should control the management, access, retention and disposition of Email records in **the Email Central Storage/Management System**.



Social Media

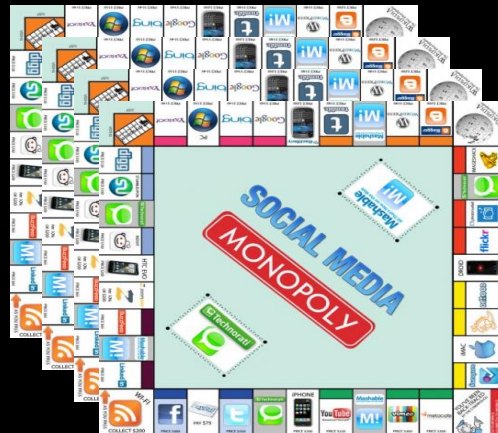
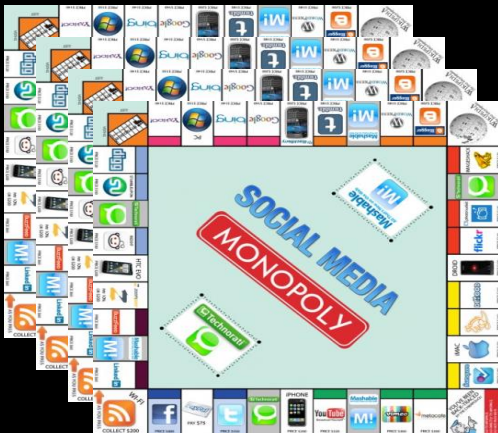
Social Media - Interactive communication via web-based and mobile technology.

- Social Media Is - Global, Immediate and Very Accessible!
- Social Media Is Not - Private.
- Social Media Is Public - in the event of e-Discovery, Litigation and Legal Rules of Evidence, directives should be established regarding content, language, subject matter, which includes: Instant messaging, blogs, Wikis, Pod casts, Metadata and Email.
- A Disclaimer - should accompany the data being placed on a Social Media site and hardcopy should be printed as an audit trail in the event of an OPRA Request, e-Discovery, Litigation, etc.
- Social Media is Not - the same as Digitally-borne or Website records. On your own website, you have control and you can print hardcopy and protect it; whereas with Social Media, you cannot control it and it can be altered and/or removed .

Social Media continued...

- Security - Social Media can be altered and used as a portal for Cyberattack, which presents a real concern for an agency's ability to operate effectively and release vital public information.
- Passwords - use different passwords for every social network used - a single password enables a hacker to get access to everything.
- Be careful of your mailbox - direct messages are a form of phishing to get access.
- Stay Professional - personal information can give hackers fuel for the fire and can lead to an attack and potential Identity Theft.

Refer to DORES-RMS Website for guidance pertaining to the Records Management and Social Media.
<https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforSchedulingSocialMediaRecordsforRetentionandDisposition.pdf>



Social Media Guidelines

Guidelines on Retention Scheduling Public Records Stored on Social Media Platforms

Introduction

These guidelines include suggested action steps for creating retention/disposition policies for public records created and stored via social media services like [Facebook](#), [Twitter](#), [LinkedIn](#), [YouTube](#), [wikis](#) and other Internet-based platforms. Social media services involve various forms of content, including text, images, audio and video recordings. Public agencies can begin to deal with the retention scheduling challenge by executing the recommended action steps.

Applicability of Public Records Law Records generated and received via social media services and stored on social media platforms are subject to the State's public records law.

Audience Generally, these guidelines are designed for professionals who work in records and information management capacities.

Note on Scope 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.

Key Contacts New Jersey Division of Revenue and Enterprise Services' Records Management Services Unit (RMS): 609-777-1020 or 609-292-8711 and the State Archives: 609-633-8304 or 609-292-6260 for permanent and historical records.

Social Media Guidelines continued...

Guidelines on Retention Scheduling Public Records Stored on Social Media Platforms

Action Steps

1. Inventory of Social Media
2. Conduct a Value Assessment(s)
3. Assign Retention and Disposition Policies to Social Media Records as found in Records Retention Schedules.
4. Choose Modes of Storage for Social Media Records
5. Implement the Retention and Disposition Program



The World Wide Web a.k.a. *The Internet*

The World Wide Web - The Internet



The World Wide Web or the Internet, is how Government operates with other Government Agencies, Business, Industry, Finance, Healthcare, Education, etc. The Web is comprised of three (3) different strata:

❑ Surface Web

The **unencrypted** part of the Internet accessible by government, education, business and industry, finance, healthcare, the general public, etc. through the use of conventional search engines, such as Google, Bing, etc.

❑ Deep Web

The part of Internet that cannot be reached by conventional search engines. Unauthorized access or hacking may be employed to obtain the information in the Deep Web such as, Medical Records, Student Records, Government Documents, etc.

❑ Dark Web

The encrypted part of the Internet that refers to alleged **questionable** content that is not easily reached and requires the multi-layered Tor software for access.

The World Wide Web - The Internet continued. . .

Due to its ever-changing content and structure, an agency's website documentation should be maintained. They reflect hardware, software, Metadata, content and their respective areas of concern:

- IT Perspective - reflects website creation, maintenance, growth and security including **data encryption** methods employed.
- Intellectual Property & Historical Perspective - digitally-born documents if not printed to hardcopy could be lost forever
- Legal Perspective - records needed for Litigation, Legal Rules of Evidence and e-Discovery
- Financial Perspective - records needed for a Local, State and/or Federal Audit
- Records Management & Access Perspective - verify retention & disposition in the event of an OPRA Request.

NOTE: Refer to the DORES-RMS General Schedule for the retention and disposition of Agency Website Records.



Data Security

Data Security – Is it really secure???

In their daily, normal course of business, Government Agencies use Information Technology, Networking, Mobile Computing, Telecommunications, Email, the Cloud and Social Media

While this creates Operational Efficiencies, it can also create the potential for Overlapping Internal and External Operational Threats such as:



- Disrupt or Shutdown Operations
- Legal, Intellectual, Political, Financial & Security Ramifications
- Alter, Corrupt or Destroy Information
- Physical Harm
- Exploitation to Ruin an Agency's Credibility & Reputation

Data Security continued...

Data Security is a rapidly evolving and highly technical area that is typically handled by an agency's IT department, which works in coordination with legal, records management*, human resources and law enforcement experts.

*It is important for Records Custodians and Records Managers to understand the general elements of cyber security and to be involved in the development and maintenance of cyber security programs.

At a very high level, Cyber Security programs are encompassing endeavors that integrate:

- Physical Security – agency-wide Policies and Procedures
- Data Encryption - storage/transit/network-wide
- Firewalls - prevent illicit network traffic
- Software - detect and prevent unauthorized access/intrusion
- Back-up - data and records
- Software - updating and patching
- Computer configuration management
- Auditing and testing
- Security Event - Management and reporting
- Security - Policies and Procedures
- Disaster Prevention & Recovery and Continuity of Operations Plan – agency-wide
- Training - On-going agency-wide employee training

Records Custodians should take the time to become acquainted with these program elements and seek to be involved in the development and maintenance of cyber security programs.

Cyber Attack

There are several types of Cyber Attack that Cyber Security programs seek to prevent or mitigate. The following are some of the common types of cyber attack:

Phishing — Phishing attacks, are carefully targeted digital messages to fool people into clicking on a link that can then install malware or expose sensitive data. This technique is becoming more sophisticated and hackers are using more advanced fake messages to lure recipients to unwittingly compromise their organization's networks and systems. Such attacks enable hackers to gain access to databases by stealing user logins, credit card credentials and other types of personal and financial information.

Ransomware — Ransomware attacks can cost its victims billions of dollars every year, as hackers deploy technologies that enable them to literally kidnap an individual or an organization's databases and hold all of the information for ransom - which may or may not ever be released regardless of payment. The rise of cryptocurrencies like Bitcoin is credited with helping fuel ransomware attacks by allowing ransom demands to be paid anonymously.

Cyber-Physical Attacks — The same technology that has enabled us to modernize and computerize critical infrastructure also brings risk. The ongoing threat of hacks targeting electrical grids, transportation systems, water treatment facilities, etc., represent a major vulnerability going forward.

Cyber Attack continued...

Nation State-Sponsored Attacks — Nation states infiltrate other countries to attack their infrastructure for the purposes of: power, control, financial gain, influence public opinion, intelligence gathering, espionage, etc.. Activities have been noted in the regions of: Asia-Pacific, the Middle East and Eastern Europe - notably Syria, India-Pakistan, China, Russia, Iran, North Korea, etc.

Internet Attacks — The Internet is becoming more ubiquitous by the day (the number of devices connected to the Internet is expected to reach almost 31 billion by 2025.). Internet connections are through: laptops and tablets, routers, webcams, household appliances, smart phones and watches, medical devices, manufacturing equipment, transportation systems, automobiles, home security systems, etc. However, this also means greater risks, making Internet networks more vulnerable to cyber invasions and infections.



Cyber Attack continued...

Third Parties (Vendors, Contractors, Partners) — Third parties such as vendors and contractors could unknowingly pose a risk to corporations through their network databases and systems if their security became compromised.

Identity Theft – Safeguards must be taken for the protection of the device and the data within. Key fields of Personal Identifying Information (PII) can be derived from:

- Employee IDs
- Smartphones
- Laptops
- Tablets, etc.



New Jersey Department of Law and Public Safety
Office of the Attorney General

New Jersey State Police

High Tech Crime Bureau

The New Jersey State Police High Tech Crime Bureau is directly responsible for the effective and efficient performance of all investigative and analytical personnel and equipment used in the investigation and apprehension of individuals perpetrating criminal activity through the use of computers and other technology.

Division Headquarters

New Jersey State Police
P.O. Box 7068
West Trenton, NJ 08628
Main: 609-882-2000



STATE OF NEW JERSEY
DEPARTMENT OF LAW & PUBLIC SAFETY
OFFICE OF THE ATTORNEY GENERAL



NEW JERSEY STATE POLICE
HONOR DUTY FIDELITY

————— New Jersey Office of Homeland Security —————
New Jersey Cybersecurity & Communications Integration Cell
(NJCCIC)

Cyber Incident or Data Breach Reporting

Main: 1-833-4-NJCCIC | 24/7

Incident Hotline: 1-866-4-SAFE-NJ

General Inquiries

Call: 1-833-4-NJCCIC

General Inquiries: njccic@cyber.nj.gov

THE
WIZARD of OZ

THE CLASSIC EDITION

Vital Records



by L. Frank Baum * Illustrated by Charles Santore

Vital Records...

VITAL RECORDS are records essential to meet operational responsibilities under emergency and/or disaster conditions. They typically comprise 10% of a public agency's record holdings. Records Custodians need to ask themselves and their colleagues:

“What records are absolutely crucial to our agency's operations and can they be quickly produced from hardcopy, digital/electronic, microfilmed backups or the cloud if the originals are lost in a disaster?”

Conduct a Risk Analysis by evaluating potential hazards to records:

- Natural & Environmental
- Human inflicted
- Facility related

Determine records protection methods:

- Appropriate protection measures
- Measures may vary by type of record
- Inclusive of paper-based, microform and electronic

Identify Vital Records:

- For emergency operations
- To resume normal business
- Comply with Legal and Fiscal obligations





*Disaster Prevention & Recovery and
Continuity of Operations (COOP)*

Disaster Prevention & Recovery and Continuity of Operations

Established emergency procedures and operations are imperative before, during and after a disaster that identify Essential Personnel; Equipment; and Alternate Space in order to resume services to a agency if closing a facility is deemed necessary.

A Disaster Prevention & Recovery Plan

- Mitigates Loss of Records - WATER is the single most significant culprit in a records disaster
- Protects Vital and Historical Records
- Protects Electronic Records, Hardware & Software

A Continuity of Operations (COOP) Plan

- To resume operations safely, quickly & efficiently
- To ensure the normal flow of business



Disaster Prevention & Recovery and COOP continued



THE OBJECTIVE

The object of a Disaster Prevention & Recovery Plan and COOP Plan is to mitigate the amount of damage and associated costs i.e., lost revenue, wages, labor, employee morale, customer goodwill, marketing opportunities; incurred bank fees and legal penalties; and bad publicity from Planned and/or Unplanned Downtime and to protect information and resume information technology services after a disaster.

PLANNED DOWNTIME & UNPLANNED DOWNTIME

PLANNED DOWNTIME: Is scheduled and recognized throughout an agency. Batch-related jobs and IT routine procedures such as hardware and software security, backups, testing, upgrades, installation and de-installation are common and staff are informed and measures are taken to store and protect data and information agency-wide before the activity.

UNPLANNED DOWNTIME: Whether Unintentional or Intentional, the Accidental Access or Release of Information or its Premature, Unauthorized or Inadvertent Disposal, can have serious impact on an agency. Downtime is related to: hardware and/or software malfunction, failure and obsolescence due to lack of proper installation, maintenance and upgrades; internal/external security attack or breach of a system or network; computer viruses; sabotage; cloud data crash and loss; data corruption; power outages; theft; human error; lack of training and tools; security violations and man-made and natural environmental disasters. The consequences of downtime are: financial hardship; lost revenue, wages and labor; low employee morale and customer goodwill; lost marketing opportunities; incurred bank fees and legal penalties; bad publicity; loss of productivity; data and information inaccessibility and/or inaccuracy and the inability to provide real-time, immediate response to constituents.

Disaster Prevention & Recovery and COOP Plan



A Disaster Prevention & Recovery and Continuity of Operations Plan is the key element to a safe and successful continuation of operations in the event of a disaster.

The Plan is to be used in conjunction with an Agency's *Security Standards* – including Guidelines, Policy and Procedures as well as an Agency's *Client Network Installation and De-installation Plan* and the associated Hardware and Software data and supporting documentation. However, before something goes wrong:

ESTABLISH

- A Disaster Prevention & Recovery and Continuity of Operations Plan
- Vendors Lists for: Disaster Recovery Services and Supplies, System Hardware and Software Information and Electronic Disaster Recovery Services
- Disaster Recovery & COOP Team – Management, Records Management, IT, Custodian of Public Record and Local Law Enforcement
- Create an Agency Chain of Command
- Identify Key IT Staff
- Designate Data Center Hot & Cold Site(s)
- Establish an Alternate Operations Site for Staff, IT and Records

IDENTIFY

- Hardware and Software supporting date (manufacturer, models and versions)
- Identify the Agency's Vital Records – Legal, Fiscal, Personnel, Contracts, Plans, etc.
- Potential Recovery Costs associated with Hardware, Software, Supplies, Technology Supplies, etc.
- Retain necessary Emergency Supplies

RETAIN

- Retain copies of the *Disaster Prevention & Recovery and Continuity of Operations Plan* in various safe and accessible offsite locations and with every Disaster Recovery & COOP Team Member.

REVISE

- Test The Plan! Revise The Plan! Re-Test The Plan!

DORES-RMS - Damaged Records Report

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
Mailing: PO Box 661, Trenton, NJ 08625
Location: 33 West State Street 5th Floor, Trenton, NJ 08618

Damaged Records Report

Agency Name: _____
Address: _____
Phone: _____
Email: _____
Contact Person: _____
Date the Damage Occurred: _____
Date the Damage was Discovered: _____

Complete the following.

1. Describe the circumstances

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
PO Box 661, Trenton, NJ 08625

Damaged Records Inventory

Agency Name: _____
Agency Retention Schedule: _____
Retention Schedule Number: _____
Record Series Number: _____
Record Series Name: _____
Retention Time: _____
Inclusive Years: _____
Volume (Cubic Feet): _____
Damage Type: _____
Other copies available? _____

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
PO Box 661, Trenton, NJ 08625

Damaged Records Disposal Certification

TO: State Records Committee
FROM: _____
DATE: _____
SUBJECT: _____

I hereby certify that the records listed on the attached *Request and Authorization for Records Disposal* form(s) have sustained significant damage that warrants their disposal. All attempts to salvage said records have proven unsuccessful or not cost-effective. Subsequently, continued retention of said records has been deemed impractical.

The Future of Information & Technology ???



Department of the Treasury
Division of Revenue and Enterprise Services
Records Management Services



PO Box 661 Trenton, NJ 08625
Phone 609-777-1020

P.S.





Thank you!