

Records & Information Management



Karen Anne Perry
Department of the Treasury
Division of Revenue and Enterprise Services
Records Management Services
2023

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

NJ Public Agencies' Constituency Base

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

Concerns

- Government - Seamless & Efficient
- Government – Trust & Reputation
- Data Fabric – Data Capture, Processing, Management, Delivery & Access
- Data Security – Enhanced Concerns International, National, State & Local
- Regulatory Compliance – International, Federal, State, County & Municipal

Records and Information Management (RIM)

Why Should We Care?

- I. **It's the Law - Data Privacy, Accessibility, Compliance & Security**
 - a. **NJ Public Records Law**
Public Agency records are Public Records and *must be* protected from theft, corruption or *unlawful access*.
 - b. **NJ Open Public Records Act (OPRA)**
OPRA Promotes Public Records - Access, Transparency & Accountability
 - c. **Globalism - International, Federal & State**
 - European Union's *General Data Protection Regulation (GDPR)* & *Regulation EU/2016/679* - privacy and protection for processing of *all personal data*;
 - *US Health Insurance Portability and Accountability Act (HIPAA)* for *all personal medical information*
 - NJ Public Records Laws & *Personal Identifiable Information (PII)* - *SSN, Government ID Number, Credit & Debit Card Numbers, etc.*
 - d. **Litigation & e-Discovery Support**
International, Federal, State and Local

Records and Information Management (RIM)

Why Should We Care?

c. Data Privacy, Compliance & Security Laws

(1.) European Union GDPR & Regulation EU/2016/679

(2.) Federal & State Confidentiality & Security Laws

- SOX = Sarbanes-Oxley Act - Securities & Exchange Commission's (SEC)
- PCI DSS = Payment Card Industry Data Security Standard
- CAN-SPAM = Unwanted Commercial Electronic Messages
- DPPA = Driver's Privacy Protection Act
- HITECH = Health Information Technology for Economic and Clinical Health
- HIPPA = Health Information Portability and Accountability Act
- PCI = Payment Card Industry
- FCRA = Fair Credit Reporting Act
- FACA = Fair and Accurate Credit Transactions Act
- COPPA = Children's Online Privacy Protection Act
- GLBA = Gramm-Leach-Bliley Act
- CCPA = California Consumer Protection Act
- FERPA = Family Educational Rights Privacy Act

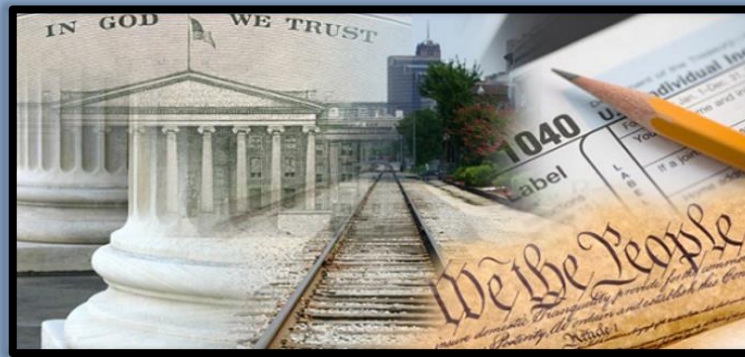
Records and Information Management (RIM)

Why Should We Care?

2. **Compliance: Audit & Program Review**
International, Federal & State
3. **Cost Effective**
Minimize costs and promotes savings, efficiency and productivity.
4. **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 and trust.
5. **Legacy Information**
Irreplaceable loss of intellectual rights, legacy records, etc.

New Jersey Public Records Laws





Public Records: A Public Trust

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.
- 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.

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 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.) which enact the standards and procedures mandated by the Law.
- Agency-specific Statutes and Administrative Rules have impact upon a public agency's records management responsibilities.



Destruction of Public Records Act

PL 1953, c. 410

RMS & The SRC

In accordance with *The Destruction of Public Records Act (PL 1953, c. 410)*, Records Management Services (RMS) is the Government Agency statutorily-entrusted to oversee the governance of New Jersey Public Agency Records. In conjunction, the State Records Committee (SRC) was established and entrusted with having the final authority over the retention and disposition of *all* New Jersey Public Agency Records.

The SRC is comprised of representatives from:

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



Destruction of Public Records Act

PL 1953, c. 410

What is a Public Record? *“New Jersey Style”*

The *Destruction of Public Records Act* (PL 1953, c. 410), defines a Public Record as :

“Information, regardless of its medium (hardcopy, microform, digital, electronic & 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.”

*In New Jersey, "Public" Can Have
Two (2) Meanings*

1. Ownership – As previously stated, a record is Public when it is evidence of the normal course of business of a Public 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 & Security, an agency may restrict access to records:

Ex.: Classified National Defense Records *are* Public Records but due to reasons of National Security – these records are *not* accessible by the Public.

Open Public Records Act (OPRA)

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

The Right to Know Law allowed access to public records in New Jersey. It was replaced by the ***Open Public Records Act (OPRA) PL 2001, c. 404, NJSA 47:1A et seq.*** - which allowed access to records in *most** cases.

- OPRA established the position of Custodian of Public Record for all public agency record-keepers.
- OPRA established Personal Financial & Legal Accountability for the intentional denial of access.
- 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.

***The degree of a record's accessibility does *not* determine whether it 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, issue advisory opinions and mediation/resolution of disputes and issues OPRA information and training for the general public.

Open Public Records Act (OPRA) PL 2001, c. 404, N.J.S.A. 47:1A et seq. – Records Retention

RECORDS RETENTION FOR OPRA-RELATED RECORDS

OPEN PUBLIC RECORDS ACT (OPRA) FILE

Open Public Records Act File contains but is not limited to the following: OPRA Request Form (copy), Denial of Access Complaint, Records Custodian Statement of Information, OPRA Request Extension, OPRA Complaint to the Government Records Council (GRC), Department of Community Affairs, email, correspondence, response documents (copy) and relevant supporting documentation. (PL 2001, c. 404)

- OPEN PUBLIC RECORDS ACT (OPRA) FILE – OPRA Request Form With Fee 7 years/Destroy
- OPEN PUBLIC RECORDS ACT (OPRA) FILE – OPRA Request Form Without Fee 3 years/Destroy
- OPEN PUBLIC RECORDS ACT (OPRA) FILE – OPRA Request Extension (Copy) 3 years /Destroy
- OPEN PUBLIC RECORDS ACT (OPRA) FILE – OPRA Complaint To Government Records Council (GRC) (Copy)
3 years after resolution/Destroy
- OPEN PUBLIC RECORDS ACT (OPRA) FILE – OPRA Litigation/Settlement Agreement File
(Not through the GRC) (N.J.S.A. 2A:14-5) 20 years after final action/Destroy

Government Records Council

“The ‘GRC’ ”



STATE OF NEW JERSEY
GOVERNMENT RECORDS COUNCIL

866-850-0511
Toll Free / GRC Information Line



- Home
- About GRC
- GRC Meetings & OPRA Training Schedule
- GRC Prior Decisions
- OPRA, Advisory Opinions & Other Laws
- OPRA for the Public
- Register a Denial of Access Complaint
- OPRA for Records Custodians
- GRC Mediation
- OPRA Inquiries, GRC News Service & OPRA ALERTS



[NJ OPRA Central](#) | [Local Government](#) | [K-12 Schools](#) | [Higher Education](#)

Address: Government Records Council/PO Box 819/Trenton, NJ 08625-0819

Phone: 609-292-6830/1- 866-850-0511

Email: Government.Records@dca.nj.gov

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



**Records Management Tools to Help
Improve Your OPRA Program**

- **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
MANAGEMENT
SERVICES

Spoliation: noun

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

Spoliation

Records and Information Management
Litigation Hold Order



Litigation Hold Order

As Public Servants, we have an obligation to preserve the Public Records in our custody – regardless of their medium.

In the event of an OPRA Request or potential Litigation, a *Litigation Hold Order* must be issued and all relevant Hardcopy, Digital and Electronic Information should be immediately segregated and stored.

[NOTE: Attention must be given to e-mail, because their automated processes may have a function that routinely deletes e-mail if no action is taken. To avoid this, relevant e-mails should be placed in a separate folder.]

- A *Notice of Acknowledgement* should be distributed to the specific agencies indicating that they have been notified of the *Litigation Hold Order*.
- The *Acknowledgement of Receipt* is to be signed and returned to the sender within five (5) days and immediate action should be taken in accordance with the directives to segregate the associated records.

Litigation Hold Order

"Litigation Hold Order"

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

"Acknowledgement of Receipt"

For Discussion Purposes Only

Consult With Legal Advisors When Dealing With Litigation Hold Orders

SAMPLE

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

Name

Date

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.

Audit:

Federal, State, Local, In-House & Private



Audit: Federal, State, Local, In-House & Private BRIEFLY DEFINED

Audit: (Federal, NJ Office of the State Auditor, Local, In-House or Private) conducted to review the status of an agency's financial records and prevent financial fraud or other unethical/ illegal financial practices.

- **Objective: Transparency** - Financial Records Governance to prevent:
 - Accounting recordkeeping and reporting errors,
 - Financial Fraud and,
 - Unethical/illegal financial practices.

- **Penalties** - The unlawful and deliberate alteration, destruction of falsifying records:
 - Fines up to the Millions of Dollars and possible criminal conviction.

- **Record Retention** - Electronic, Digital, Hardcopy and Cloud Storage:
 - Financial Records Retentions vary depending on the individual record series and the laws and associated statutes. They may vary between Permanent, 7 years, 5 years, 3 years, 1 year, etc.
 - Conditions linked to retention are: after audit, end of fiscal period, etc.
 - Public Records commonly associated with an audit include: financial disclosure statements, work papers, financial statements, memoranda, correspondence, communications etc.

- **IT Security** – Prevent data breaches:
 - **Access** - Physical and electronic controls to prevent unauthorized access.
 - **Data Backup** – Backup and migration systems to protect sensitive data onsite and offsite.
 - **Change management** - Document new employee access, hardware, software, database updates; infrastructure changes; etc.

Audit RECAP

EXTERNAL & INTERNAL AUDITS

- Implement Monitoring Controls to aid in efficient, accountable & transparent recordkeeping for a Federal, State, Local, In-House & Private Audit(s).
- Identify the records required to uphold Federal and State Financial Compliance Mandates, Statutes, Codes, etc.
- List the retention periods for the records.
- Ensure safe document (hardcopy, electronic & digital) storage for the records.
- Implement an agency-wide records management program and ongoing training.

Records and Information Management

Records Retention & Disposal



Records Retention

PL 1953, c. 410/NJSA 47

Records Management Services (RMS): is the Government Agency statutorily-entrusted with the creation of *Records Retention Schedules* and authorizing *Request and Authorization for Records Disposals* for **EXPIRED*** Public Records.

Records Retention Schedules: In accordance with the New Jersey Public Records Laws PL 1953, c. 410 & NJSA 47, Records Retention Schedules must be created for the records maintained by a public agency, noting the **MINIMUM** Legal and Fiscal time periods the records must be retained.

***Unless in Litigation, e-Discovery, Audit or OPRA, then the retention time period is not applicable until after final settlement or resolution.**

Records Retention Schedules

Records Retention Schedules creation and maintenance for all New Jersey Public Agencies was mandated in accordance with:

- ❖ New Jersey Public Records Laws PL 1953, c. 410
- ❖ NJ Statutes Annotated Title 47 et. seq.

Records Retention Schedules address the following areas:

- ❖ Vital
- ❖ Legal, Fiscal & Administrative
- ❖ Historical
- ❖ Confidential
- ❖ Retention Period
- ❖ Final Disposition

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	

Records Disposition

PL 1953, c. 410/NJSA 47

In accordance with PL 1953, c. 410/NJSA 47, a Public Agency must obtain prior authorization from DORES-RMS to legally dispose of the Public Records in their custody whose retention periods have **EXPIRED**.

This is accomplished by the online creation and submission of a “*Request and Authorization for Records Disposal*” in Artemis.

NOTE: It is imperative that all **HARDCOPY** 4-Part “*Request and Authorization for Records Disposal*” forms (Ex., “Agency ‘PINK’ Copy”) **prior to Artemis**, be kept **PERMANENTLY** in the event of present & future OPRA Requests, Litigation, Audits, etc.



**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 view the status (Pending, Approved & Denied) to legally dispose of their records
- **Produce** - Authorized Records Disposal Requests for OPRA, Audits & Litigation
- **Generate** – Reports pertaining to Records Retention & Disposal

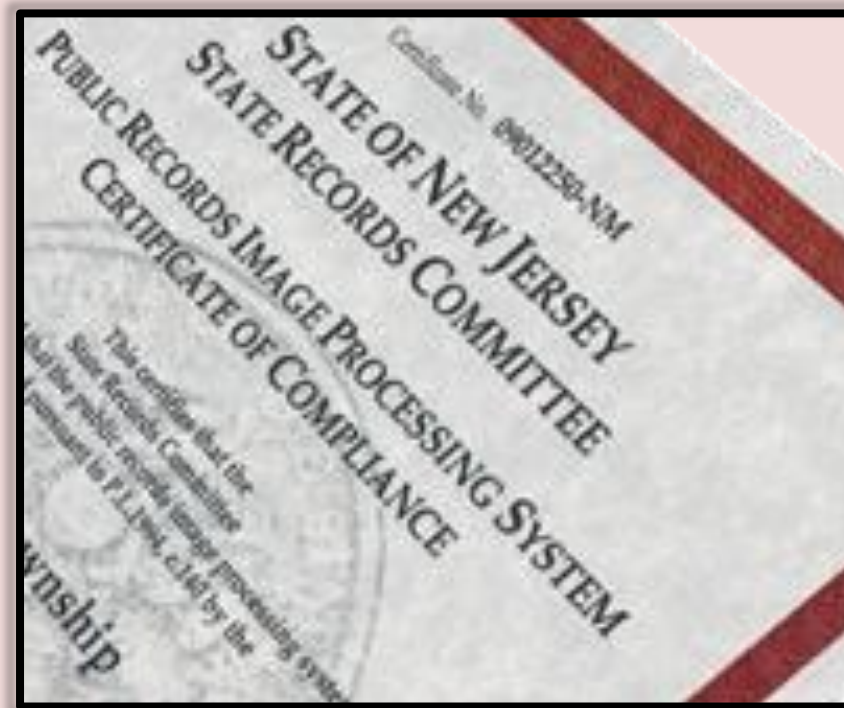
Artemis-Generated "Request and Authorization for Records Disposal"

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 609.630.7404.		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) <i>Karen A. Perry</i>	4. Request Approved By (Electronically Signed by) <i>Elizabeth Hartmann</i>	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		13. Dispose After	14. Volume (in Cubic Feet)
				From (MM/YYYY)	To (MM/YYYY)		
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> (CAK)	16.A Authorization Date	16.B Authorization Number		
15.B Date	16.C Authorizing Signature, Records Management Services <i>L. V. [Signature]</i>		17.A Verification Signature	17.B Date

Records and Information Management Alternatives – Image Processing



Records and Information Management Alternatives –

Image Processing System Certification



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-Set seq.) BEFORE completing this application, please read the [Instructions](#).

AGENCY NAME: _____

This is an application for:

- In-house Imaging System
- Service Bureau Imaging
- Special Document Imaging Services (DORES services)


APPLICATION PACKAGE CHECKLIST (PLEASE INCLUDE ALL THAT APPLY IN YOUR PACKAGE)

<input type="checkbox"/> Review Form	<input type="checkbox"/> Imaged Records Series List
<input type="checkbox"/> Feasibility Study and or RFP/RFI/RFB (if applicable)	<input type="checkbox"/> Microfilm Inspection Report (if applicable)
<input type="checkbox"/> Data Migration Report (replacement systems)	<input type="checkbox"/> Data Migration Statement (all applications)

Registration No. «Certification_»

**STATE OF NEW JERSEY
STATE RECORDS COMMITTEE**

**PUBLIC RECORDS IMAGE PROCESSING SYSTEM
CERTIFICATE OF REGISTRATION**



Assistant Director
Division of Revenue and Enterprise Services-RMS

«Certification_Date»

Records and Information Management Alternatives – Image Processing System Registration Application

As per PL 1994, c. 140, the State of New Jersey allows for the replacement of hardcopy public records with digital and microform images (e.g., Optical Disk, CD, DVD, Magnetic Tape & Microfilm).

The State Records Committee and Records Management Services issues Initial and Imaging System Certifications to an Agency for an in-house or outsourced, **Non-Proprietary** imaging application. Documents required for obtaining an Initial 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

The image shows a registration application form for an image processing system. It includes the state seal, the title 'IMAGE PROCESSING SYSTEM REGISTRATION APPLICATION', and a checklist of required documents. The form is titled 'IMAGE PROCESSING SYSTEM REGISTRATION APPLICATION' and includes the following text: 'State of New Jersey, Division of Revenue and Enterprise Services (DORES), Records Management Services - RMS'. Below the title, it says '(N.J.A.C. 15:3-5et seq.) BEFORE completing this application, please read the [Instructions](#).' The form has a section for 'AGENCY NAME:' with a light blue background. Below that, it asks 'This is an application for:' and lists three options: 'In-house Imaging System', 'Service Bureau Imaging', and 'Special Document Imaging Services (DORES services)'. At the bottom, there is an 'APPLICATION PACKAGE CHECKLIST (PLEASE INCLUDE ALL THAT APPLY IN YOUR PACKAGE)' with a table of checkboxes and labels.

APPLICATION PACKAGE CHECKLIST (PLEASE INCLUDE ALL THAT APPLY IN YOUR PACKAGE)	
<input type="checkbox"/> Review Form	<input type="checkbox"/> Imaged Records Series List
<input type="checkbox"/> Feasibility Study and or RFP/RFI/RFB (if applicable)	<input type="checkbox"/> Microfilm Inspection Report (if applicable)
<input type="checkbox"/> Data Migration Report (replacement systems)	<input type="checkbox"/> Data Migration Statement (all applications)

Image Processing System Certificate of Registration

Registration No. 22110901-MP

STATE OF NEW JERSEY STATE RECORDS COMMITTEE

PUBLIC RECORDS IMAGE PROCESSING SYSTEM CERTIFICATE OF REGISTRATION

This certifies that Records
Management Services
has determined that the public records image processing system
submitted pursuant to P.L.1994, c.140 by the

Township of _____

is in compliance with all specifications and standards as set forth in
N.J.A.C. 15:3-4, Image Processing of Public Records
and has met the requirements for registration set forth in
N.J.A.C. 15:3-5, Registration of Image Processing Systems
and has therefore authorized the issuance of this
Registration of Compliance.

This registration has a migration path component,
Therefore it is understood that the aforementioned agency
may destroy all short term, long term and non-historical permanent
original records after image processing.

Division of Revenue and Enterprise Services-RMS

09 November 2022

Image Processing System Certification Letter



State of New Jersey

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
P. O. BOX 661
TRENTON, NEW JERSEY 08625-0661

PHILIP D. MURPHY
Governor

ELIZABETH MAHER ~~MUNOZ~~
State Treasurer

SHEILA Y. OLIVER
Lt. Governor

JAMES J. FRUSCIONE
Director

9 November 2022

Clerk
City of Brigantine
1417 West Brigantine Avenue
Brigantine, New Jersey 08203

Dear

This is to verify that the public records image processing system for the City of Brigantine was registered by the Records Management Services (RMS) on 09 November 2022, Registration Number 22110905-MP and is in compliance with the standards, procedures and guidelines adopted under N.J.A.C. 15:3-4, *Image Processing for Public Records*. This registration should be retained permanently by your agency, and a copy of it should accompany any future disposal requests for destruction of original records maintained on this system, pursuant to N.J.S.A. 47:3-17. Your agency must submit appropriate documentation to request destruction of the imaged records at such time as the record's lifecycle has expired.

Your system will be due for an annual review and renewal of registration per N.J.A.C. 15:3-5.6 on 1 October 2023.

Sincerely,

Division of Revenue and Enterprise Services-RMS

c: file

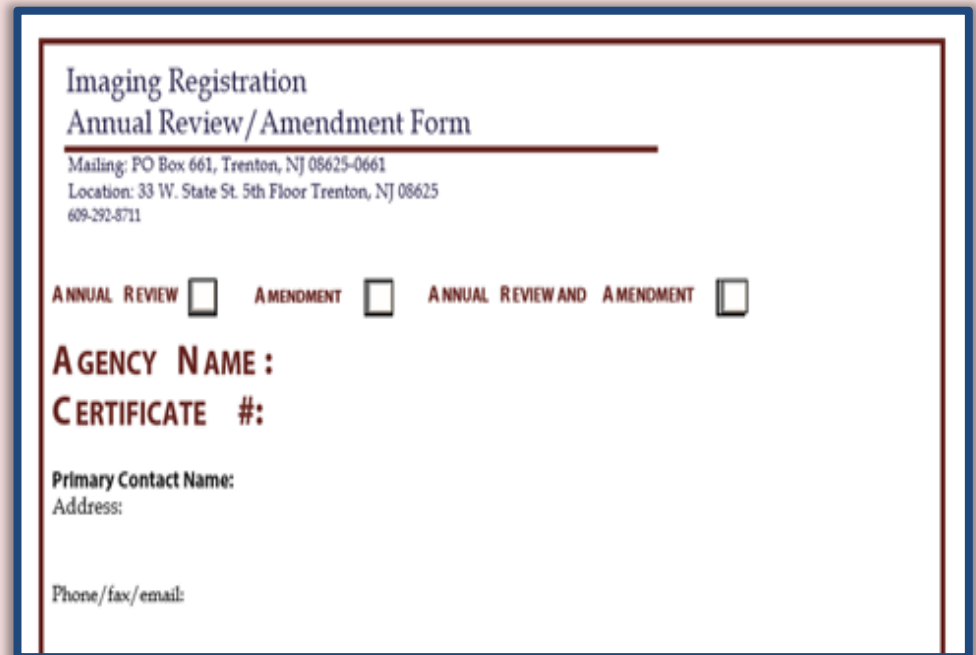
Records and Information Management Alternatives – Image Processing System Certification Annual Renewal/ Amendment Application

The State Records Committee and Records Management Services issues Annual Renewal Imaging System Certifications to an Agency for an in-house or outsourced, **non-proprietary** imaging application.

Documents required for obtaining an Annual Renewal Imaging Certification from the State Records Committee and Records Management Services include:

➤ Annual Review/Amendment

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



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 AND AMENDMENT

AGENCY NAME :
CERTIFICATE #:

Primary Contact Name:
Address:

Phone/fax/email:

Image Processing System Annual Renewal/Amendment

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 AND AMENDMENT

AGENCY NAME :

CERTIFICATE #:

Primary Contact Name:
Address:

Phone/fax/email:

Custodian of Records Name:
Address:

Phone/fax/email:

Preferred Annual Review Date (choose 1):

January 1 April 1 July 1 October 1

Do you want to make this the annual review date for all certified systems in your agency?

Yes No

If yes, please list other certified systems:

1. Has your agency added additional records series or inclusive years to your imaging system?

Yes No

All Agencies must submit the Imaged Records Series List for each retention schedule/office whose records are scanned into this system

Imaged Records Series List(s) attached

2. Has your agency added to or upgraded the hardware and/or software for your image processing system?

Yes No (If yes, attach appropriate documentation.)

Image Processing System Annual Renewal/Amendment

3. Has your agency updated your Disaster Prevention/Recovery Plan?

Yes No (If yes, attach appropriate documentation.)

4. Microfilm Inspection Microfilm Inspection Report attached

- a. Our agency has not produced any microfilm since our last annual review
b. Our agency has its microfilm produced or processed by DORES
c. Our agency produces its own microfilm or has its microfilm produced by a vendor.

If you checked c, you must submit a reel of microfilm for each size produced for inspection BEFORE submitting an Annual Review / Amendment. This reel should be an original silver halide production copy, NOT a sample. Microfilm must be accompanied by a completed Microfilm Submission Form. Microfilm will be returned to the agency. A passing Microfilm inspection must accompany this Annual Review / Amendment Form.

5. Has your agency changed vendors? This includes vendors for: imaging services, micrographics, hardware or software, maintenance.

Yes No (If yes, attach appropriate documentation, including the names of the old and new vendors and contact information)

6. Does your agency want to implement a migration path for long term records if you have not already?

Yes No (If yes, attach appropriate documentation.)

AGENCY VERIFICATION :

I hereby certify that the documentation listed on and/or attached to this **Image Processing System Annual Review/Amendment Form** is a true and an accurate reflection of the agency's image processing system upon this date and is submitted in compliance with N.J.A.C.15:3-5.6.

Legal Custodian: Print Name

Signature:

Date

For questions or further assistance, contact your agency Records Analyst.

Submit by Email

Attach Documentation

Records and Information Management Alternatives – Image Processing System Certification Letter of Annual Renewal



State of New Jersey
DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND
ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
P.O. BOX 661
TRENTON, NJ 08625-0661

PHILIP D. MURPHY
Governor
SHEILA Y. OLIVER
Lt. Governor

ELIZABETH MAHER MUOIO
State Treasurer
JAMES A.FRUSCIONE
Director

21 June 2022

[Name] _____
NJ Department of Transportation
1305 Parkway Avenue
Ewing NJ 08625

Dear [Name] _____

This is to verify that the annual renewal/amendment for the registered Public Records Image Processing System (#01092001) for public records of NJ Department of Transportation has been determined by the staff of the Department of Treasury Division of Revenue and Enterprise Services, Records Management Services to be in compliance with the standards, procedures and guidelines adopted under *N.J.A.C. 15:3-4, Image Processing for Public Records*.

The destruction of original records must adhere to the procedures mandated by State Statutes per *N.J.S.A. 47:3-15 to 30*, including the submission of a "Request and Authorization for Records Disposal" form accompanied by a copy of the "Certificate of Registration."

Regulations allow an agency to choose their annual review date from the following dates, January 1, April 1, July 1 and October 1. We have temporally assigned you a new date. *Your next annual review will be due, July 1, 2023*. If you would rather have one of the other dates, please let us know as soon as possible.

Respectfully,

Liz Hartmann
Liz Hartmann

Image Processing System Guidelines

Image Processing System Guidelines

Mailing: PO Box 661, Trenton, NJ 08625-0661
Location: 2300 Stuyvesant Avenue, Trenton, NJ 08625
609-530-3200



The following guidelines have been developed to assist public entities that are currently using or considering the acquisition of an electronic imaging system for storage and retrieval of public records:

- **Establish and routinely audit comprehensive records management guidelines:**
...for paper, microfilm/fiche, and image-processed records through use of state- issued records retention schedules and records disposition forms, and consult with the Division of Revenue and Enterprise Services, Records Management Services (RMS) for guidance when questions arise.
- **Form a team of agency representatives:**
...that will review and select the system. This team should be comprised of users, finance, MIS, and legal representatives. Review the key resources existing within the agency - staff knowledge and expertise, and existing in-house data and telecommunications systems.
- **Consult State standards:**
...Image Processing for Public Records (NJAC 15:3-4 et seq.) before preparing specifications for an RFQ, RFI, or RFP for any new system or upgrade.
- **Consult RMS:**
... before preparing specifications for an RFQ, RFI, or RFP for any new system or upgrade.
- **Conduct a feasibility study:**
...to determine if an imaging system will be appropriate and cost-effective for your records management needs. Maybe another system would provide a better alternative or could be employed alongside an imaging system (e.g. microfilming or COM).
- **Set realistic timelines:**
...for the following project phases: feasibility study; vendor bidding; system selection, implementation, testing, and conversion; training; backfile document scanning; and production.

Image Processing System Guidelines continued

- **Be wary:**
...of claims regarding new technologies without track records or standards. RMS can provide guidance in the evaluation of such claims.
- **Determine system compatibility:**
...with existing in-house records and information management systems. Identify any agency-specific recordkeeping needs to be incorporated into an imaging system.
- **Ensure that system hardware and software are applicable:**
...for the in-house applications they will automate. The system should serve the agency and its applications, and not have the agency serving the system.
- **Plan for data migration:**
...during the initial stage of development, for system hardware and software upgrades which should incorporate the creation of a history file which includes copies of old and new versions of system hardware and software documentation (see NJAC 15:3-4.3,4.7).
- **Ensure that the system has an open architecture:**
...with nonproprietary dependent hardware and software (see NJAC 15:3-4.3).
- **Use high-quality hardware and software:**
...for your entire imaging system (see NJAC 15:3-4.3).
- **Create a data index:**
...data is useless if it cannot be searched and accessed through user specified parameters (see NJAC 15:3-4.7). The index *at a minimum must* recreate the functionality of the existing records management system.
- **Specify security measures:**
...desired with the vendor during initial system discussions.
- **Permanent and long-term records (retentions of 10 years or longer):**
...maintained on optical media may require hardcopy, microfilm backup, or have a documented path to migrate (see NJAC 15:3-4.3).
- **Develop and implement:**
...routine magnetic tape refreshing and optical media backup procedures (see NJAC 15:3-4.3, 4.4).
- **Create and periodically test disaster prevention/recovery plans:**
... for storage media, hardware, and software (see NJAC 15:3-4.4).

Image Processing System RFP Concerns

Image Processing System RFP Concerns

Mailing: PO Box 661, Trenton, NJ 08625-0661
Location: 2300 Stuyvesant Avenue, Trenton, NJ 08625
609-530-3200



The following are areas on concern that an agency should consider when developing a Request for Proposal (RFP) for an Image Processing System or Image Processing Services.

Scanner Information/Requirements:

- o Does the scanner(s) allow for imaging at the following resolutions?
 - 200dpi required for small format documents (e.g. correspondence and forms)
 - 300dpi required for large format documents (e.g. engineering drawings)
- o What type of scanner does your agency need?
 - Flatbed
 - Auto Document Feed
 - Medium Speed
 - High Speed
 - Large Format

Image Capture Software:

- o Does the capture software save the images using industry standard file formats?
 - Single-page TIFF, PNG, PDF/A, ODA/ODIF
- o Does it have OCR and/or zonal OCR capabilities?
- o Does it include redacting tools?
- o Does the system produce Scanning Logs?
- o Does the system produce hardware/software logs?

Database/Retrieval Software:

- o What kind of storage database would be used?
 - SQL Server, Oracle, Access, etc.
- o Does it have an Open Architecture at the Application Programming Interface (API) level?
- o Will your agency be storing images on-line, near-line, or off-line?
- o What type of security/levels of access does the system have?
- o What type of retrieval software will be used?
- o Does it have an Open Architecture at the Application Programming Interface (API) level?
- o Is the system web-enabled?
- o Indexing should include at a minimum the identical indexing access as the existing records management system.

NOTE:

PDF/A is an
Acceptable Format -
PDF is **NOT**.

Image Processing System RFP Concerns continued

Image Processing System RFP Concerns



Mailing: PO Box 661, Trenton, NJ 08625-0661
Location: 2300 Stuyvesant Avenue, Trenton, NJ 08625
609-530-3200

- o Does the system produce hardware/software logs?
- o Does the system require a dedicated server?

Backup:

- o Operating System must be backed up.
- o Database must be backed up.
- o Does system create a bootable backup?
- o What media will be used to backup?
 - Optical Disk (WORM)
 - CD
 - DVD
 - Magnetic Tape
 - Microfilm
 - o Does the vendor have a solution that will allow the agency to create microfilm from the images?
 - o Can the vendor provide this service as a service bureau?
- o Can the vendor provide offsite storage of the paper records, digital records, or microfilmed records that is in compliance with State record storage standards?
- o Can the vendor supply a Hot/Cold site?
- o Does the vendor have a documented migration path to guard against the risk of records loss due to the obsolescence of underlying technology?

Support:

- o Provides Training and Technical Support
- o Provide Operational and Administrative Manuals for users
- o Provides periodic upgrades and updated versions of system
- o What tools are available for support?
- o Do you provide hardware maintenance?
- o Company Information
 - Where are you located?
 - Do you have local representation?
 - How long have you been in business?
 - Would you be able to provide us with financial information regarding your company?
- o Have you done work for State, Federal, or municipal/local agencies?
- o Are you aware of State laws regarding the imaging of public records and the associated standards and certification process promulgated and coordinated by the Division of Archives and Records Management?
- o What type of assistance in the certification process can you provide?

Image Processing System RFP Concerns continued

Image Processing System RFP Concerns



Mailing: PO Box 661, Trenton, NJ 08625-0661
Location: 2300 Stuyvesant Avenue, Trenton, NJ 08625
609-530-3200

- o Does the system produce hardware/software logs?
- o Does the system require a dedicated server?

Backup:

- o Operating System must be backed up.
- o Database must be backed up.
- o Does system create a bootable backup?
- o What media will be used to backup?
 - Optical Disk (WORM)
 - CD

NOTE: Original Minutes, Resolutions & Ordinances can be Imaged, however their ORIGINAL HARDCOPY source document(s) cannot be destroyed – the hardcopy, original documents must be maintained Permanently.

- o Do you provide hardware maintenance?
- o Company Information
 - Where are you located?
 - Do you have local representation?
 - How long have you been in business?
 - Would you be able to provide us with financial information regarding your company?
- o Have you done work for State, Federal, or municipal/local agencies?
- o Are you aware of State laws regarding the imaging of public records and the associated standards and certification process promulgated and coordinated by the Division of Archives and Records Management?
- o What type of assistance in the certification process can you provide?

Image Processing System Guidelines

When Contracting a Vendor

1. Ensure it is understood that hardcopy & imaged records are Public Records and belong to the Public Agency.
 2. Ensure that the stored records are classified in accordance with their records retention schedules.
 3. Require security controls to prevent unauthorized records access, manipulation, defacement or destruction.
 4. Be aware of storage and backup locations restrictions.
 5. Prohibit the Vendor from destroying or image records unless the agency specifically directs the action.
 6. Require the Vendor to document changes in their format/programming that may affect records access.
 7. Specify records transfer requirements for contract-exit processes.
 8. Ensure records are retrievable and accessible in response to OPRA Requests, Audits, Subpoenas, Investigations, e-Discovery, Litigation Holds and Litigation.
-

Records and Information Management – 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 and/or electronic.

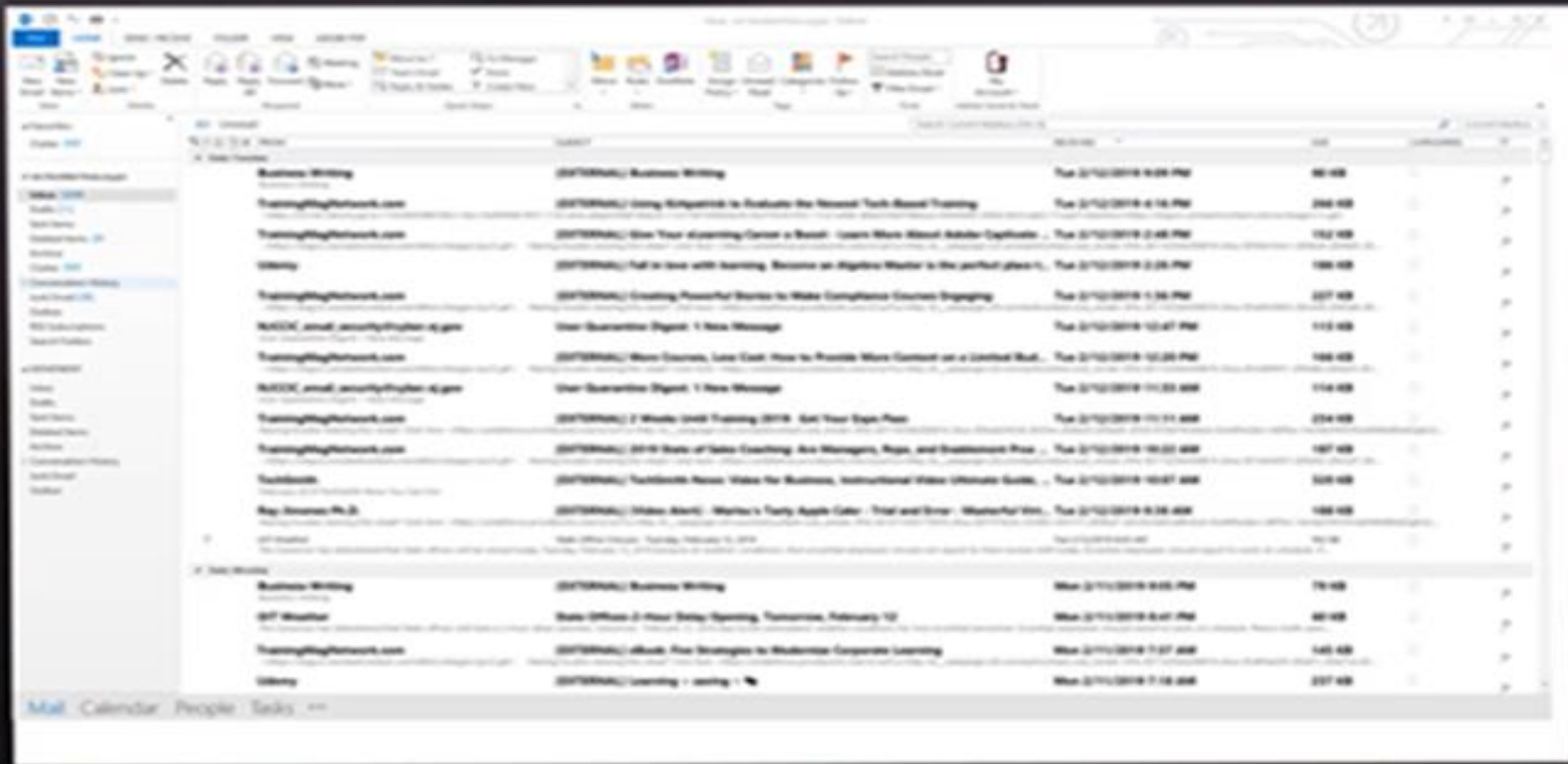
Records and Information Management professionals should work across disciplinary lines to protect these records:

- **Auditors**
- **Procurement Professionals**
- **Legal Advisors**
- **Information Technology Staff**
- **Information/Internal Security Staff**
- **Agency Managers**
- **Records Management Liaisons**
- **Risk Management Professionals**

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

When Storing in the Cloud

1. Make it clear to the Contractor that records stored in the Cloud Facility are Public Records and belong to the Public Agency.
2. Ensure that the Cloud Storage Facility classifies and stores the records in accordance with their associated retention schedules.
3. Require security controls to prevent unauthorized access, manipulation, distribution, defacement & destruction of the records.
4. Be aware of storage location restrictions.
5. Monitor the life-cycle of records stored in the Cloud – creation, storage, access, storage or legal destruction.
6. Prohibit the Contractor from deleting/destroying Cloud-based records unless the Agency specifically directs the action.
7. Require Contractors to document any changes in their format or programming that affect the access and use of stored records.
8. Specify records transfer requirements for the Contract-Exit process.
9. Ensure records are quickly retrievable in response to OPRA Requests, Audits, Subpoenas, Investigations, Litigation, etc.



Email.....

Email

Email

noun

\ 'ē- māl \

variants: **e-mail**

Definition

1: a means or system for transmitting messages electronically (as between computers on a network) communicating by *email*

2a: messages sent and received electronically through an email system

bplural emails or e-mails

3: a system for sending messages from one individual to another via telecommunications links between computers or terminals.

4: a message sent by email

verb

variants: *or* **e-mail**

emailed *or* **e-mailed**; **emailing** *or* **e-mailing**; **emails** *or* **e-mails**

(transitive verb)

1: to send email to (someone)

2: to send (something) by email

3: to send a message by email

intransitive verb

: to communicate by 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, Posts, Chats, etc.

..... *Email*

Email continued...

Remember...

- Email is a Public Record.
- Email is Discoverable.
- Email may be Accessed under OPRA.
- Email may be Accessed under an Audit.
- 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 authorization from DORES-RMS.

Email Management

- Consult the General Schedule for the general 7-year retention period regarding the Retention and Disposition of Email. This applies to hardcopy, email (tracking, indexing and archiving software) and electronic business records, audit and review documents, memos, correspondence, financial statements, etc.
- 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” and Compliance Audits.
- 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 tracking, indexing archiving, access, retention and disposition of Email records in the Email Central Storage/Management System.

Records and Information Management – Social Media



Social Media

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

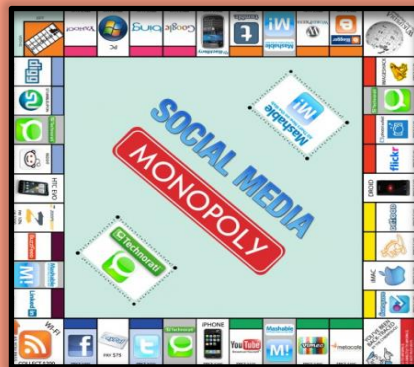
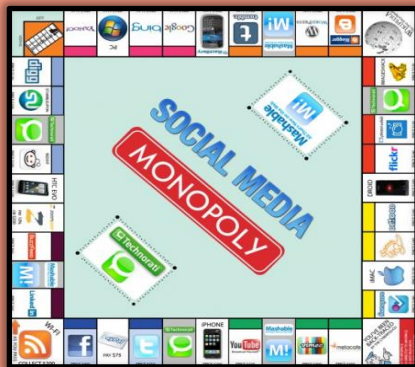
- Social Media Is - Global, Immediate and Very Accessible!
- Social Media Is - Not Private.
- Social Media Is - Public and in the event of e-Discovery, Litigation and Legal Rules of Evidence, directives should be established regarding content, language, subject matter, which includes: Instant messaging, blogs, Wikis, Pod casts, Metadata, TEAMS, OneDrive, SharePoint and Email regarding – Operational Records, Meetings, Events, Chats & Recordings)
- 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 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 DORES-RMS' Records Retention Schedules.
4. Choose Secure Modes of Storage for Social Media Records
5. Implement the Retention and Disposition Program

Records and Information Management – The Internet



The Internet

- The Internet is how a Government Agencies and Private Sector interact and inter-connect with other (such as, Finance, Healthcare, Education, etc.) in a World-wide Information Community, aka. – **the Internet of Things (IoT)**.
- Due to its ever-changing content & structure, an agency's website documentation should be maintained as it reflects hardware, software, metadata, content and the following 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 Federal, State or Local Audit.
- **Records Management & Access Perspective** - verify retention & disposition in the event of an OPRA Request.

The Internet

Records associated with website development and maintenance include:

- Agency Website/Internet Access Log – *Internal and External Users*
- Agency Website Creation and Update File – Content
- Agency Website Creation and Update File - Operation
Contains: graphic files, source code, operation and application software documents, user logs, statistical data, records verifying copyrighted documentation, website governance policies and procedures, input documents, testing reports, screen copies and supporting documentation.
- Agency Website Creation and Update File – Structure
Contains: website diagnostics, website mapping data, source code, testing reports, screen copies, configuration data and supporting documentation.
- Upon the revision or discontinuance of the website, for preservation purposes it is advised that hardcopy be maintained for agency-generated and supported documents that were solely created and maintained in an electronic format.



Records and Information Management – Data Security



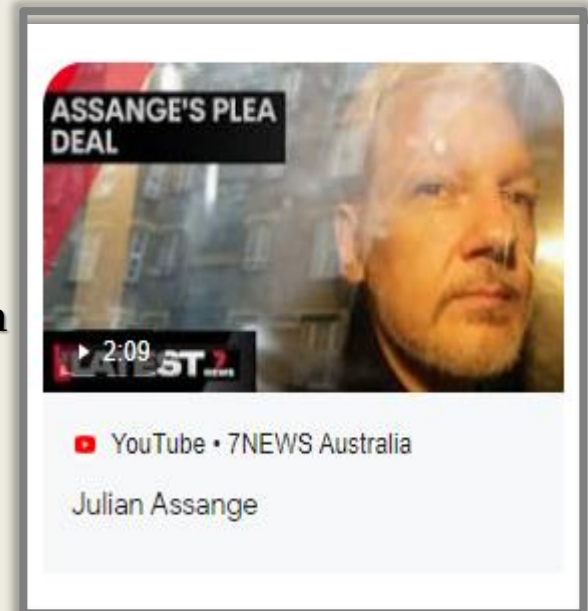
Data Security – Is it ever really secure???

In their *daily, normal course of business*, Government Agencies use Information Technology, Networking, Mobile Computing, Telecommunications, Email, the Cloud and Social Media to send and receive data and information.

While this creates Data/Information Processing & Operational Efficiencies, it can also create the potential for Overlapping Internal & External Operational Single Threat & Multiple Threat Groups that can:



- 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

Global Target Areas

- *Government & Military*
- *Business*
- *Financial Institutions*
- *High Tech*
- *Healthcare & Medical*
- *Retail & Manufacturing*
- *Hospitality*
- *Entertainment & Media*
- *Construction & Engineers*
- *Telecommunications*
- *Transportation & Logistics*
- *Education*
- *Energy & Utilities*
- *Nonprofit*

Data Security ...

To mitigate internal and external operational threats, Data Security should be approached as an Enterprise-wide collaborative effort with an Agency's IT Department working in coordination with Legal, Records Management*, Human Resources and Law Enforcement. However, like any other "risk" an agency must face – it should be with unified Governance and Accountability - that starts from the top down.

Data Security Programs should integrate:

- **Acceptable Use Policy** – Document read & signed by all employees re: Agency computer usage.
- **Physical Security** – Enterprise-wide Policies and Procedures
- **Data Encryption** - Storage/transit/network-wide - (NJ “Real ID” Drivers License)
- **Passwords** - Strong passwords, routinely change them, Multi-Factor Authentication
- **Firewalls/Spam Filters** - Prevent illicit network traffic
- **Software** -Antivirus/Antimalware update, detect & prevent unauthorized access/intrusion & minimize Dwell Time
- **Back-up** - Data and records
- **Software** - Routine updating and patching
- **Computer** - Configuration management
- **Auditing** - Audit and test
- **Security Event** - Management and reporting
- **Security** - Policies and Procedures
- **Training** - On-going agency-wide employee training
- **Disaster Prevention & Recovery & Continuity of Operations Plan** – Enterprise-wide

***Records Custodians** should take the time to become acquainted with these program elements and seek to be involved in the development and maintenance of Agency-wide Cyber Security Programs.

Cyber Attack: ZERO Trust!

Zero Trust is a Cyber Security strategy employed to prevent Cyber Attack – a user or a device is *never* trusted to have access to the network until its identify and authorization have been thoroughly verified.

These Attacks may be a single or group attack, a one-time or a repeated attack for Financial Gain, Espionage, Sabotage, Fraud, Influence, Notoriety, etc. The following are some of the common types of Cyber Attack:



Phishing, Spearphishing, Smishing, Vishing, Whaling — Phishing Attacks, are carefully targeted digital messages to fool people into clicking on a link that can then install malware or expose sensitive data also referred to as Social Engineering. 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/Scareware — Ransomware attacks by means of fear and extortion, 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.

Malware & Wiper Malware Families — “Malicious Software” designed but not limited to: damage/destroy, launch, reconfigure, tunnel, steal data, erase (aka, “Wiper”), and overwrite (aka, “SwiftSlicer”) data, software and programs from a hard drive. It is opportunistic, bent on financial gain, notoriety, sabotage, espionage, etc.

Cyber Attack continued...

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.

Nation State-Sponsored Cyber-Security Wars and 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:

Americas - North & South ● Asia-Pacific (APAC) ● Europe-Middle East-Africa (EMA)

Third-Party - Vendors or Contractors — Third-Party Contractor or Vendors who have direct access to people, facilities, networks and/or systems could unknowingly pose a risk to an agency. In addition, they could pose a threat through their network databases and systems if their security became compromised.

Identity Theft & Stolen Devices/Credentials – Personal Identifying Information (PII) can be derived from: Employee IDs, Smartphones, Laptops, Tablets, etc. which include Personal, Medical and Financial data which are targets for extortion for financial gain.

“Exploit” & Prior Compromise - Code or a Program that can target and infiltrate compromised areas in hardware and/or software and vehemently, repeatedly attack. **NOTE:** The use of PoC Code (Proof of Concept Code) is used to detect software security flaws during an exploit. PoC can also be employed to simulate attacks to identify vulnerabilities and threat level.

Cyber Attack continued...

SIM Swap Attacks — A SIM Swap (also known as SIM Swap Scam, Port-out Scam, SIM Splitting, Smishing, Simjacking, SIM Swapping) is an Account Takeover (ATO) that targets a weakness in Multi-Factor Authentication on a mobile telephone.

Or the actual theft of a Mobile Phone with the SIM Card being swapped to login and access data and information which leads to Identity Theft.



————— 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

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

Records and Information Management –
Vital Records

In New Jersey, "Vital Records" Can Have Three (3) Meanings

1. Life-Related – Records of Life Events maintained by a Public Agency.
2. Medical – Recorded data imperative to maintain life.
3. Operational – **VITAL RECORDS** are the records (hardcopy, microform, digital, electronic & Internet-based) that are Essential to document responsibilities:
 - a.) Under Emergency and/or Disaster Conditions and
 - b.) Prove Legal Ownership.

Vital Records...

VITAL RECORDS are records essential to meet operational responsibilities under Emergency and/or Disaster conditions. They typically comprise **10%** of an agency's record holdings.

Records Custodians must ask themselves and their colleagues:

“what records are absolutely VITAL to operations, and can they be quickly reproduced (from hardcopy, digital/electronic, microfilm or the cloud) if the originals are destroyed in a disaster?”

Conduct a Risk Analysis - Evaluate Potential Records Hazards:

- 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 & electronic

Identify Vital Records:

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

Records and Information Management –

Disaster Prevention & Recovery, Business Continuity of Operations (COOP) & Cybersecurity Incident Response & Vital Records Plans

Disaster Prevention & Recovery, Business Continuity of Operations (COOP), Cybersecurity Incident Response & Vital Records Plans

THE OBJECTIVE

The Object of a Disaster Prevention/Recovery & COOP Plan is, in the event of a Disaster, to be able to resume operations and information technology services quickly, efficiently and effectively in order to mitigate the amount of damage and its associated costs relating to:

- Lost Revenue
- Wages
- Labor
- Employee Morale
- Customer Goodwill
- Marketing Opportunities
- Incurred Bank Fees
- Incurred Legal Penalties &
- Bad Publicity



Disaster Prevention & Recovery, Business Continuity of Operations (COOP), Cybersecurity Incident Response & Vital Records Plans

As seen, “UNPLANNED DOWNTIME” can have serious & life-threatening consequences. That is why Established Emergency Procedures and Continuance of Operations Plans are imperative **before, during & after** a Disaster or Incident. It identifies Essential Personnel, Equipment, Alternate Site(s), etc. in order to mitigate incident/loss & expediently resume operations/services in-house or remotely.

Disaster Prevention & Recovery Plan

- Mitigates Loss of Records
NOTE: **WATER** is the biggest culprit in a records disaster!!!
- Protects Vital and Historical Records
- Protects Electronic Records, Hardware & Software

Business Continuity of Operations (COOP) Plan

- Resume operations safely, quickly & efficiently
- Ensure the normal flow of business

NOTE: Retain accessible copies of updated Insurance Policies – Hazard, flood, etc.

Disaster Prevention & Recovery, Business Continuity of Operations (COOP), Cybersecurity Incident Response & Vital Records 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 *hardcopy* 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! Etc.**

Records and Information Management —
Damaged Records Report

Damaged Records Reports

DORES-RMS Damaged Records Report Forms

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 Discov _____

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.

Damaged Records Reports ...



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.

Date

NJDORES-RMS Damaged Records Report Form – Disposal Certification



Contact Information

Department of the Treasury
Division of Revenue and Enterprise Services
Records Management Services
PO Box 661 Trenton, NJ 08625
609-292-8693 & 609-777-1020

<https://www.nj.gov/treasury/revenue/rms/index.shtml>



RECORDS MANAGEMENT SERVICES



Department of the Treasury

Division of Revenue and Enterprise Services

Records Management Services

RMS Staff Contact

The screenshot shows the 'Records Management Services' website. The top navigation bar includes links for 'RMS', 'Records', 'Imaging', 'New Jersey Records Manual', 'Contact RMS', and 'RMS Consultation'. The 'RMS Consultation' link is circled in red. A red arrow points from this link to a dropdown menu that is open, showing 'Directions' and 'Contact' options. Below the navigation is a 'Records Management Services' section with contact information for Liz Hartmann (609-777-1020) and a table of staff contacts categorized by county and municipality.

Category	Staff Name	Contact Number
County: A - C	Terricka Page	609-292-8708
County: E - H	John Berry	609-292-8683
County: M - W	Marcella Campbell	609-292-8689
Municipalities: A - E	Terricka Page	609-292-8708
Municipalities: F - L	John Berry	609-292-8683
Municipalities: M - R	Marcella Campbell	609-292-8689
Municipalities: S - Z	Robert Herrick Virma Guzman-Reyes	609-292-8698 609-292-8711
Schools	Karen Perry	609-292-8697
County and Municipal Prosecutors	Terricka Page	609-292-8708
County Community Colleges/County Vo-Tech Schools	Karen Perry	609-292-8697
County Detention Centers - Adult and Juvenile	Robert Herrick Alternate Virma Guzam-Reyes	609-292-8698 609-292-8711

Department of the Treasury

Division of Revenue and Enterprise Services

Records Management Services

RMS Staff Consultation

The screenshot displays the Records Management Services website interface. At the top, a navigation bar includes links for 'RMS', 'Records', 'Imaging', 'New Jersey Records Manual', 'Contact RMS', and 'RMS Consultation'. The 'RMS Consultation' link is circled in red. Below the navigation bar, a breadcrumb trail reads 'Home / RMS Contact Information Records Retention and Disposition'. The main content area is titled 'Records Management Services Contact Information Records' and features several service categories: 'Division Management', 'Imaging Services Group', and 'Records Storage - Unit Supervision'. The 'Division Management' section lists the 'State Records Center' with its address and phone number. The 'Imaging Services Group' section lists 'Sue Cramer' and her phone number. A red arrow points from the 'RMS Consultation' link in the navigation bar to a 'RMS Consultation' button in a pop-up window. This pop-up window is titled 'Contact Us - Records Management Consultations' and is also circled in red. It contains a service request form with fields for 'Prefix', 'First Name', 'Middle I', 'Last Name', and 'Address Line 1'. Below the form, contact information for 'Marcella Campbell' and the phone number '609-292-8689' is visible.

Records Management Services

RMS [Records](#) [Imaging](#) [New Jersey Records Manual](#) [Contact RMS](#) **RMS Consultation**

Home / RMS Contact Information Records Retention and Disposition

Records Management Services Contact Information Records

Division Management

State Records Center

2300 Stuyvesant Avenue,
PO Box 661,
Trenton, NJ 08625-0661

Imaging Services Group

Microfilm Client Relations and Billing

Sue Cramer
609-777-0902

Records Storage - Unit Supervision

Home / Contact Us - Records Management Consultations

Contact Us - Records Management Consultations

For business records please visit the [Business Records Service portal](#).

The Division of Revenue and Enterprise Services, Records Management Service Unit, is pleased to offer online, real-time consultations to public agencies throughout New Jersey. If your agency is experiencing problems with managing its public records or needs guidance on a particular records management topic or practice, use this service to obtain help.

Fill out and send the following service request to us. We will assemble a team of experts who will respond to your request or problem and then schedule a live video conference with you and your team. We look forward to serving you.

Service Request

Prefix: First Name: Middle I: Last Name:

Address Line 1:

Marcella Campbell 609-292-8689

*Thank
you*

