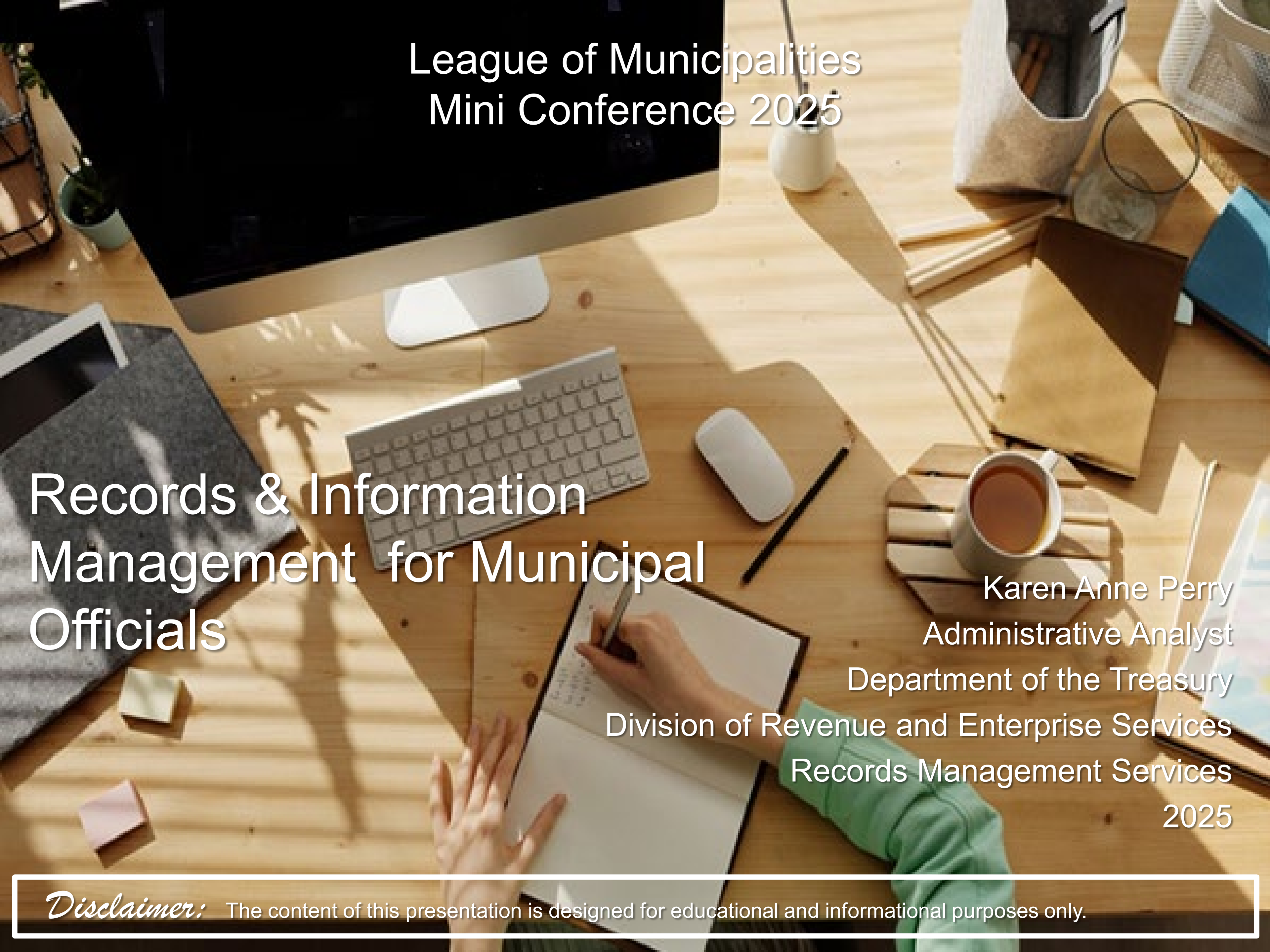


League of Municipalities
Mini Conference 2025

Records & Information Management for Municipal Officials

Karen Anne Perry
Administrative Analyst
Department of the Treasury
Division of Revenue and Enterprise Services
Records Management Services
2025

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

Why should *we* be concerned?

It’s The Law

- NJ Public Records Law
- Open Public Records Act (OPRA)
- Data Privacy, Compliance and Security Laws
- Litigation and e-Discovery Support
- Globalism: International, Federal and State
    - **European Union’s *General Data Protection Regulation (GDPR)* & Regulation (EU) 2016/679** for privacy and protection for processing of personal data;
    - ***Health Information Technology for Economic and Clinical Health Act (HITECH)* for Health Information Technology and Electronic Health Records (EHR)*;***
    - ***Health Insurance Portability and Accountability Act* (HIPAA)** for personal medical information
    - **Securities & Exchange Commission’s (SEC) *Sarbanes-Oxley Act* (SOX)** which protects shareholders from public companies’ accounting errors & financial fraud.

Compliance

- Information Governance: Data Access & Migration
- Coding and Classification: **ICD-10** for diagnosis, procedure, and treatment coding - for billing and data analysis.
- Data Analytics: Identify trends, improve care, and foster research.
- Audit: Financial & Programmatic - Relevance with Regulations & Standards
- Program Review: Joint Commission & NJ State Medical Examiners’ Board

Cost Effective

- Minimize costs and promotes savings, efficiency and productivity.

Legacy Information

- Irreplaceable loss of intellectual rights, legacy records, etc.

Valuable Asset

- Establish Policies and Procedures - Health Data Governance with ongoing training.

- Data Quality and Accuracy: Ensuring the completeness, consistency, and accuracy of medical records to avoid compromised decision-making.

- Collaborative, seamless information exchange between the different systems, other departments, clinicians, administration and, stakeholders.

- Loss, theft or damage can cause a patient’s personal loss, financial loss, disrupt business operations, damage an agency’s reputation resulting in loss of public confidence and trust.

New Jersey Public Records Law

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.

What is a Public Record?

Records Management Services

NJSA 47:3-16: 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."

Government Records Council

NJSA 47:1A-1.1., OPRA: Defines a **Government Record** as "All records that are made, maintained, kept on file, or received in the course of official business."

National Archives & Records Administration

CFR 44: Defines a **Federal Record** 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 ... 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."

In New Jersey, "Public" Has Two (2) Meanings

Ownership
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.

Access
The *Open Public Records Act (OPRA)/NJSA 47:1A* provides that public records must be accessible. However, because of issues of **Privacy, Confidentiality & Security,** an agency may restrict access to records:

- OPRA Requests
- Common Law Requests
- Discovery Requests
- Administrative Requests
- Informal Requests
- Subpoenas, Court Orders, etc.

Litigation Hold Order

Litigation Hold Order

In the event of an OPRA Request or Litigation, a **Litigation Hold Order** should be issued for all associated information (Hardcopy, Digital and Electronic) should be immediately segregated.

A Notice Of Receipt

Should be distributed to the associated agencies indicating they have been notified of the **Litigation Hold Order** and sign and return to the sender within five (5) days and that associated records will be segregated.

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.

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

AUDIT
ACCOUNTING
RECORDS
ENGAGEMENT
TRUST
RECEIPTS
SUPERVISION
FINANCE

Audit

Objective
Transparency in Good Records Governance

Penalties
The unlawful and deliberate alteration, destruction or falsifying of records

Retention
Electronic, Digital, Hardcopy and Cloud Storage Records

IT Security
Prevent Data Breaches

Records
Retention & Disposition

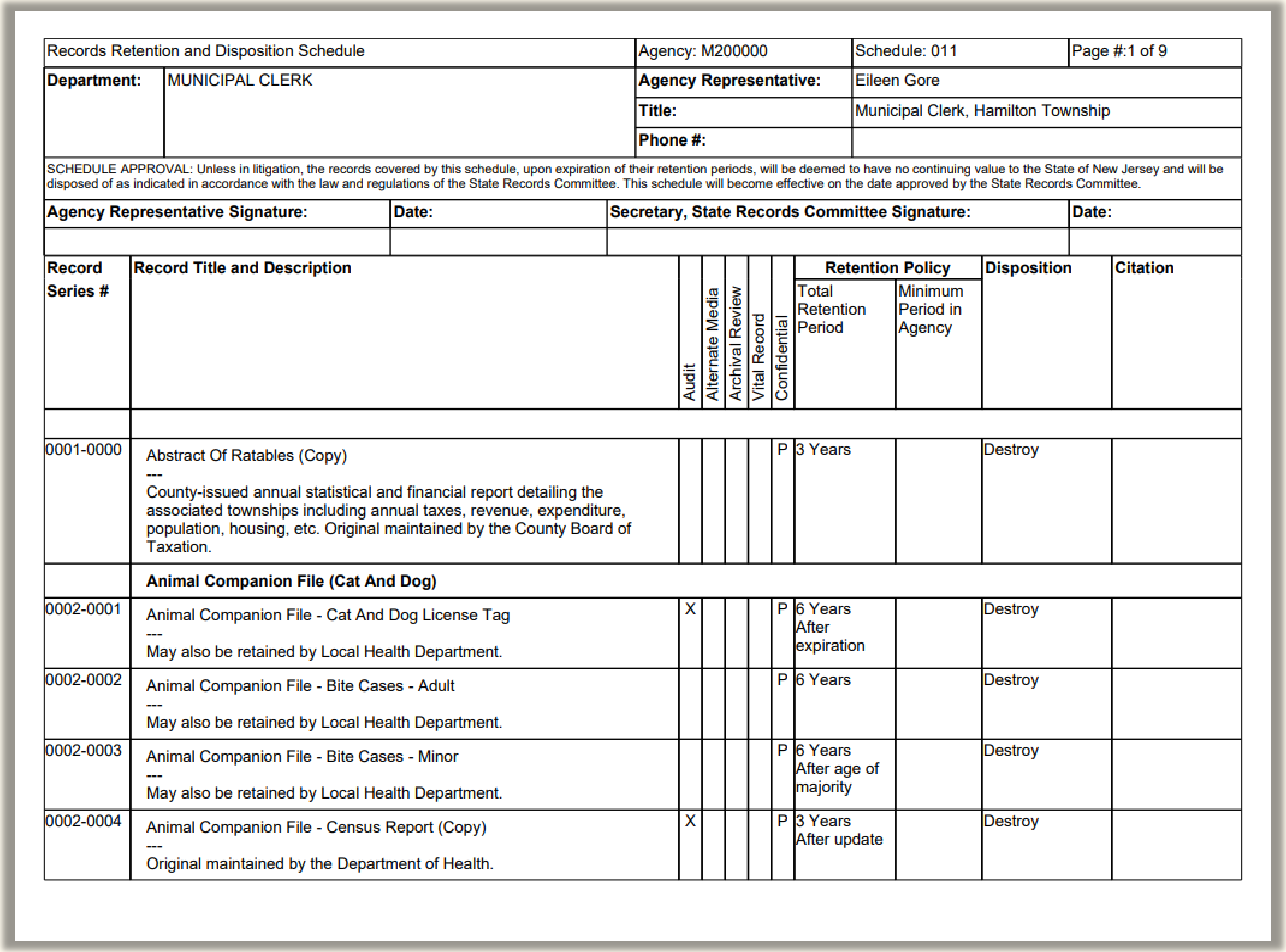
Records Retention

NJSA 47

Records Management Services (RMS)
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 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.



Records Retention and Disposition Schedule	Agency: M200000	Schedule: 011	Page #:1 of 9

Department:	MUNICIPAL CLERK	**Agency Representative:**	Eileen Gore
		Title:	Municipal Clerk, Hamilton Township
		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.

Agency Representative Signature:	**Date:**	**Secretary, State Records Committee Signature:**	**Date:**

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	Abstract Of Ratables (Copy) --- County-issued annual statistical and financial report detailing the associated townships including annual taxes, revenue, expenditure, population, housing, etc. Original maintained by the County Board of Taxation.					P	3 Years		Destroy	
	Animal Companion File (Cat And Dog)									
0002-0001	Animal Companion File - Cat And Dog License Tag --- May also be retained by Local Health Department.	X				P	6 Years After expiration		Destroy	
0002-0002	Animal Companion File - Bite Cases - Adult --- May also be retained by Local Health Department.					P	6 Years		Destroy	
0002-0003	Animal Companion File - Bite Cases - Minor --- May also be retained by Local Health Department.					P	6 Years After age of majority		Destroy	
0002-0004	Animal Companion File - Census Report (Copy) --- Original maintained by the Department of Health.	X				P	3 Years After update		Destroy	

Records Disposition

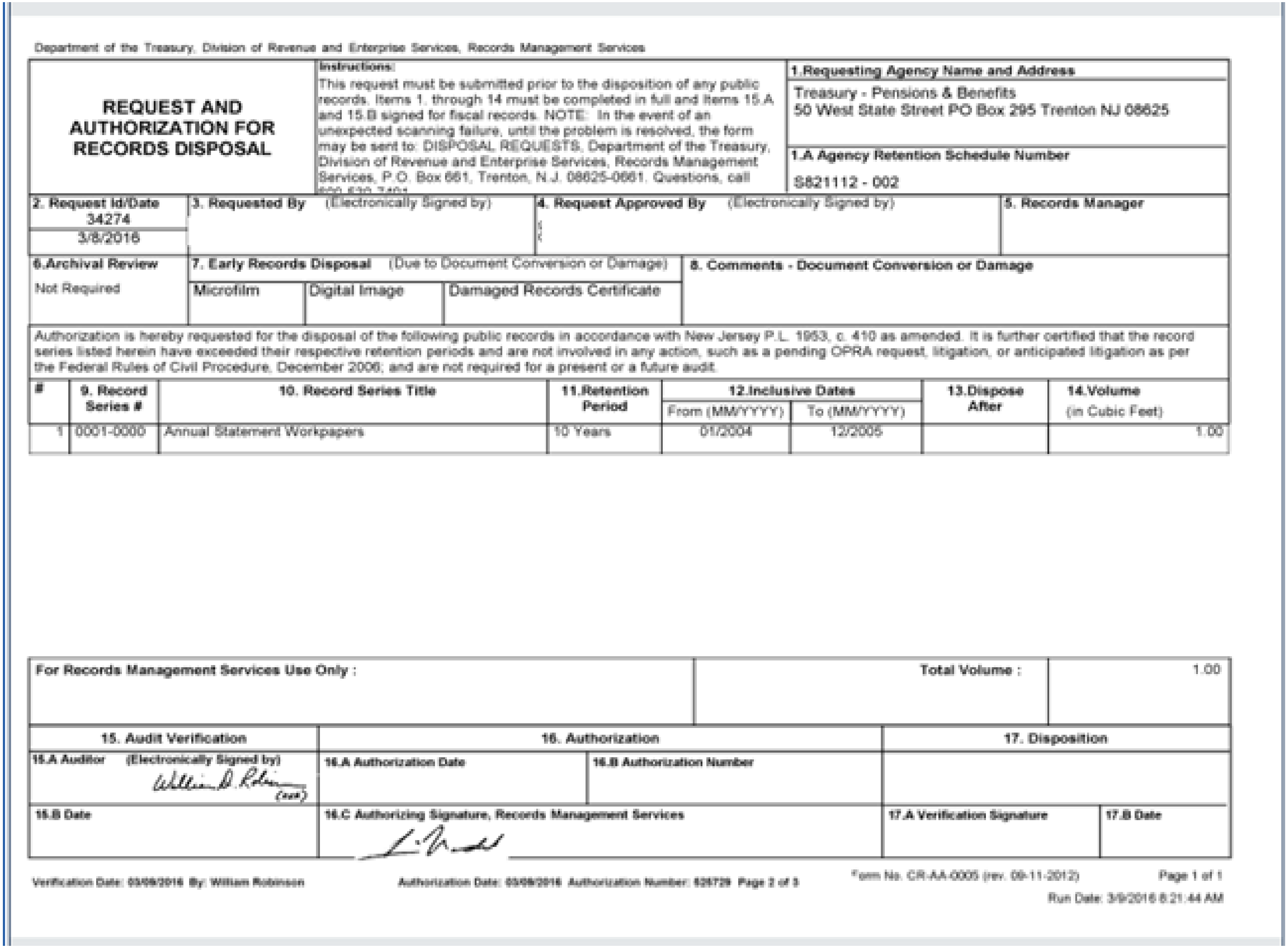
NJSA 47

Public Agencies must submit
A *“Request and Authorization for Records Disposal”* to obtain **prior** authorization from DORES-RMS, to legally dispose of the **expired** Public Records in their custody through Artemis.

Upon receiving authorization
The associated records should be disposed as they are **Discoverable** as long as they are in an Agency’s **Physical Custody** regardless of receipt of a disposal authorization from DORES-RMS.

Request and Authorization for Records Disposal
Are Permanently retained in Artemis for immediate access in the event of:

- OPRA
- Litigation
- Audit



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 7401

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		13.Dispose After	14.Volume
				From (MM/YYYY)	To (MM/YYYY)		(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

15.A Auditor (Electronically Signed by)
William D. Robin

15.B Date

16. Authorization

16.A Authorization Date

16.B Authorization Number

16.C Authorizing Signature, Records Management Services

17. Disposition

17.A Verification Signature

17.B Date

Verification Date: 03/09/2016 By: William Robinson

Authorization Date: 03/09/2016 Authorization Number: 626729 Page 2 of 3

Form No. CR-AA-0005 (rev. 09-11-2012)

Page 1 of 1

Run Date: 3/9/2016 8:21:44 AM

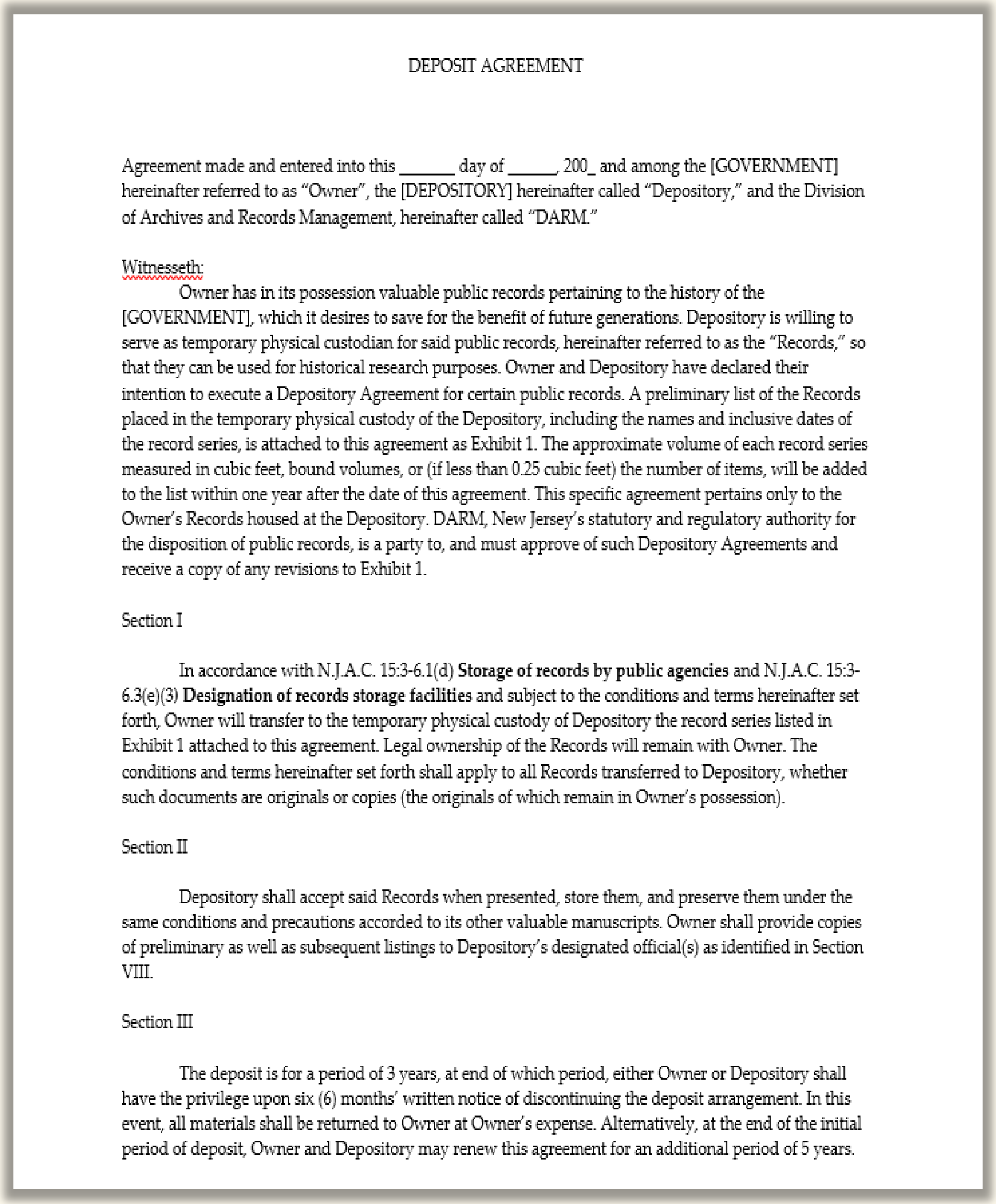
Record Storage

ACTIVE RECORDS
On-site records storage.

INACTIVE RECORDS/
Records Transfer Request
Should be used to determine the records retention time periods for offsite storage for either a government or Commercial Facility to avoid incurring lengthy storage fees if the records are kept beyond the legal retention requirement.

HISTORICAL RECORDS/
Depository Agreement
Should be Established (for the protection of the Historical Records) between the Agency and the **Public** Historical Records Depository.

Depository Agreement



DEPOSIT AGREEMENT

Agreement made and entered into this ______ day of ______, 200_ and among the [GOVERNMENT] hereinafter referred to as "Owner", the [DEPOSITORY] hereinafter called "Depository," and the Division of Archives and Records Management, hereinafter called "DARM."

Witnesseth:

Owner has in its possession valuable public records pertaining to the history of the [GOVERNMENT], which it desires to save for the benefit of future generations. Depository is willing to serve as temporary physical custodian for said public records, hereinafter referred to as the "Records," so that they can be used for historical research purposes. Owner and Depository have declared their intention to execute a Depository Agreement for certain public records. A preliminary list of the Records placed in the temporary physical custody of the Depository, including the names and inclusive dates of the record series, is attached to this agreement as Exhibit 1. The approximate volume of each record series measured in cubic feet, bound volumes, or (if less than 0.25 cubic feet) the number of items, will be added to the list within one year after the date of this agreement. This specific agreement pertains only to the Owner's Records housed at the Depository. DARM, New Jersey's statutory and regulatory authority for the disposition of public records, is a party to, and must approve of such Depository Agreements and receive a copy of any revisions to Exhibit 1.

Section I

In accordance with N.J.A.C. 15:3-6.1(d) **Storage of records by public agencies** and N.J.A.C. 15:3-6.3(e)(3) **Designation of records storage facilities** and subject to the conditions and terms hereinafter set forth, Owner will transfer to the temporary physical custody of Depository the record series listed in Exhibit 1 attached to this agreement. Legal ownership of the Records will remain with Owner. The conditions and terms hereinafter set forth shall apply to all Records transferred to Depository, whether such documents are originals or copies (the originals of which remain in Owner's possession).

Section II

Depository shall accept said Records when presented, store them, and preserve them under the same conditions and precautions accorded to its other valuable manuscripts. Owner shall provide copies of preliminary as well as subsequent listings to Depository's designated official(s) as identified in Section VIII.

Section III

The deposit is for a period of 3 years, at end of which period, either Owner or Depository shall have the privilege upon six (6) months' written notice of discontinuing the deposit arrangement. In this event, all materials shall be returned to Owner at Owner's expense. Alternatively, at the end of the initial period of deposit, Owner and Depository may renew this agreement for an additional period of 5 years.

Records Storage Guidelines: When Contracting With a Vendor

1. Ensure it is understood that hardcopy 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 the 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.**

https://www.nj.gov/treasury/revenue/rms/imgregistration.shtml

Imaging Certification

INITIAL APPLICATION

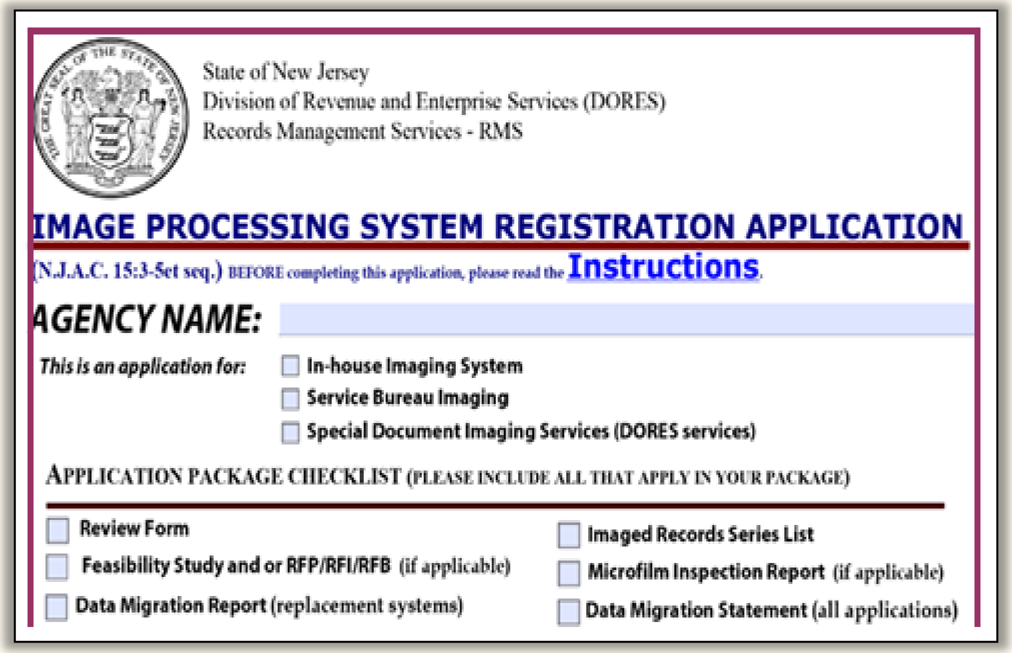
PL 1994, c. 140, allows for the replacement of hardcopy public records with digital and microform images (e.g., Optical Disk & Microfilm).

Initial Imaging Certification: The State Records Committee & Records Management Services issue an Initial Imaging System Certification to an Agency for an in-house or outsourced, **Non-proprietary** imaging application. Documents required for obtaining Certification include:

Imaging Certification Initial Registration Required Documents

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

NOTE: **PDF-A** is the acceptable format.



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.

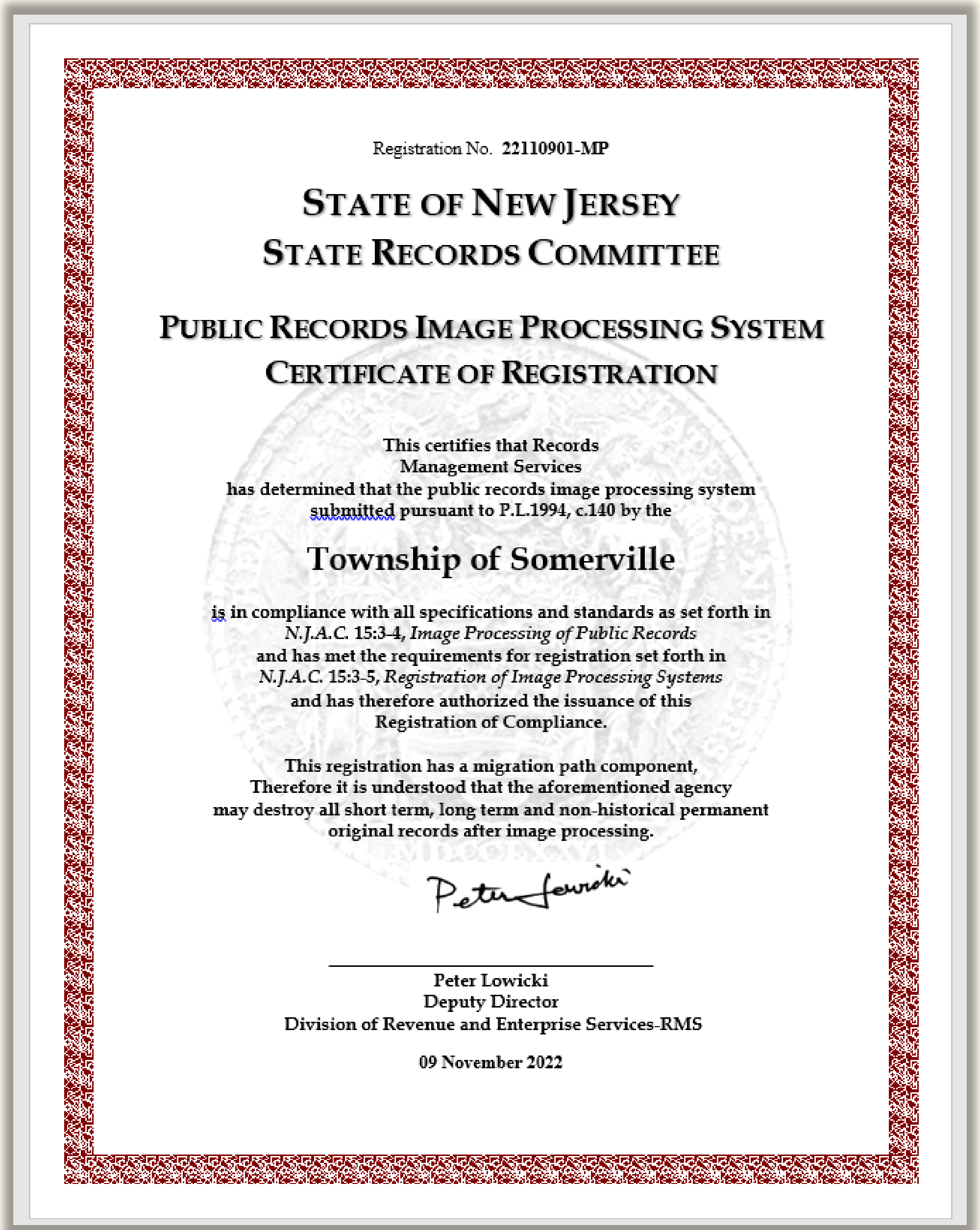
AGENCY NAME:

This is an application for:
□ In-house Imaging System
□ Service Bureau Imaging
□ Special Document Imaging Services (DORES services)

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

□ Review Form
□ Feasibility Study and or RFP/RFI/RFB (if applicable)
□ Data Migration Report (replacement systems)
□ Imaged Records Series List
□ Microfilm Inspection Report (if applicable)
□ Data Migration Statement (all applications)

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 Somerville

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.

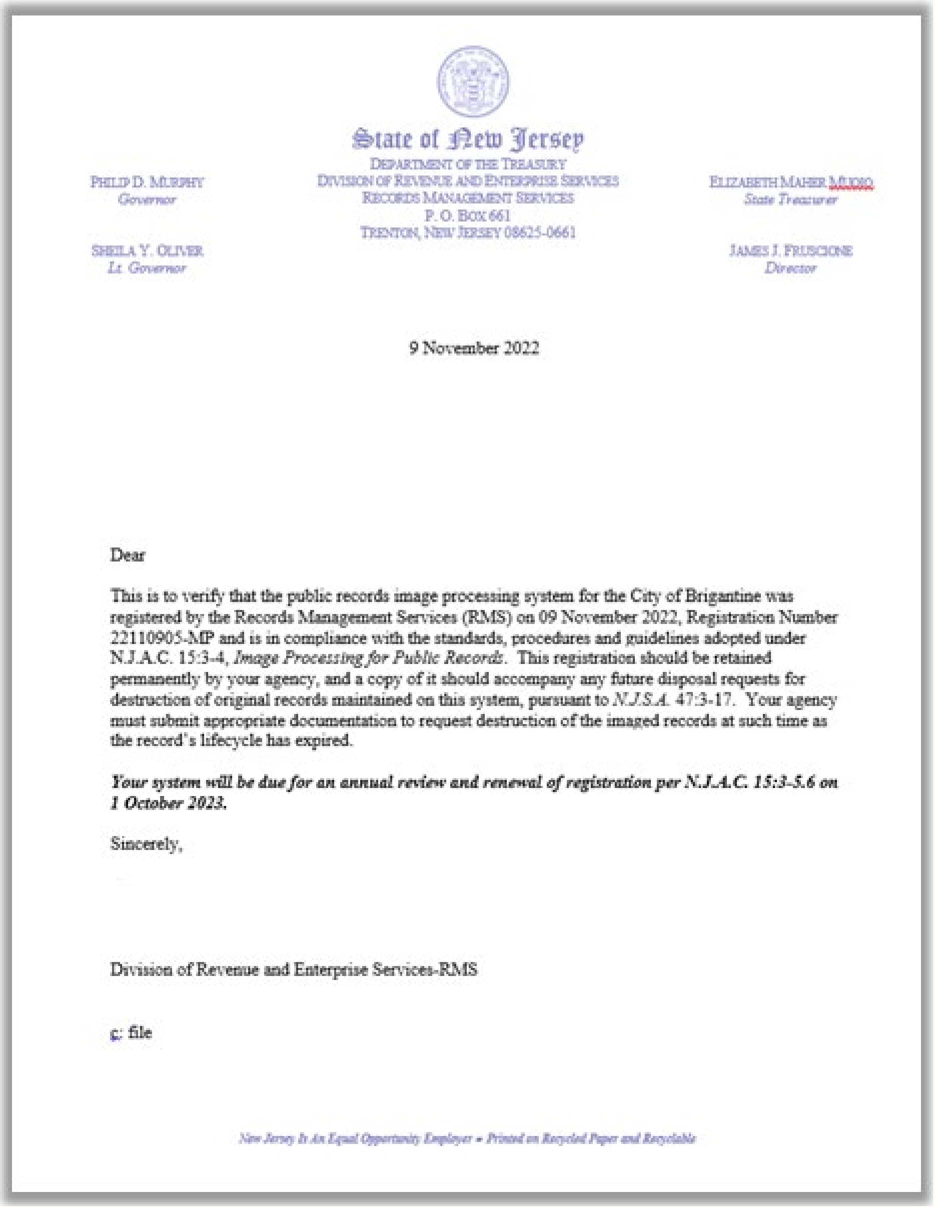
This registration has a migration path component,
Therefore it is understood that the aforementioned agency
may destroy all short term, long term and non-historical permanent
original records after image processing.

Peter Lowicki

Peter Lowicki
Deputy Director
Division of Revenue and Enterprise Services-RMS

09 November 2022

LETTER OF CERTIFICATION



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

SHEILA Y. OLIVER
Lt. Governor

ELIZABETH MAHER MUOIO
State Treasurer

JAMES J. FRUSCIONE
Director

9 November 2022

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.

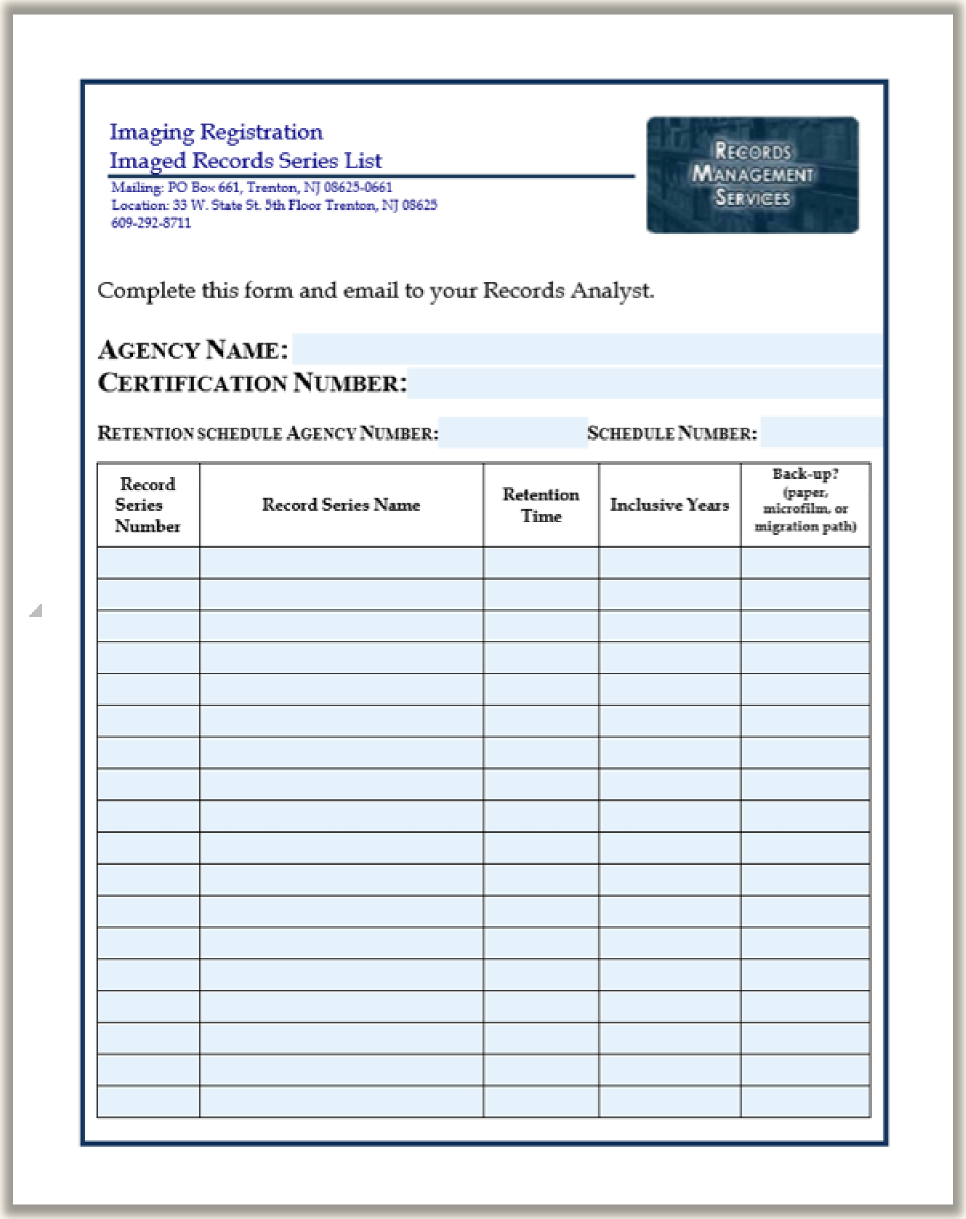
Sincerely,

Division of Revenue and Enterprise Services-RMS

c: file

New Jersey Is An Equal Opportunity Employer • Printed on Recycled Paper and Recyclable

RECORD SERIES LIST



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

Records Management Services

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)

ANNUAL RENEWAL/AMENDMENT

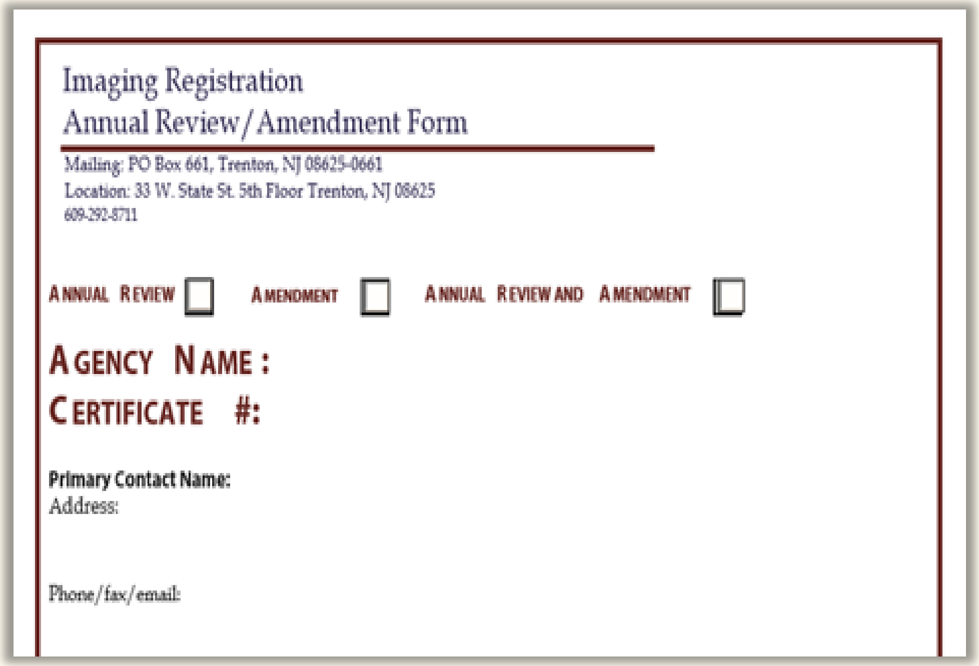
To maintain Certification: The State Records Committee and Records Management Services also issue an Annual Renewal/Amendment Imaging System Certification to an Agency for an in-house or outsourced, **non-proprietary** imaging application.

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

Annual Review/Amendment Documents

- Annual Renewal Application
- Data Migration Path/Backup
- Imaged Records Series List
- Hardware/Software Specifications – ***only*** if upgrades/changes were made.

NOTE: **PDF-A** is the acceptable format.



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

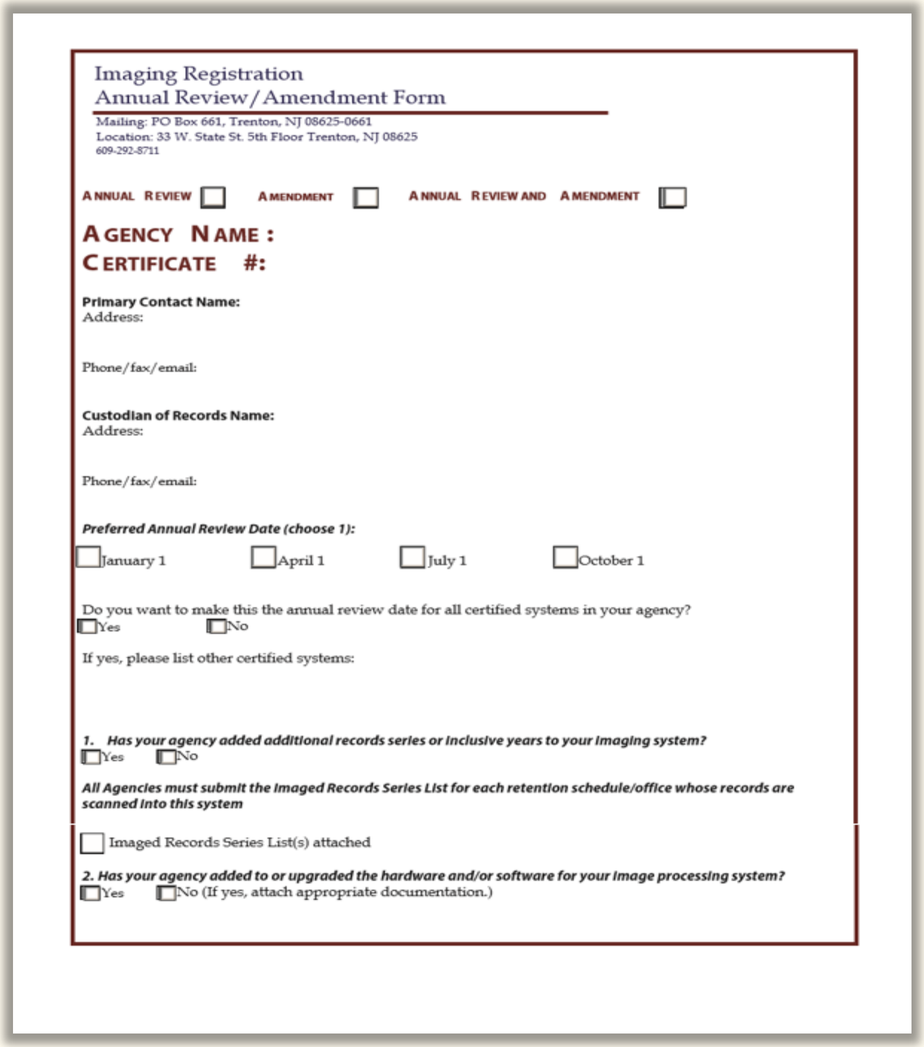
ANNUAL REVIEW □ AMENDMENT □ ANNUAL REVIEW AND AMENDMENT □

AGENCY NAME:
CERTIFICATE #:

Primary Contact Name:
Address:

Phone/fax/email:

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

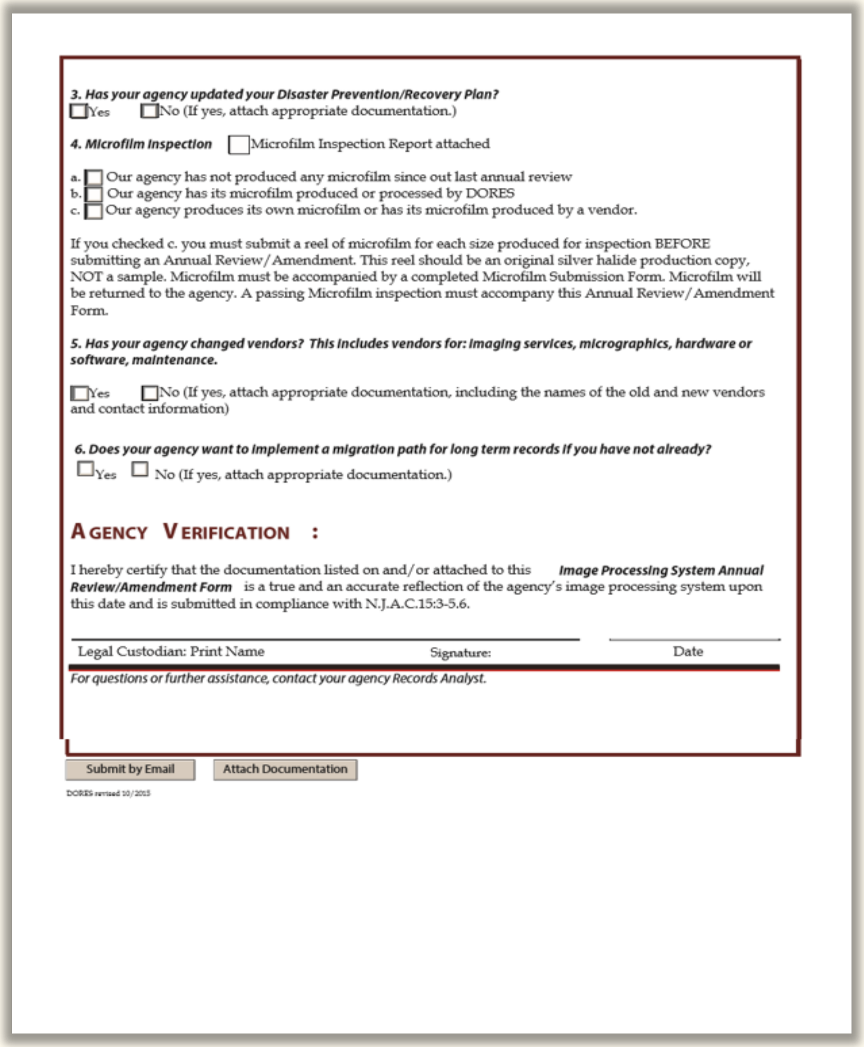
If yes, please list other certified systems:

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.)



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 out 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 :

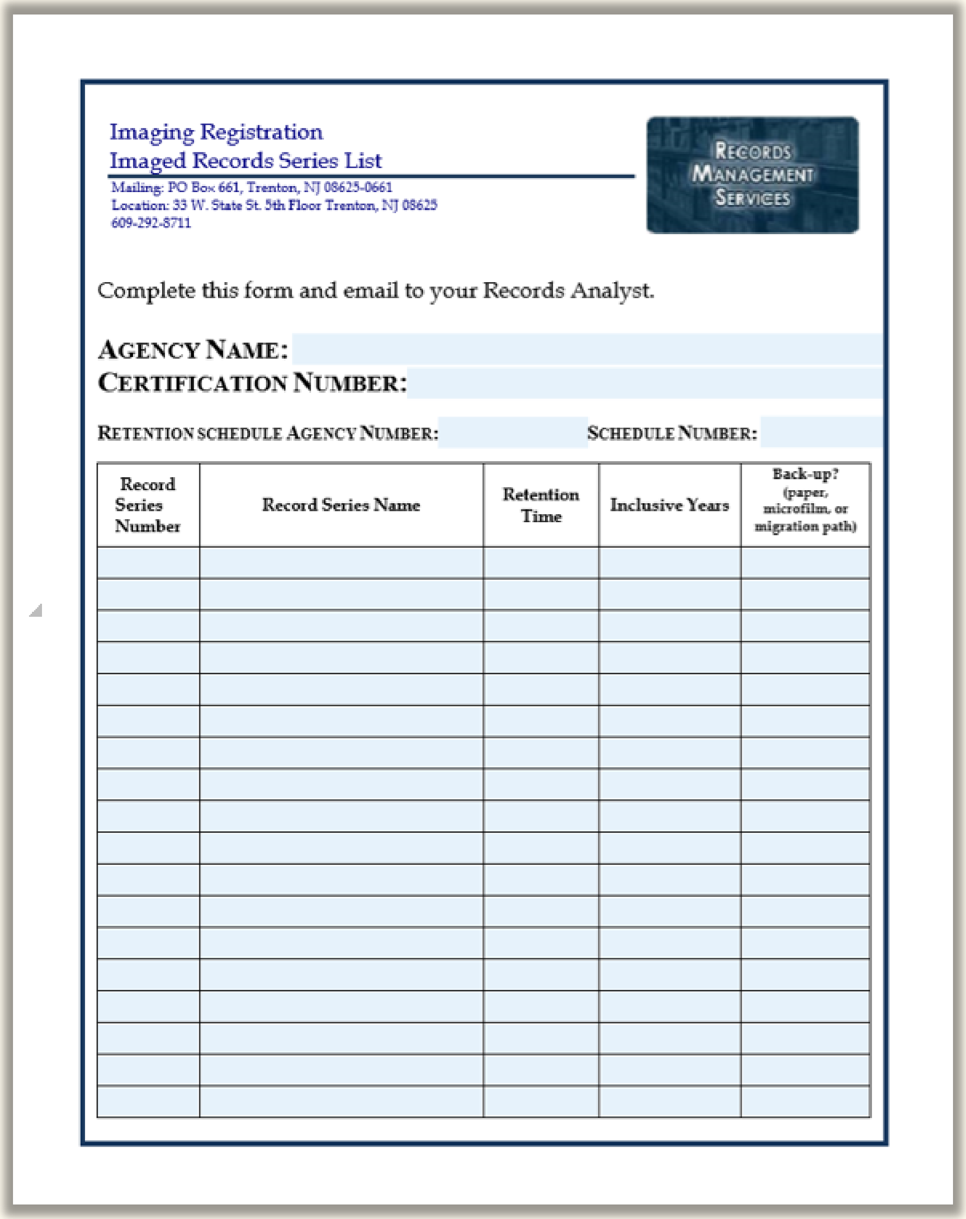
I hereby certify that the documentation listed on and/or attached to this ***Image Processing System Annual Review/Amendment Form*** is a true and an accurate reflection of the agency's image processing system upon this date and is submitted in compliance with N.J.A.C.15:3-5.6.

Legal Custodian: Print Name Signature: Date

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

DORES revised 10/2015

RECORD SERIES LIST



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

RECORDS MANAGEMENT SERVICES

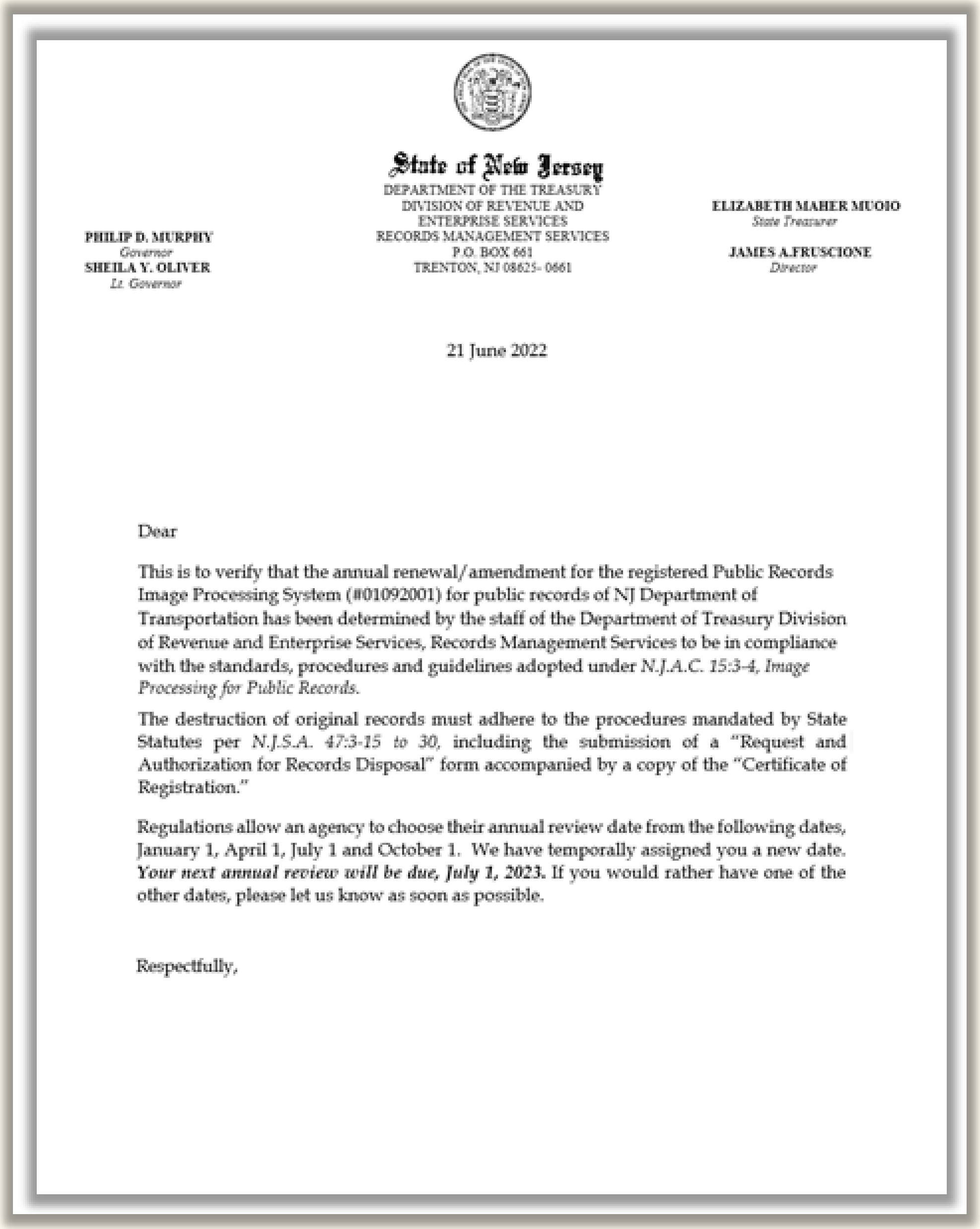
Complete this form and email to your Records Analyst.

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)

ANNUAL/AMENDMENT 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

Dear

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,

Image Processing Guidelines: When Contracting With 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.**

https://www.nj.gov/treasury/revenue/rms/imgregistration.shtml

THE CLOUD

THE CLOUD

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

Records and Information Management Professionals should work across disciplinary lines to protect these records with the same considerations for hardcopy records:

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

Cloud Storage Guidelines: When Contracting With 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. Monitor the life-cycle of records stored in the Cloud – creation, storage, access, storage or legal destruction.
6. Prohibit the Vendor from destroying or image records unless the Agency specifically directs the action.
7. Require the Vendor to document changes in their format/programming that may affect records access.
8. Specify records transfer requirements for contract-exit processes.
9. **Ensure records are retrievable and accessible in response to OPRA Requests, Audits, Subpoenas, Investigations, e-Discovery, Litigation Holds and Litigation.**

www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforRecordsManagementintheCloud.pdf

Email & Electronic Communication

Email & Electronic Communication (including content, metadata and attachments) are Public Records with the same Records Retention, Disposition, Access, Intellectual Property, Legal Rules of Evidence and e-Discovery concerns as hardcopy or microform records. This includes: Email, Blogs, Wikis, Pod Casts, Social Media, Posts, Text, Chats, etc.

Remember…

Email and Electronic Communication are

Public Records

Accessed under OPRA

Accessed under an Audit

Discoverable

- May be Disclosed in a Court of Law
- May be Disclosed through e-Discovery

May Not be Destroyed Without Prior Authorization from DORES-RMS

Email & Electronic Communication Management

Consult the General Schedule

For the retentions for Email and Electronic Communication - in general, a **7-year retention period** is regarded for the Retention and Disposition of Email.

Adopt policies

For Email, Social Media and Internet usage with **ongoing** Agency-wide training.

Email and Electronic Communications System should have:

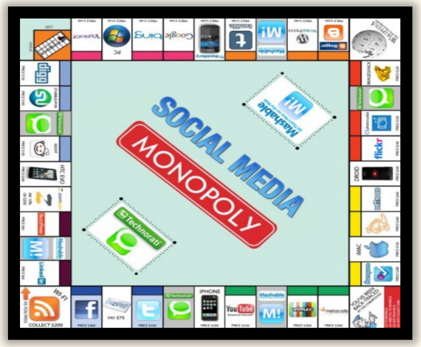
Security Controls that guard against **unauthorized** access, use, modification, dissemination, disclosure and/or destruction as Email is often a phishing target.

- **Provisions** for the administration of "Litigation Holds" and Compliance Audits.
- **Back-up and Disaster Recovery** for the restoration of Email.
- ***Authorized* Agency IT Staff** should control the tracking, indexing archiving, access, retention and disposition of Email records in the Email Central Storage/Management System.

https://https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforSchedulingElectronicMessagingRecordsforRetentionandDisposition.pdf

Social Media

SOCIAL MEDIA



Interactive communication via web-based and mobile technology.

Global, Immediate and **Very Accessible!**

Public: and in the event of e-Discovery, Litigation, OPRA and Legal Rules of Evidence - Records Retention & Disposition directives should be established regarding content, language, subject matter, which includes: blogs, Wikis, Pod casts, Metadata, TEAMS, OneDrive, SharePoint and Email regarding – Operational Records, Meetings, Events, Chats & Recordings

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.

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 .

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.

https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforSchedulingSocialMediaRecordsforRetentionandDisposition.pdf

The Internet

THE INTERNET

Due to ever-changing content & structure, an agency's website should be routinely maintained and its hardware, software, metadata and content should reflect the following areas of concern:

Enterprise-wide Records & Information Management Policy

Records Management & Access Perspective: OPRA Request

Security Perspective: Implemented & Monitored Data Security/Encryption

IT Perspective: Website Creation, Maintenance, Growth & Security

Intellectual Property & Historical Perspective: Digitally-born documents if not printed may be lost.

Legal Perspective: Litigation, Legal Rules of Evidence & e-Discovery.

Financial Perspective: Federal, State or Local Audit.

“The Stafford Act”

ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT
[Public Law 93–288; Approved May 22, 1974]
[As Amended Through P.L. 117–328, Enacted December 29, 2022]

EMERGENCY

Any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.

MAJOR DISASTER

Any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of State, County and Municipal Governments and Disaster Relief Organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Vital Records

VITAL RECORDS: LIFE RELATED

Life event-related records maintained by State, County, Municipal Agencies and Religious Institutions – Birth, Death, Marriage, Adoption, Divorce, Domestic Partnership, Civil Union, Custody, Separation, Drivers License, Disability ID, SSN and Religious.

Public Health
Data collection, statistics, research, monitoring trends, tracking disease and developing public health programs.

Legal
Legal procedures, proving identity and residence, applying for benefits and obtaining citizenship.

Genealogical Research

VITAL RECORDS: MEDICAL

Records and data imperative to maintain life, such as:

- **Prescriptions**
- **Medication(s)**
- **Living Will**
- **Medical Diagnosis**
- **HIPAA**
- **Power of Attorney**

VITAL RECORDS: OPERATIONAL

Records, regardless of their medium, that are deemed Essential in case of Litigation, Prove Legal Ownership, Emergency, Disaster, and Cyber Breach – they typically comprise 10% of an Agency's records.

Disaster Prevention & Recovery and Business Continuity of Operations

DISASTER PREVENTION & RECOVERY/BUSINESS CONTINUITY OF OPERATIONS (COOP) PLAN

THE OBJECTIVE

To **identify an agency's major operational records** (Hardcopy, Electronic, Digital, etc.) and institute measures for their protection in the event of a Disaster (Cyberattacked or Destroyed) and mitigate data loss; ensure data integrity and access and resume operations and services quickly, efficiently and effectively and lessen the amount of damage and associated costs relating to:

Data & Information
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) PLAN

Used in conjunction with Agency Security Standards, Guidelines, Policy and Procedures, Client Network Installation and De-installation Plans, Hardware and Software supporting documentation.

ESTABLISH

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

DISASTER PREVENTION & RECOVERY/BUSINESS CONTINUITY OF OPERATIONS (COOP) PLAN

IDENTIFY

- Hardware and Software (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

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

REVISE

Create the Plan! Test The Plan! Revise The Plan! Re-Test The Plan!

However,

The best laid plans…

If a disaster should strike…

Check: Your **Insurance Policy**!

Assemble Disaster Prevention & Recovery Team: Management, Records Management, Custodian of Public Record, Law Enforcement Agencies

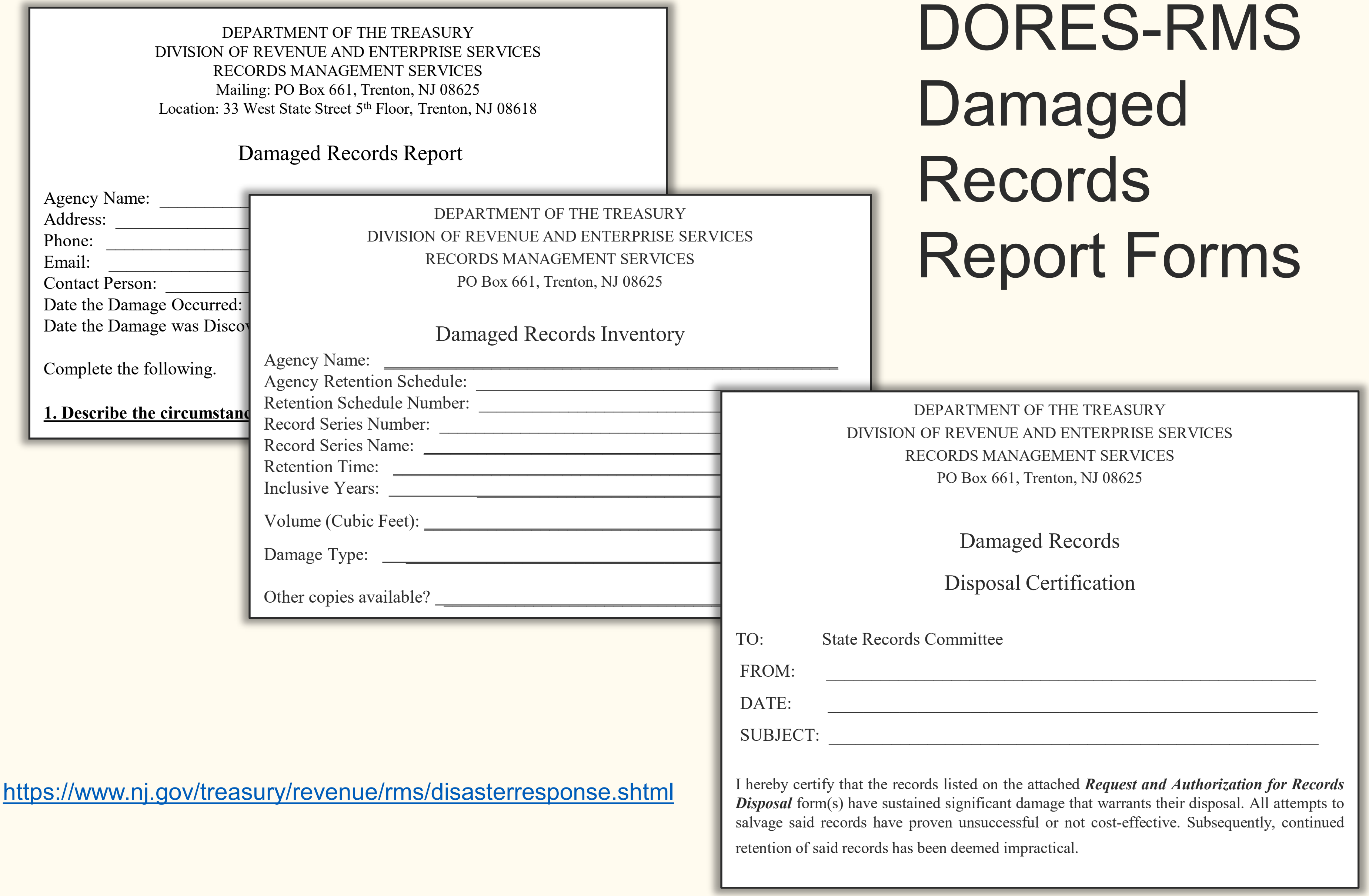
Implement: Disaster Prevention & Recovery and Business Continuity of Operations Plan

Conduct an Assessment: To ascertain if the damaged or destroyed records and information may have had backups such as, Hardcopy, Optical disk or Microform that may be salvaged.

Complete and Submit DORES-RMS Damaged Records Report: For presentation before the State Records Committee (SRC).

https://www.nj.gov/treasury/revenue/rms/pdf/DamagedRecordsReportForms.pdf

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 Disco

Complete the following.

1. Describe the circumstanc

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.

https://www.nj.gov/treasury/revenue/rms/disasterresponse.shtml

Cyber Security

Cyber Security

Cyber Security: Safeguarding devices, hardware, software, networks, data and information from cybercriminal attacks including but not limited to: phishing, ransomware, identity theft, data breaches, espionage and nation-state attacks.

Data and Information Targets: Sensitive Data, Protected Health Information (PHI), Personally Identifiable Information (PII), Intellectual Property, Personal Information, Financial, Educational and Government & Business Information Systems.

Cyber Security Key Areas:

Disaster Prevention & Recovery & Business Continuity
Cloud Security
Email Security
Internet Security
Social Media Security
Identity Management
Data Security
Mobile Security
Network Security
Vital Records

YouTube • 7NEWS Australia

Julian Assange

IS IT EVER *REALLY* SECURE?

Information Technology for Data/Information Processing can foster Operational Efficiencies, but It can also create the potential for Overlapping Internal & External Operational Single & Multiple Threat Groups that can:

- **Disrupt or Shutdown Operations**
- **Inflict Legal, Intellectual, Political, Financial & Security Ramifications**
- **Alter, Corrupt or Destroy Information**
- **Cause Physical Harm**
- **Exploit to Ruin an Agency’s Credibility & Reputation**

CYBER ATTACK STRATEGIES…

ZERO TRUST

Answer:

A User or Device is *never* trusted and access is denied until Identity *and* Authorization have been thoroughly verified.

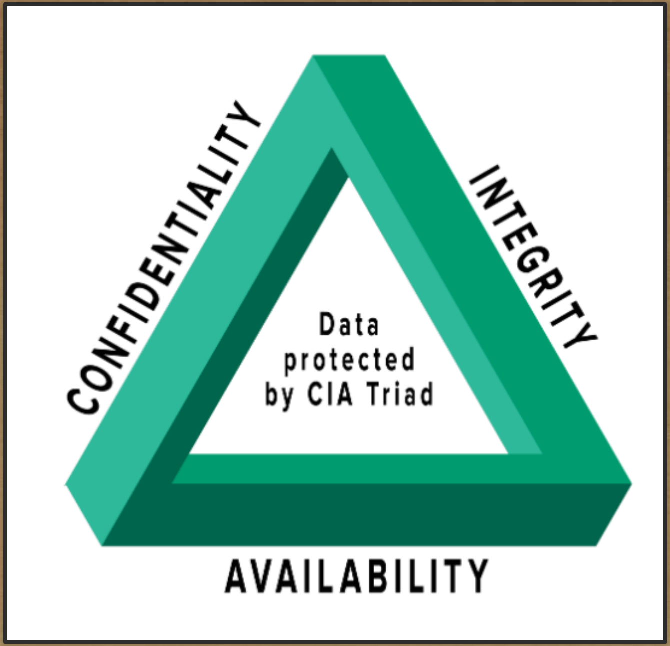
CIA

CIA:

Confidentiality: Only Authorized Individuals can access the information.

Integrity: Only Authorized Individuals can alter, add or remove sensitive information.

Availability: Systems, Functions and Data must be accessible on-demand.



ETHICAL HACKING

Ethical Hacking:
An *agency-authorized* deliberate attempt to gain unauthorized access to its System, Applications and/or Data through duplicating the strategies and actions of a Hacker to identify system security vulnerabilities and resolve them before a real cyber attack occurs.

".gov" Domain – email & Website

It is advantageous to use a ".gov" domain that is available for usage by **only** US-based government agencies for email and website.

CYBER ATTACK:
TYPES

Cyber Attacks may be a single or group attack, a one-time or a repeated attack for: Financial Gain, Espionage, Sabotage, Fraud, Influence, Notoriety, etc.

Phishing, Spearphishing, Smishing, Typosquatting, 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.

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.

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

CYBER ATTACK: TYPES

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.

Cyber-Physical Attack

The ongoing threat of hacks targeting electrical grids, transportation systems, water treatment facilities, etc.,

Man-in-the-Middle Attack (MITM)

A hacker will insert themselves into a two-person online transaction to infiltrate and steal data and information this can happen on secure and unsecure public Wi-Fi Networks.

SQL injection

An attack that inserts malicious code into a SQL Server.

CYBER ATTACK: TYPES

Identity Theft, Medical Information & Stolen Devices/Credentials/IDs

Personal Health Information (PHI) and Personal Identifying Information (PII) can be derived from: Employee IDs, Smart Medical Devices, Smartphones, Electronic Medical Records, Laptops, Tablets, etc.

AI-generated Voices in Video & Robocalls

Artificial Intelligence (AI)-generated voice scams and voice cloning in "Robocalls", are deemed illegal and artificial by the Federal Communications Commission (FCC) and the Telephone Consumer Protection Act (TCPA).

Stalkerware/Spyware

A monitoring spying app utilized through a mobile phone, device or computer.

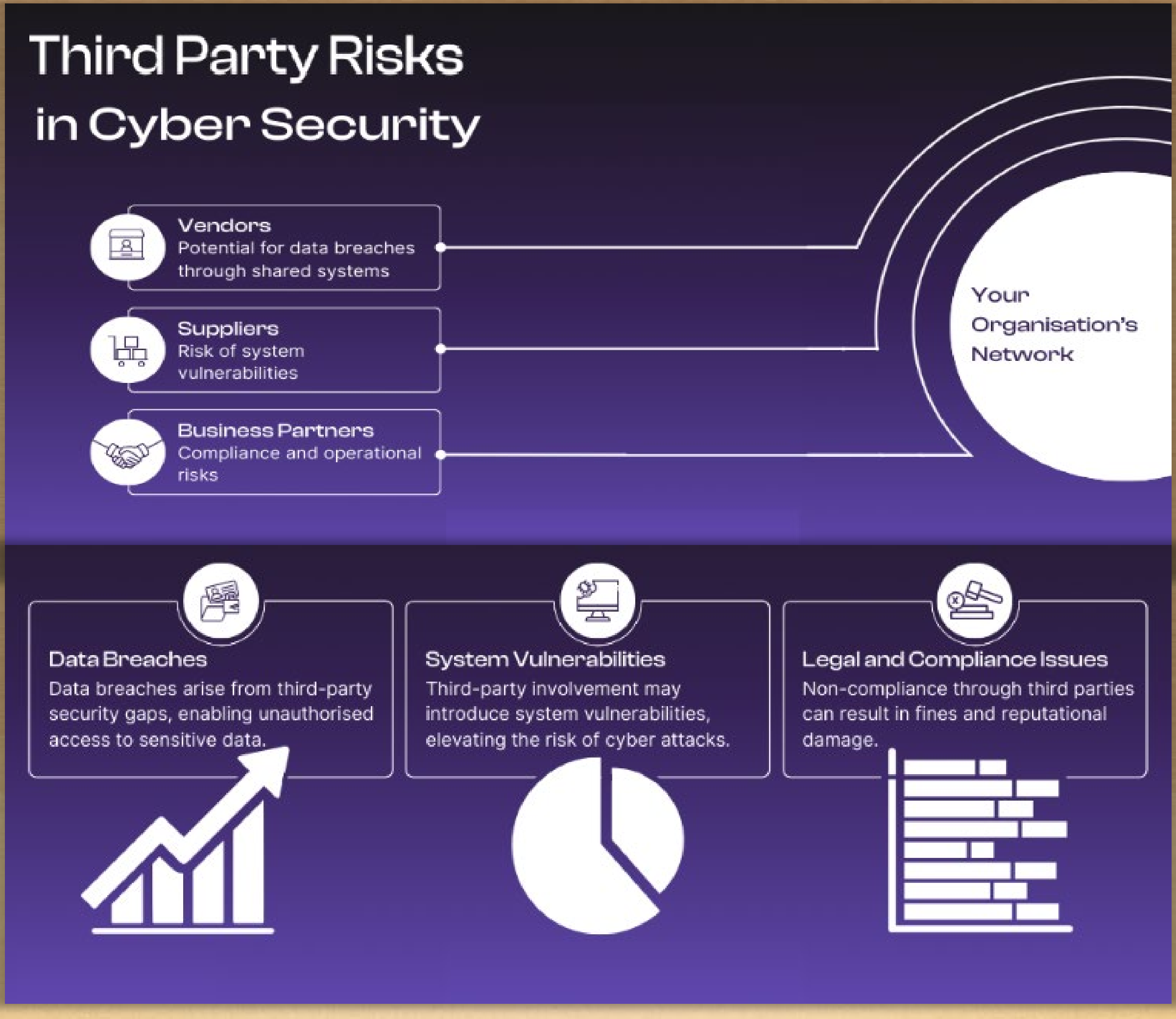
Denial of Service (DoS)

An attack where a network is flooded with processes, actions and requests that overload and shutdown the system.

SIM Swap Attacks/SIM Swap Scam/Port-out Scam/SIM Splitting/ Smishing / Simjacking /SIM Swapping)
Account Takeover (ATO) that targets a weakness in Multi-Factor Authentication on a mobile telephone or theft of a Mobile Phone with the SIM Card being swapped to gain login and access data and information**.** **Solution:** An **eSIM** or **embedded SIM** is a digital SIM card built into a phone without the need of a physical SIM card.

CYBER ATTACK TYPES

Third-Party Contractor or Vendor 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.



Third Party Risks in Cyber Security

Vendors
Potential for data breaches through shared systems

Suppliers
Risk of system vulnerabilities

Business Partners
Compliance and operational risks

Your Organisation's Network

Data Breaches
Data breaches arise from third-party security gaps, enabling unauthorised access to sensitive data.

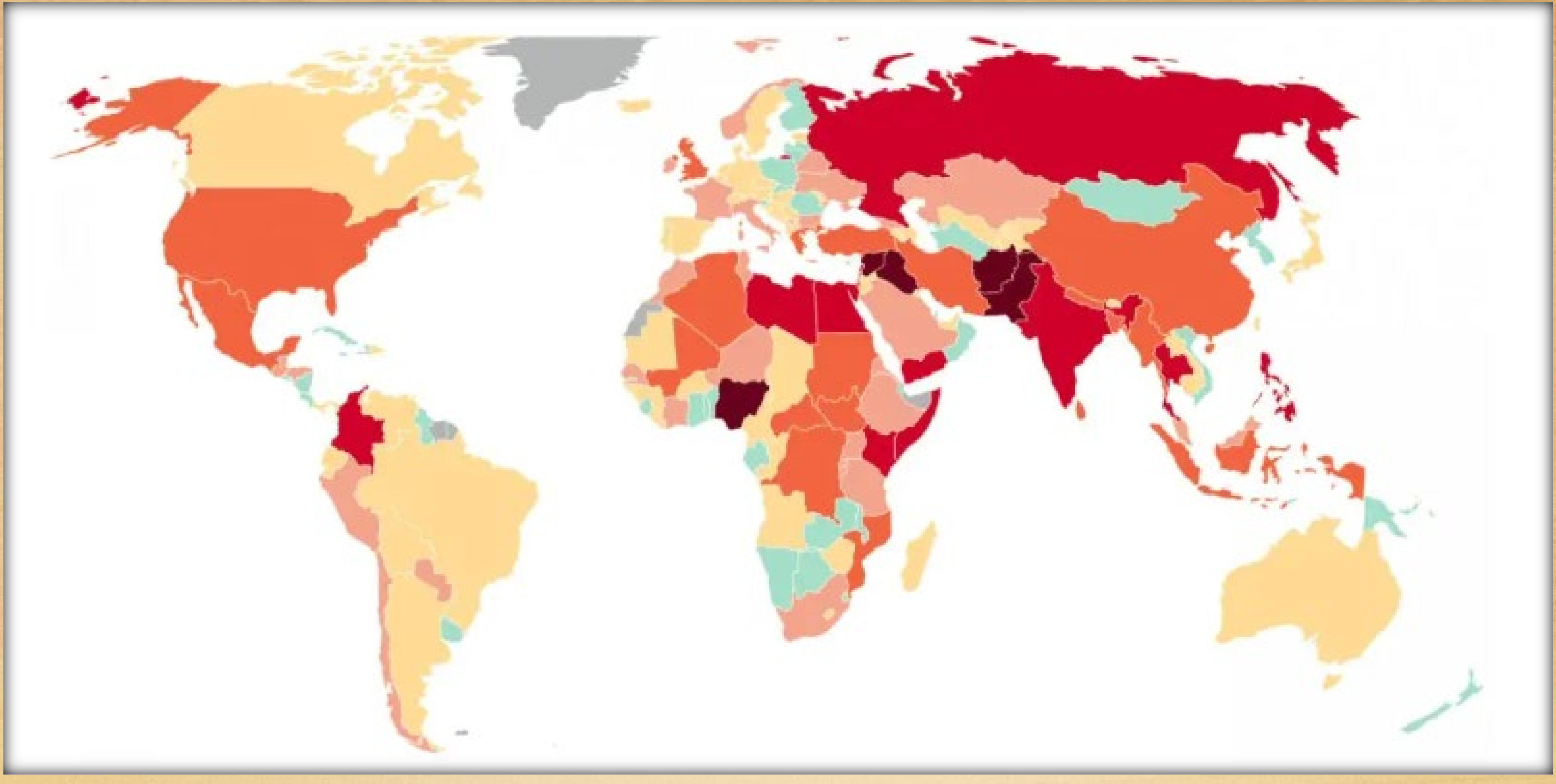
System Vulnerabilities
Third-party involvement may introduce system vulnerabilities, elevating the risk of cyber attacks.

Legal and Compliance Issues
Non-compliance through third parties can result in fines and reputational damage.

CYBER ATTACK TYPES

Noted Regions of Nation State-Sponsored Cyberterrorism, Cyber Security Wars & Attacks

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



Cyber Attacks may be a single/group attack(s), a one-time/repeated attack(s) for Financial Gain, Espionage, Fraud, Sabotage, Influence, Notoriety, etc.

DATA SECURITY:
KEY AREAS

To mitigate internal & external operational threats, Data Security should be approached Enterprise-wide with IT working in coordination with Legal, Records Management, Human Resources and Law Enforcement employing unified Governance and Accountability that starts from the top down.

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

Disaster Prevention & Recovery/Business Continuity of Operations Plan

Acceptable Use Policy: Read & signed by **all** employees for Agency computer usage
Firewalls/Spam Filters: Prevent illicit network traffic
MVR Monitoring: Continuous (**24/7/365**)automated **M**onitoring, **V**erification & **R**eporting
Physical Security: Enterprise-wide Policies and Procedures
Data Encryption: Storage/transit/network-wide
Passwords: Strong passwords, routinely change them w/ Multi-Factor Authentication
Software: Antivirus/Antimalware
Back-up: Data and records
Software: Routine updating and patching
Computer: Configuration management
Auditing: Audit and test
Security Event: Management and Reporting
Data Security: Policies and Procedures
Training: On-going, agency-wide employee training

CYBER SECURITY
INCIDENT RESPONSE PLAN

Components

Much like the Vital Records Plan, a Cybersecurity Incident Response Plan, identifies essential personnel, vendors, equipment and alternate space which are imperative to resume offsite daily operations and safely mitigate the consequences of such an event:

- Activation Authority Procedures
- Specific Task(s) List
- Disaster Recovery Team List
- Response Team List
- Vital Records Protection Methods/Equipment Already Employed
- Cyber Security Response Procedures Distribution List
- Cyber Security Monitoring Procedures
- Communications and Media Sources
- Backup and Hot/Cold Site Locations
- Federal Agency & State Agency Cyber Security Resource Lists
- Cyber Security & Firewall Software Vendor Lists
- Hardware and Software Lists

CYBER SECURITY
INCIDENT RESPONSE PLAN

ESTABLISH

- Vendors Lists: Disaster Recovery Services/Supplies, System Hardware/Software Information and Electronic Disaster Recovery Services
- Cyber Security Team: Management, Records Management, IT, Custodian of Public Record, State Cyber Security Agencies & Local Law Enforcement
- Create an Agency Chain of Command
- Designate Data Center Hot & Cold Site(s) and establish an Alternate Operations Site for Staff, IT and Records
- MVR Monitoring: Continuous (24/7/365) automated Monitoring, Verification and Reporting

CYBER SECURITY
INCIDENT RESPONSE PLAN

ESTABLISH cont.

- Physical Security: Enterprise-wide Policies and Procedures
- Data Encryption: Storage/transit/network-wide
- Firewalls & Filters: Prevent illicit network traffic
- Software/Antivirus/Antimalware: Routine update and patching, detect & prevent unauthorized access and/or intrusion and minimize Dwell Time
- Back-up: Data and Records
- Computer: Configuration Management
- Security Event: Management and Reporting
- Data Security: Policies and Procedures

CYBER SECURITY
INCIDENT RESPONSE PLAN

IDENTIFY

- Identify and Target attacked areas as best as possible
- Isolate them from further attack, quickly as possible
- Check your Insurance Policy
- Reach out immediately to the NJ Office of Homeland Security for assistance
- Resume operations safely & efficiently as possible
- Reassure staff, clients, constituents
- Ensure the normal flow of business as quickly as possible

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.

If a cyber breach should strike…

Check: Your **Insurance Policy**!

Assemble Cybersecurity Team: Management, Records Management, Custodian of Public Record, State Cybersecurity and Law Enforcement Agencies

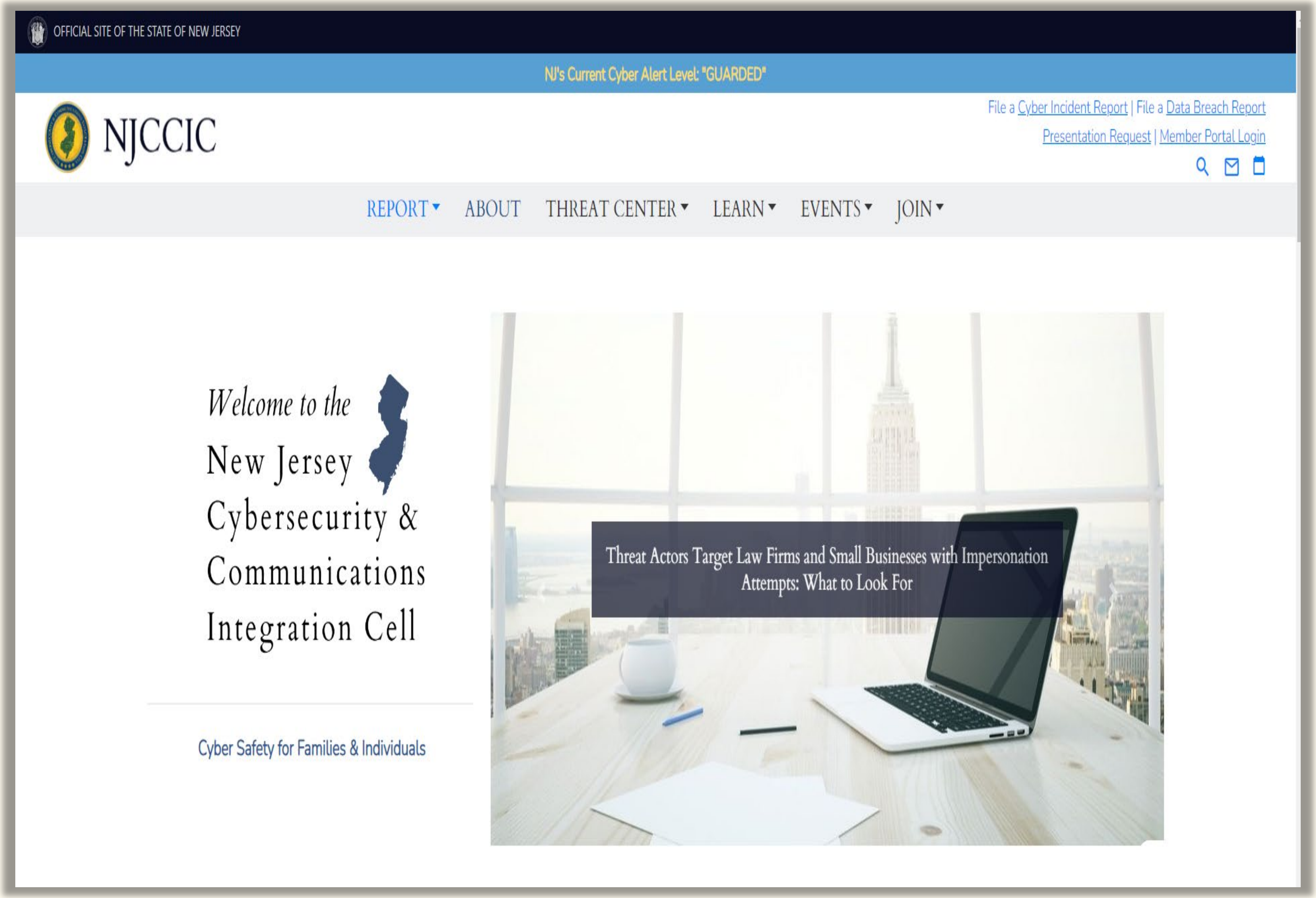
Implement: Cyber Attack Plan.

Conduct an Assessment: To ascertain if the Cyber-breached records and information may have had backups such as, Hardcopy, Optical disk or Microform that may be salvaged.

PL 2023, c.19: Contact the NJ Office of Homeland Security to report the Cyber Attack https://www.cyber.nj.gov/report **Incident Hotline**: 1-866-4-SAFE-NJ

Complete and Submit DORES-RMS Cyber Attack Records Report: For presentation before the State Records Committee (SRC).

NJ Cybersecurity & Communications Integration Cell (NJCCIC)



OFFICIAL SITE OF THE STATE OF NEW JERSEY

NJ's Current Cyber Alert Level: "GUARDED"

NJCCIC

File a Cyber Incident Report | File a Data Breach Report

Presentation Request | Member Portal Login

REPORT ▾ ABOUT THREAT CENTER ▾ LEARN ▾ EVENTS ▾ JOIN ▾

Welcome to the

New Jersey Cybersecurity & Communications Integration Cell

Cyber Safety for Families & Individuals

Threat Actors Target Law Firms and Small Businesses with Impersonation Attempts: What to Look For

Artificial Intelligence (AI)

AI Defined

Artificial Intelligence (AI): A computer system comprised of Computers and Machines that can perform complex tasks such as, reasoning, decision making, problem solving and learning acting similar to human intelligence on a scale that exceeds human function.

Learning is achieved through processing large amounts of data while identifying patterns and relationships through disciplines including computer science, data analytics and statistics, hardware and software engineering, linguistics, neuroscience, philosophy and psychology.

- **Machine Learning (ML):** A subset of **AI** and that uses data and algorithms to replicate how a human learns to quantitatively improve its accuracy.

- **Deep Learning:** A subset of **ML** that uses multilayered neural networks (Deep Neural Network) to simulate the complex decision-making function of the human brain.

- **Generative Artificial Intelligence (GAI):** A subset of AI that can **a**nalyze code, syntax, functions, words, grammar, semantics and context to constantly refine, rebuild and perfect itself.

- **Natural Language Processing (NLP):** The process of Speech Recognition and Synthesis, Question Answering, Information Retrieval in a human language format.

AI Applications & Strategies: the Good

Medical: *DaVinci Robot* Enhanced Surgical Procedures

Advanced Web Search Engines: Google Search

Recommendation Systems: Amazon, MAX and Netflix

Interaction via Human Speech: Siri, and Alexa

New Human-Machine: Interaction techniques

Robotics: Productivity enhancements

Government: Enhance processing times

Educational: Intelligent tutoring and adaptive learning tools

Generative & Creative Tools: ChatGPT, CoPilot, Gemini, Claude, AI Art & Music

Superhuman: Play and Analysis in Strategy Games

Cyber Incursions & Defense: Applications for Detection and Elimination

Climate Change: Advanced Strategies & Techniques

AI Applications & Strategies:
the Bad

Medical: Bad AI Data resulting in Misdiagnosis & Incorrect Procedure/Treatment

Human Visual & Speech: Perfect Impersonation

New Human-Machine Interaction Techniques: Replace Human involvement

Government: Warfare, Espionage, Control, Fake Data & Fake Information

Education: Replace Human Student-Teacher Classroom Learning Experience

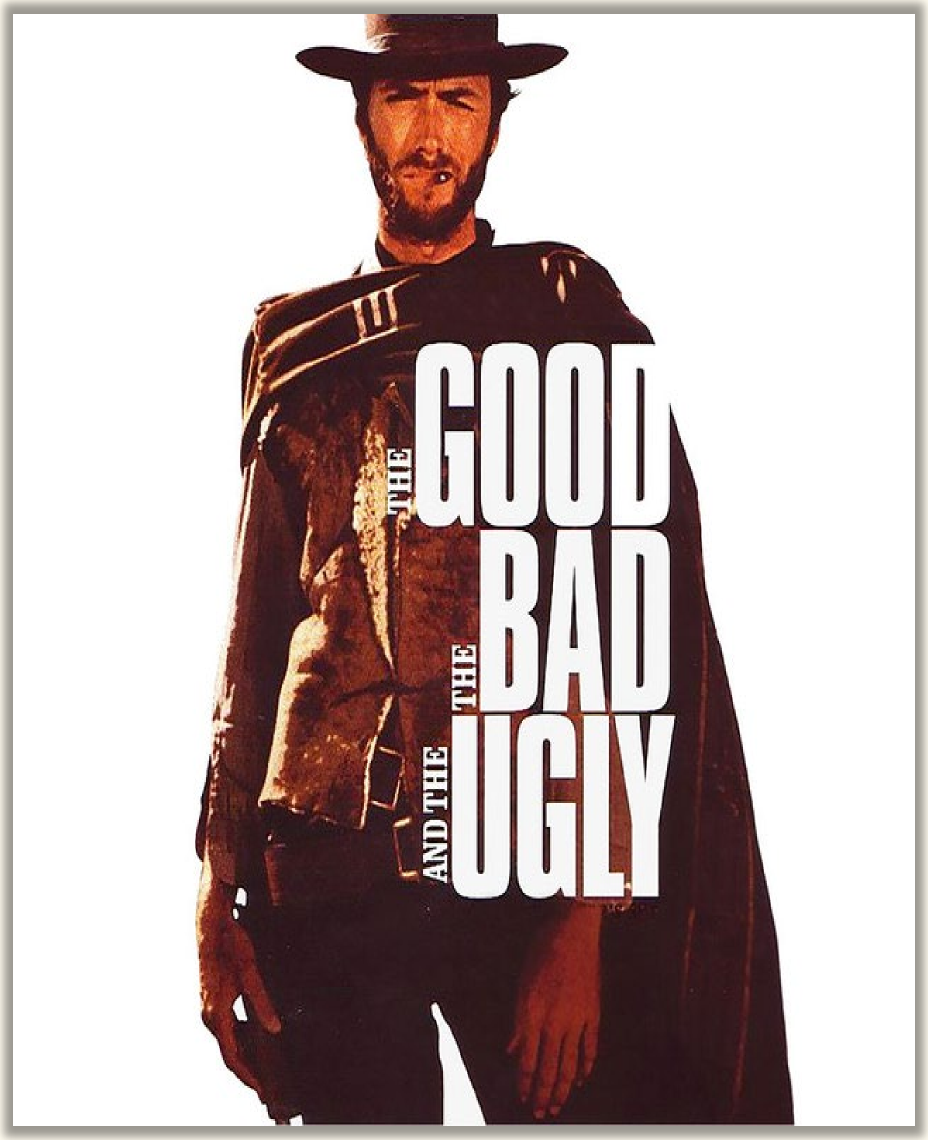
Übermensch, Super-man, Superhuman: “Terminator”?

War-gaming: Advanced Warfare Techniques and Strategies

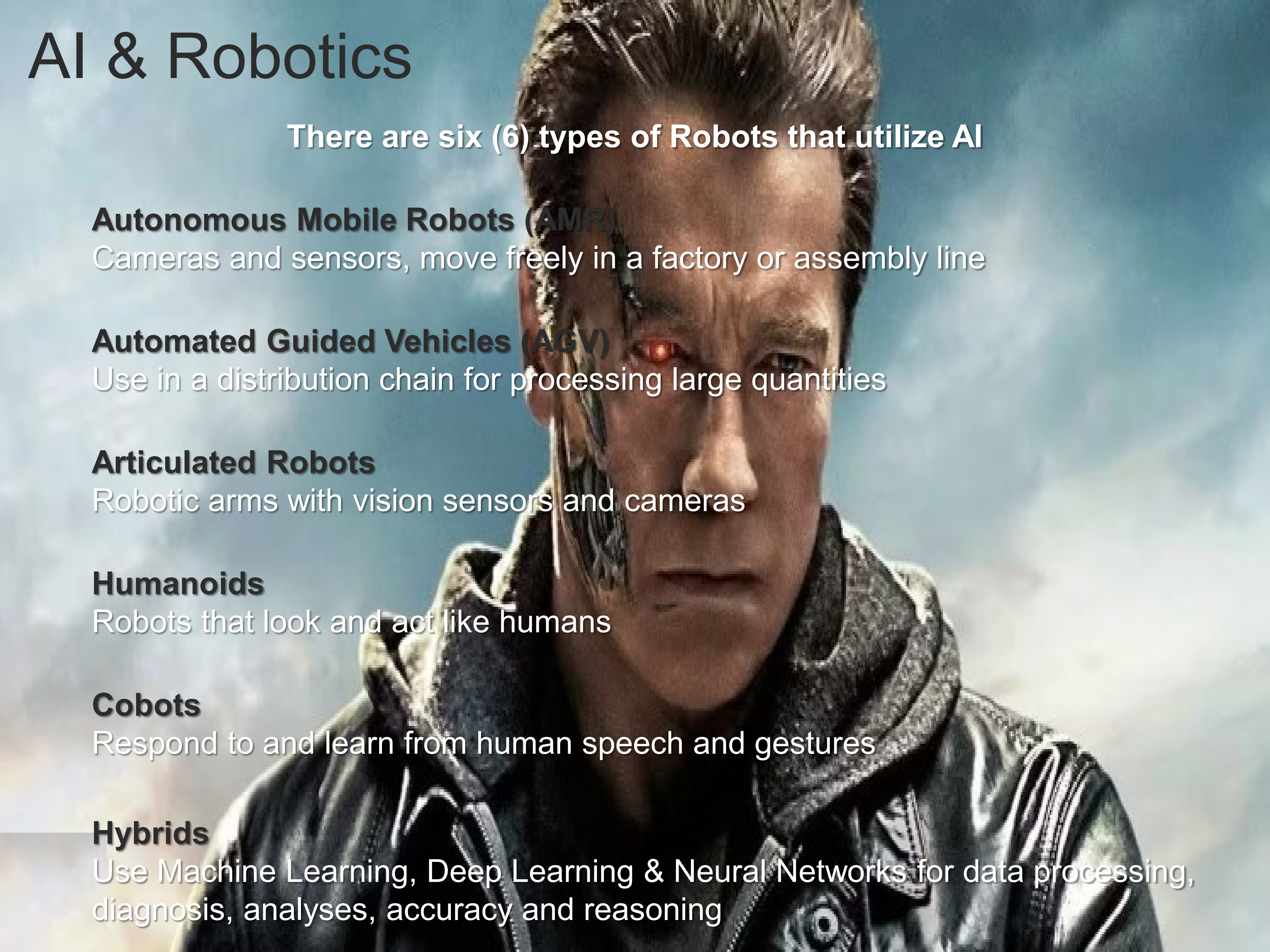
Workforce: Replace White Collar and Blue Collar Jobs

Global Control & Interaction: Distribute False Information

AI Applications and Strategies: and the Ugly



AI & Robotics



There are six (6) types of Robots that utilize AI

Autonomous Mobile Robots (AMR)
Cameras and sensors, move freely in a factory or assembly line

Automated Guided Vehicles (AGV)
Use in a distribution chain for processing large quantities

Articulated Robots
Robotic arms with vision sensors and cameras

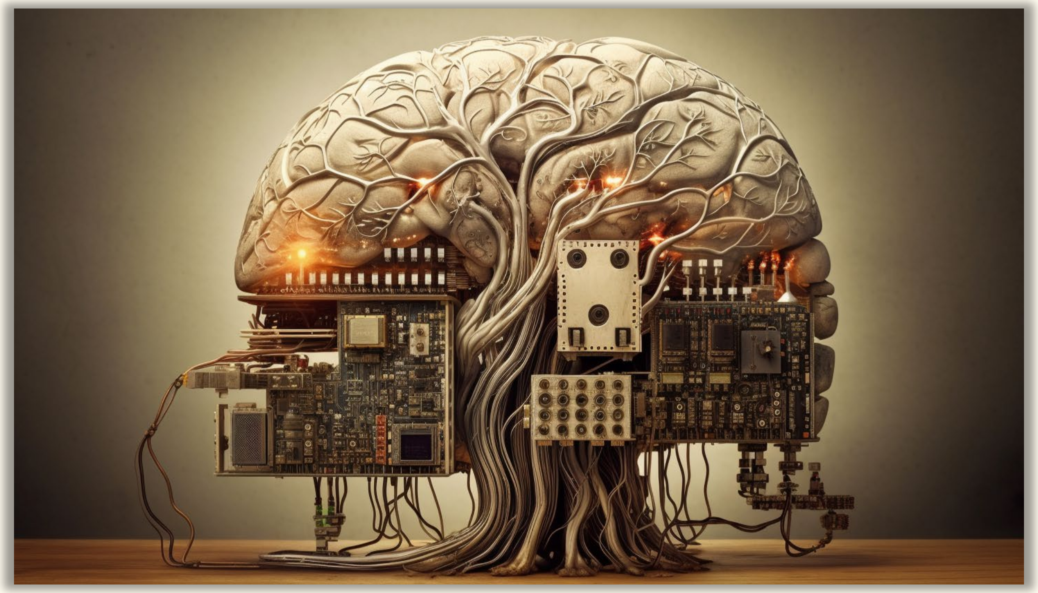
Humanoids
Robots that look and act like humans

Cobots
Respond to and learn from human speech and gestures

Hybrids
Use Machine Learning, Deep Learning & Neural Networks for data processing, diagnosis, analyses, accuracy and reasoning

AI & Ethics

The NEED for Government Regulations and Control to Prevent Misuse



Moral Compass for Emerging Tech & Innovation

Legal & Financial Ramifications

Maintaining Confidentiality

AI Threats & Ethical Risks

Fake Data & Information Distribution

AI Threat of Replacing Humans Jobs

An Overall Threat

AI & the Human Touch

AI is touted as “The Way of Life” to enhance processing time, quantity, accuracy and eliminate errors…

AI Needs a real flesh & blood Human Being to:

- Be part of the loop.
- Perform Decision Management
- Human introduction & oversight of standards, procedures, etc.
- Foster Effective Negotiations between individuals or groups.
- Ensure that no Bad Data is getting into the process. The IT adage still holds true: “Garbage in, Garbage out” → “Bad AI in, Bad AI out.”

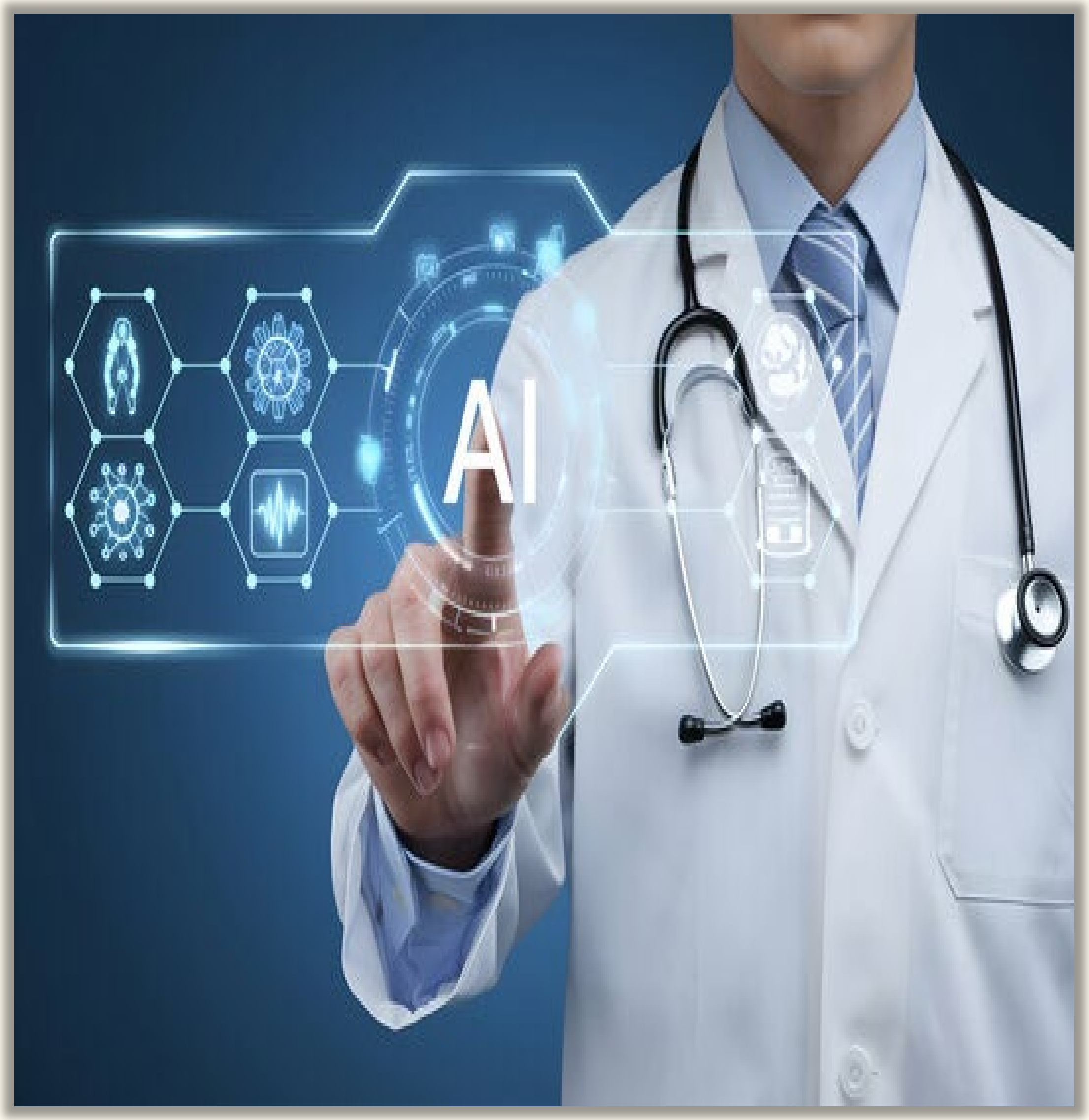
GLOBAL AREAS OF AI PROCESSING EFFICIENCY OR AI TAKE OVER?

Agencies & Institutions

Healthcare
Government
Financial Institutions
Education
Higher Education
Nonprofit Organizations
Religious Institutions
Business
Military

Operations & Services

High Tech
Telecommunications
Entertainment & Media
Construction & Engineering
Transportation & Logistics
Energy & Utilities
Retail
Manufacturing
Hospitality



Records & Information Management, OPRA and AI

A thorough and efficient Records and Information Management Program should be the foundation when implementing an AI Application. Public Agencies must continue safeguarding their Public Records and conducting **ongoing due diligence** on the part of the "Human Component" - Records Manager, IT, Legal, etc. pertaining to Data Retention, Disposition, Conversion, Preservation, Migration and Protection of the AI process:

Records Type

Medium

Routine Retention/Disposition

Proper Records Storage

Document Conversion

Disaster Prevention & Recovery

Business Continuity/COOP

Vital Records Preservation,

Applicable Federal & State Laws, Guidelines, etc.

Records & Information Management, OPRA and AI

Enhanced Knowledge Capture and Analysis for Information and Services: AI and Generative AI can search, retrieve, process and provide information at rapid speed and create reports, audio & video –

Customer Service Process: Enhancing customer response turnaround for information processing and delivery.

High Speed Data Search & Retrieval: Search and retrieval systems are able to understand queries and extract relevant information from structured and unstructured data sources quickly and accurately ex., OPRA Request Processing.

Data Governance: Data Analysis repositories and can identify PII, PHI and Confidential information providing guidelines for ethical use of information.

Data Compliance: Regulatory Compliance monitor and detect abnormalities, visual security, authentication which has the potential to reduce risk of data breaches.

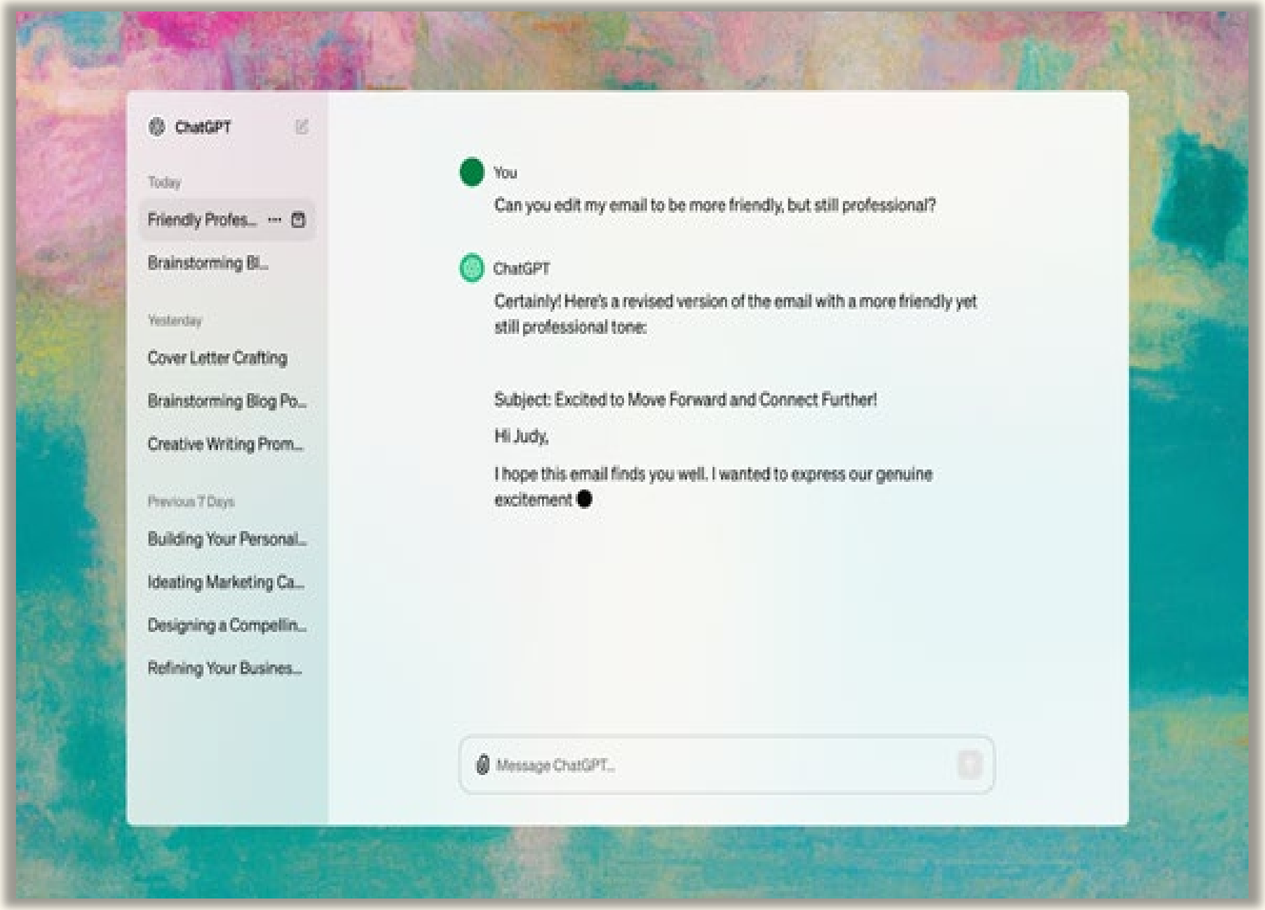
Consult DORES-RMS Guidelines for Records Retention & Disposition for AI/ML Systems

www.nj.gov/treasury/revenue/rms/pdf/BackgroundandGuidelinesonRetentionandDispositionPolicies.pdf

ChatGPT

ChatGPT (Chat Generative Pre-trained Transformer): Created by **Sam Altman** (Open AI) is a chatbot (a program that replicates human conversation) with Natural Language Processing for Human-like Communication and Exchange.

Calculate Math Problems
Write an Essay
Create an Image
Create an App
Write Code
Write a Resume
Write Excel Formulas
Summarize Content
Write a Cover Letter
Create Charts and Tables
Browse the Web
Analyze a PDF
Digitize Handwriting



You

Can you edit my email to be more friendly, but still professional?

ChatGPT

Certainly! Here's a revised version of the email with a more friendly yet still professional tone:

Subject: Excited to Move Forward and Connect Further!

Hi Judy,

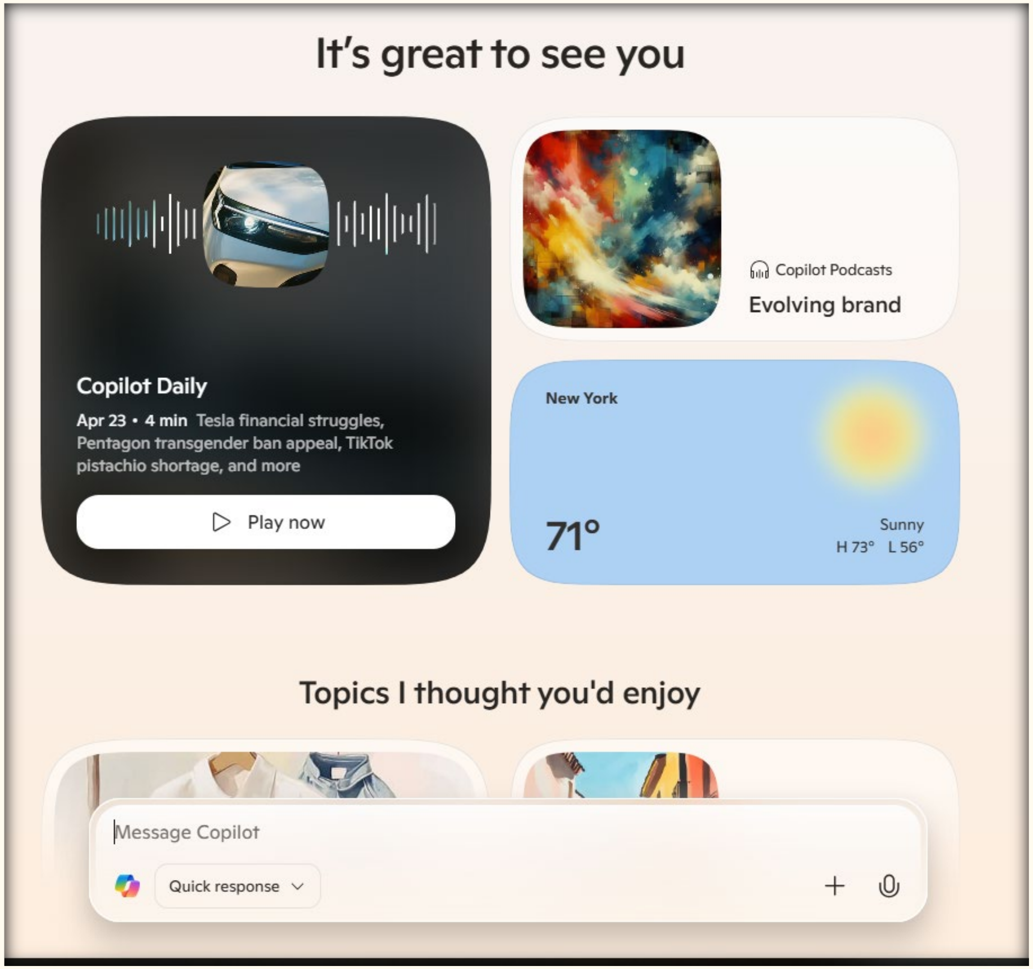
I hope this email finds you well. I wanted to express our genuine excitement ●

Microsoft Copilot: “Your AI Companion”

Copilot: Created by Microsoft, is a chatbot (a program that replicates human conversation) with Natural Language Processing for Human-like Communication and Exchange.

Touted by Microsoft as, “Your AI companion to inform, entertain, and inspire. Get advice, get feedback, and straightforward answers.”

- **Write a draft**
- **Get advice**
- **Learn something new**
- **Create an image**
- **Make a plan**
- **Brainstorm ideas**
- **Practice a language**
- **Take a quiz**
- **Write a Cover Letter**
- **Create Charts and Tables**



It’s great to see you

Copilot Daily

Apr 23 • 4 min Tesla financial struggles, Pentagon transgender ban appeal, TikTok pistachio shortage, and more

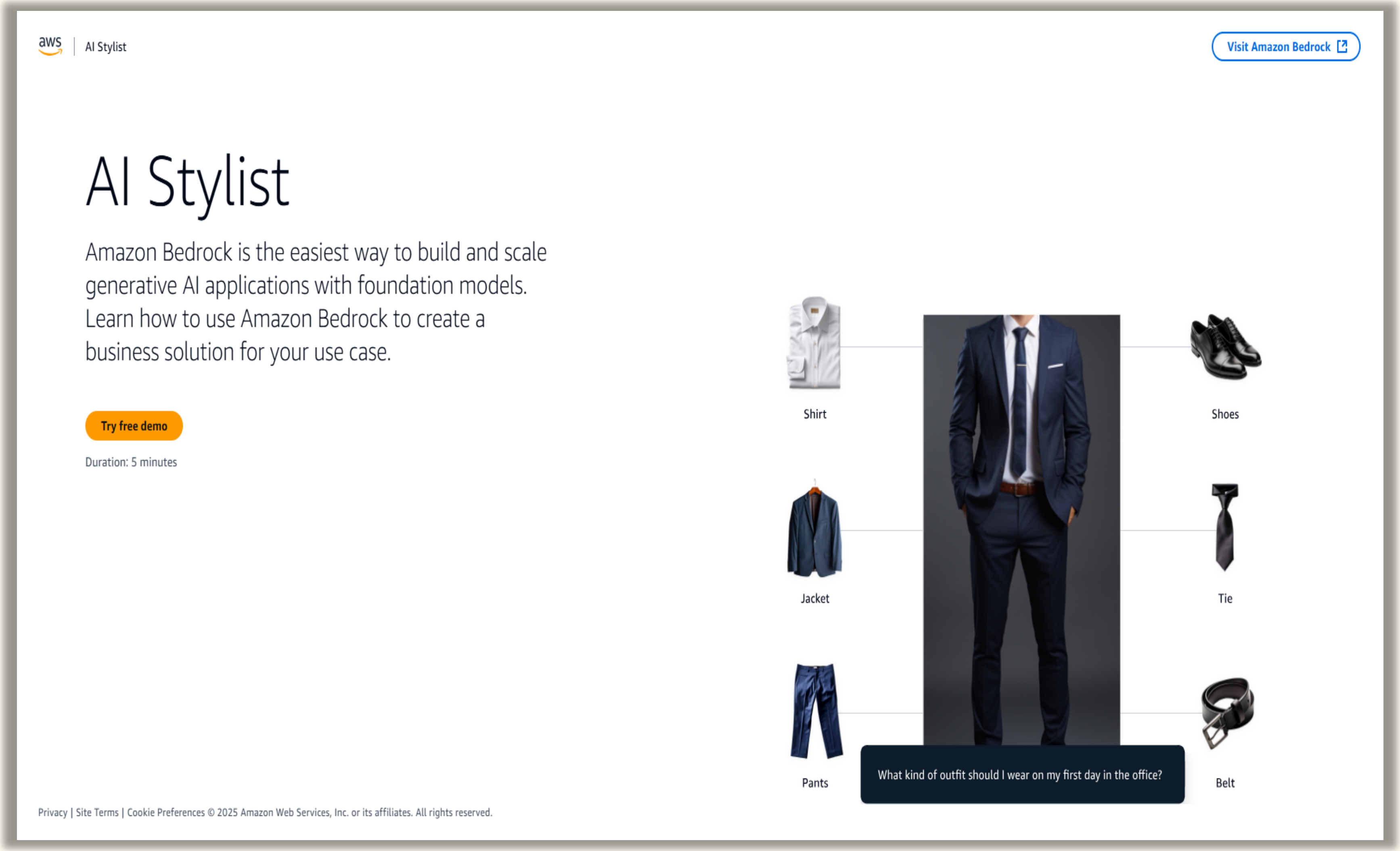
Copilot Podcasts

Evolving brand

Topics I thought you'd enjoy

Amazon Bedrock

Amazon Bedrock is a an AI application where you can choose a wide range of foundation models and capabilities to build generative AI applications with security, privacy, and responsible AI.



aws | AI Stylist

Visit Amazon Bedrock

AI Stylist

Amazon Bedrock is the easiest way to build and scale generative AI applications with foundation models. Learn how to use Amazon Bedrock to create a business solution for your use case.

Try free demo

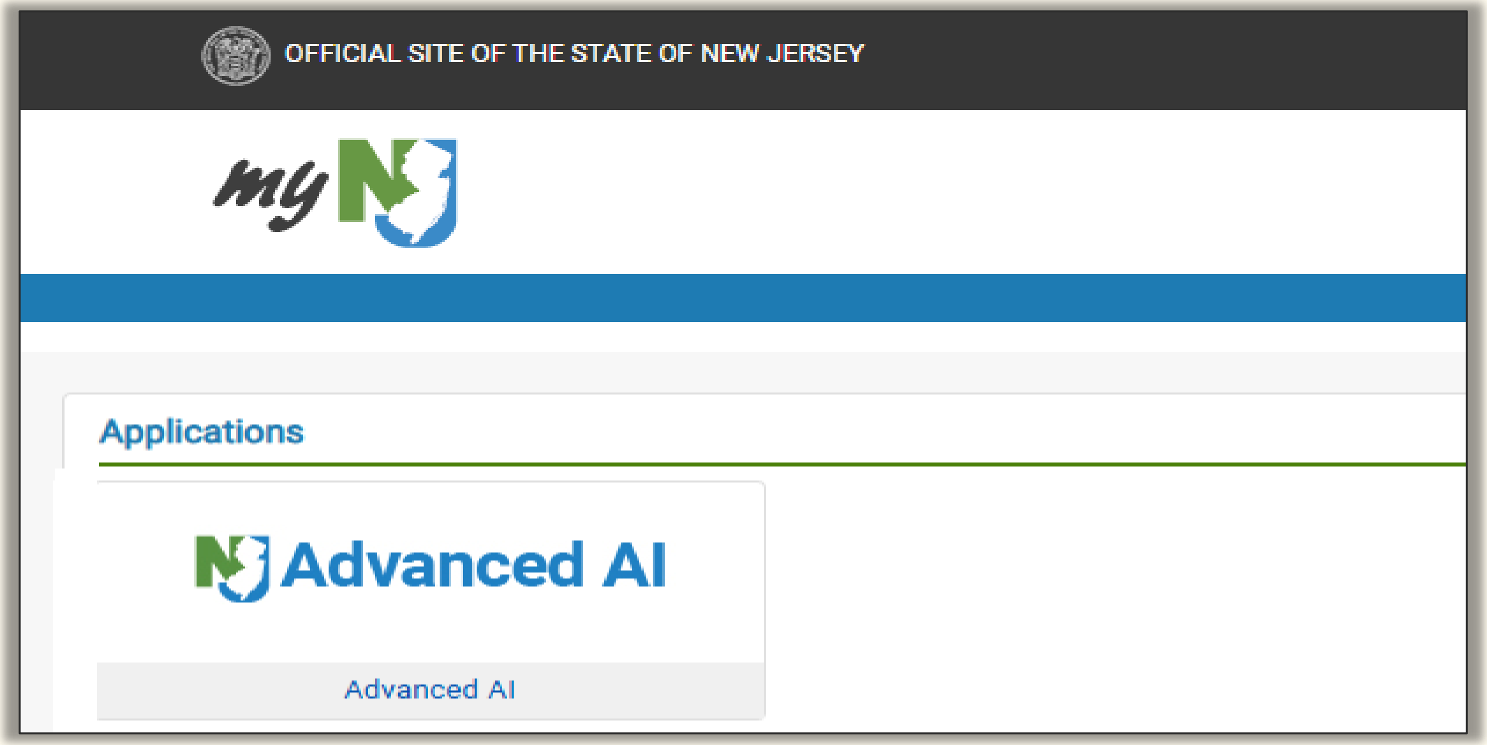
Duration: 5 minutes

What kind of outfit should I wear on my first day in the office?

Privacy | Site Terms | Cookie Preferences © 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved.

NJ Advance AI

NJ Advances AI: Is a NJ State Government internal generative artificial intelligence chatbot …. Using Amazon Bedrock.



OFFICIAL SITE OF THE STATE OF NEW JERSEY

Applications

Advanced AI

Advanced AI

Department of the Treasury
Division of Revenue and Enterprise Services
Records Management Services
PO Box 661   Trenton, NJ 08625
609-292-8711
www.nj.gov/treasury/revenue/rms/contact.shtml

Thank
you