Records Security in the Virtual World

Elizabeth Hartmann

Karen A. Perry

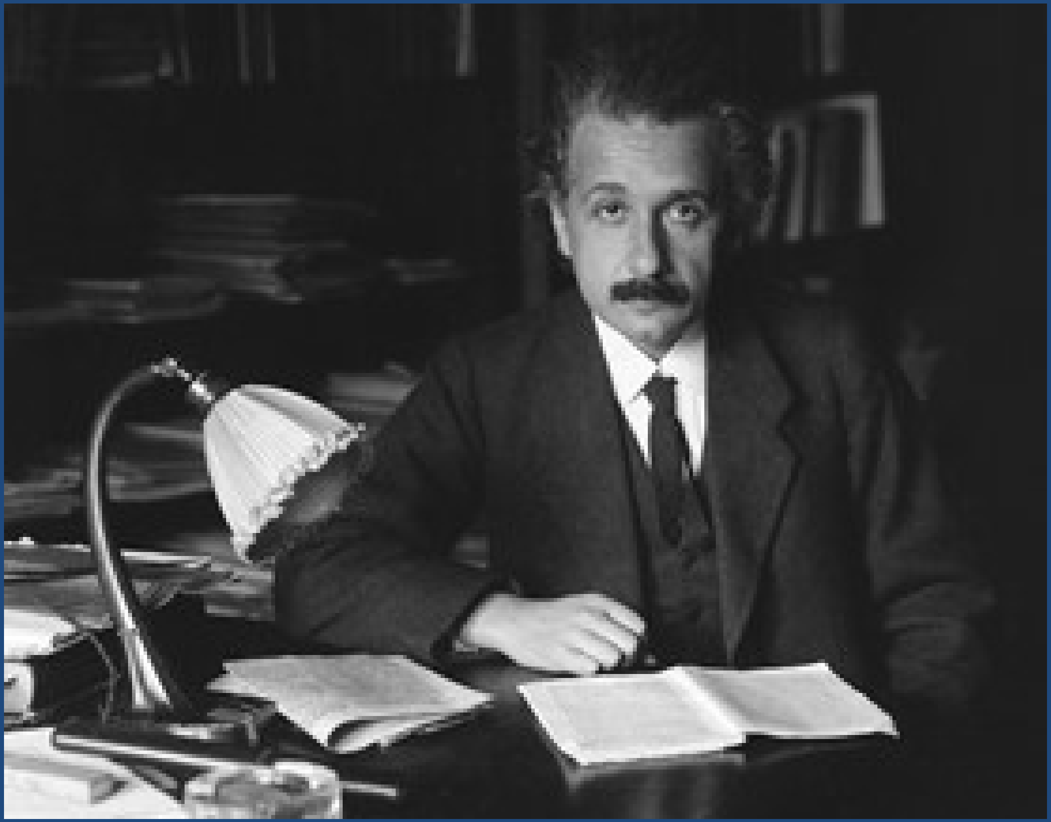
Department of the Treasury

Division of Revenue and Enterprise Services

Records Management Services

2021

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



Albert Einstein and the *Laws of Physics,*
“Nothing can exist in a vacuum” ...
and Government is no exception.

Records Security in the Virtual World

Traditionally, New Jersey, Public Agencies consist of: State, County and Municipal Agencies; Boards; Authorities & Associations; School Districts and Colleges; Public Healthcare Facilities; etc. Their Constituency Base consisted of:

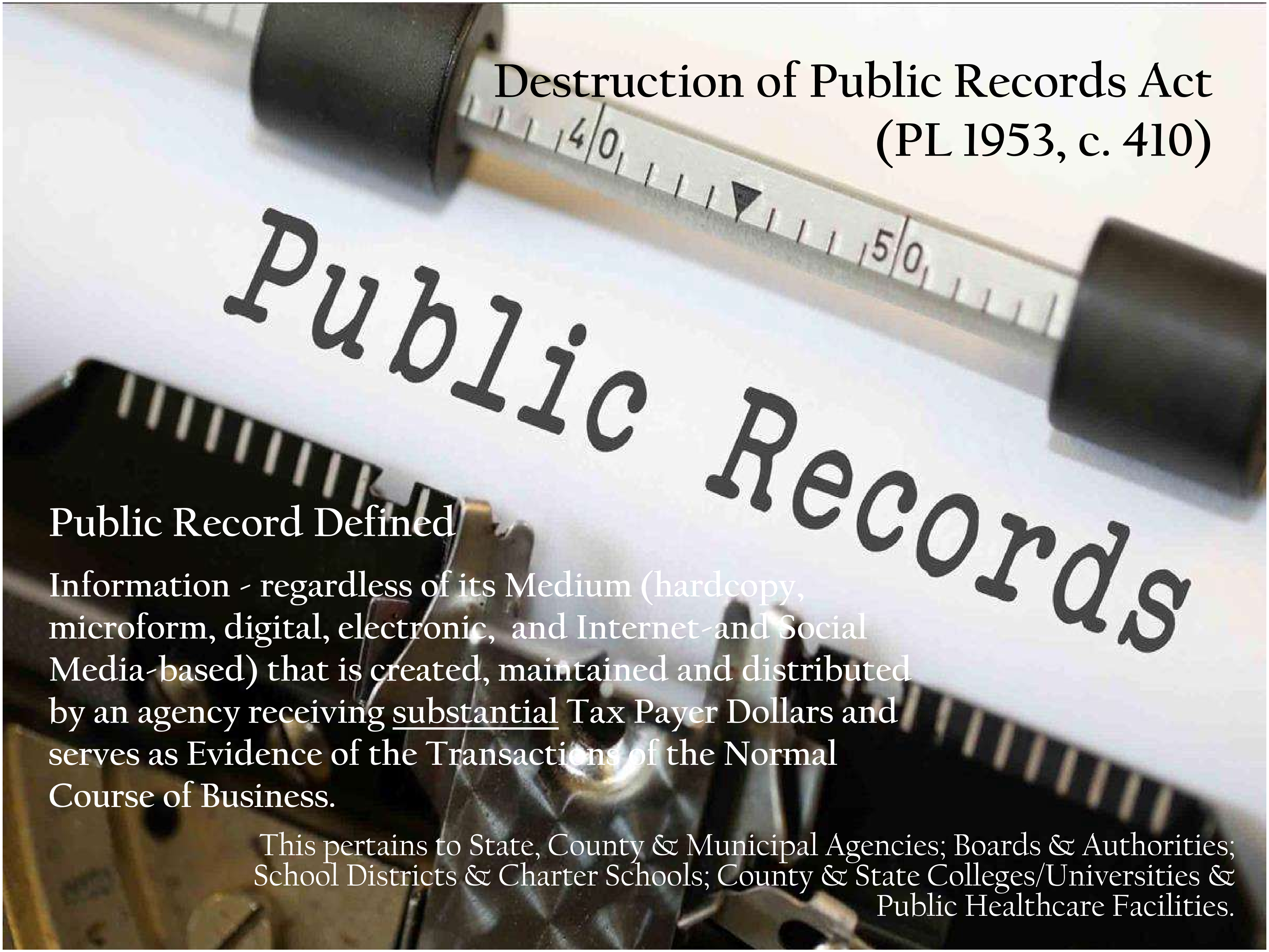
- Federal Agencies
- Government Agencies from other States
- Private Sector
- Financial Institutions
- The Media
- The Public at Large

Interactions with their Constituents usually resulted in the exchange of varying amounts of public information in hardcopy, microform, tape and disk format.

However, their Constituency has expanded to include the International Arena resulting in a global exchange of even larger quantities of public information now being transmitted in hardcopy, electronic and/or digital format which is stored via the Internet, Social Media and the Cloud. Thus compounding electronic records concerns in the areas of:

- Security,
- Regulatory Compliance
- Access, Retention, Preservation and Disposition

Destruction of Public Records Act
(PL 1953, c. 410)



Public Record Defined

Information - regardless of its Medium (hardcopy, microform, digital, electronic, and Internet-and Social Media-based) that is created, maintained and distributed by an agency receiving <u>substantial</u> Tax Payer Dollars and serves as Evidence of the Transactions of the Normal Course of Business.

This pertains to State, County & Municipal Agencies; Boards & Authorities; School Districts & Charter Schools; County & State Colleges/Universities & Public Healthcare Facilities.

Open Public Records Act (OPRA) PL 2001, c. 404, NJSA 47:1A et seq.

The Open Public Records Act (OPRA) PL 2001, c. 404, NJSA 47:1A et seq. :

- Provides that Public Records regardless of their medium (hardcopy, microform, tape, disk, digital and electronic) and where it resides (hand-held, eye-readable, machine-readable, Internet, Social Media and the Cloud) must be made accessible to the public in *most* cases
- Established the position of Custodian of Public Record for public agency record-keepers
- <u>Personal</u> Financial & Legal Accountability for intentional denial of public records access

However, the degree of a record's accessibility and its medium does *not* determine whether a record is Public or Private. For example, classified military records concerning the National Defense are Public Records, but they are *not publicly accessible* due to reasons of National Security. 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 which:

- Responds to inquiries and complaints about OPRA from the Public and Records Custodians
- Issue public information and training about OPRA
- Issues advisory opinions on public records accessibility or exemption
- Provides mediation and resolution of disputes about public records

Open Public Records Act (OPRA) PL 2001, c. 404, NJSA 47:1A et seq. – Access

OPRACentral
OPRA|New Jersey
Open Public RecordsAct

OPRA PUBLIC RECORDS REQUEST for ACCESS to GOVERNMENT RECORDS

An OPRA Request for Information verifies what documents have been requested, the medium in which they were requested and that they have been supplied within the specified time limits of the request.

- Immediate Access – **Means Immediate Access!**

  Budgets, Bills, Vouchers, Contracts, and Employee Salary & Overtime Information

- Seven (7) Business Days Access

  Non-Immediate access records and Offsite-Stored Records must be supplied within a seven (7) Business Day time period.

EXTENSION of TIME for REQUEST for ACCESS to GOVERNMENT RECORDS

If the Custodian of Public Record *cannot* fulfill the request within these Time Periods, a written *Extension of Time* with an explanation, must be submitted within Seven (7) Business Days to the Requestor.

Open Public Records Act (OPRA) PL 2001, c. 404, NJSA 47:1A et seq. – Government Records Council

New Jersey Government Records Council

New Jersey Government Records Council
P.O. Box 819
Trenton, NJ 08625-0819
Phone: (609) 292-6830
Fax: (609) 633-6337
Toll-Free 1-(866) 850-0511
E-Mail: Government.Records@dca.nj.gov
Website: http://www.nj.gov/grc

Records Custodians and the Law:
Litigation Hold Order – Electronic Data

Records Custodians and the Law: Litigation Hold Order – Electronic Data

For Discussion Purposes Only

Consult With Legal Advisors When Dealing With Litigation Hold Orders

SAMPLE

<date>

TO: <individual and/or custodian>

FROM: <issuing office>

SUBJECT: <subject or nature of the matter>

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

<Agency> has received the above-captioned complaint and a copy is attached. We have identified you as a <custodian or individual> who may have potentially relevant paper records (e. g. memoranda, letters, pictures) or electronically stored information (e. g. e-mails, other electronic communications such as word processing documents, spreadsheets, databases, calendars. telephone logs, Internet usage files and network access information) or authority over such records.

You must immediately take every reasonable step to preserve this information until further notice.

Your failure to do so could result in significant penalties against us.

Records Custodians and the Law: Litigation Hold Order continued

While your obligation to preserve all forms of information is the same, we specifically bring to your attention the need to take action to preserve e-mail and other electronic communications, because there may be automated processes which will delete your e-mail if you take no action and for many individuals the deletion of e-mail is a routine practice. You should take immediate action to store any relevant e-mails in a separate folder or storage area for this potential litigation.

For paper documents and other types of electronically stored information, to the extent that it will not interfere with your ongoing work, you should take action to segregate those materials. In the case of electronically stored information, you should leave it in its current location, but may make a copy for a separate folder or storage area related to the potential litigation. In the case of paper records, you may either move them to a separate location, noting the files from which each record was retrieved, or make copies of the records.

This is a continuing obligation. So if you discover, create or receive relevant documents or electronically stored information in the future you should similarly take action to preserve those materials. You should preserve all relevant documents and electronically stored information in accordance with these instructions until you are affirmatively advised that you are no longer obligated to do so. Attached is an acknowledgement that you have received this memorandum. You should return it to me within five days of your receipt. If you have any questions regarding these instructions please call <contact> immediately at (___) _______. Again, it is imperative that you take immediate action in accordance with these directions.

Records Custodians and the Law:
Litigation Hold Order Acknowledgement of Receipt

Acknowledgement of Receipt of “Litigation Hold” Instructions

RE: <subject or matter>

I, <individual or custodian>, acknowledge that I have received the <date of notice> notice regarding the above-captioned matter from <representative> advising me of my obligation to conduct a reasonable search for any documents, whether stored in hard copy or electronically, that may be relevant to the matter and to take reasonable steps to ensure the preservation of those documents.

I understand the instructions contained in the memorandum.

___________________________.

Signature

____________________________ . Date: ________________________

Name

Note: If you do not understand the instructions, prior to completing this acknowledgement, you should contact <representative> at <___>-<___-____> with any questions you may have regarding either 1) what documents might be relevant to the above matter or 2) what actions you are reasonably expected to take in order to conduct a reasonable search for and preserve any documents, whether stored in hard copy or electronically, that may be relevant to the above matter.

Records and Information Management (RIM)

Records and Information Management (RIM)

Why?

- Documents an Agency’s History
- Protects Vital, Confidential and Security Records
- Provides Federal & State Litigation and e-Discovery Support
- Provides Federal & State Audit & Program Review Compliance
- Provides Federal & State Regulatory Compliance
- Fosters OPRA Public Records Access

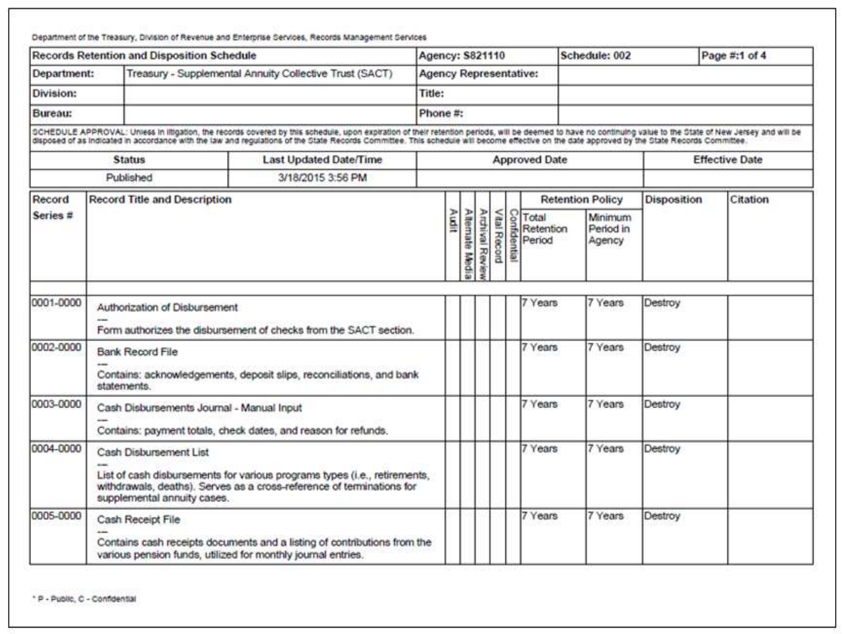
Records Retention Schedules

Records Management Services

Mandated by the New Jersey Public Records Laws – Records Retention Schedules are a detailed listing of the records maintained by an agency and the *Minimum* Legal and Fiscal time periods they must be retained.

Records Retention Schedules address:

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



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

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

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

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

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

* P - Public, C - Confidential

Records Disposal – Regulatory Compliance

In accordance with the New Jersey Public Records Laws, a *Request & Authorization for Records Disposal* must be submitted to Records Management Services for legal authorization for disposal *before* records can be destroyed.

The records disposal authorization:

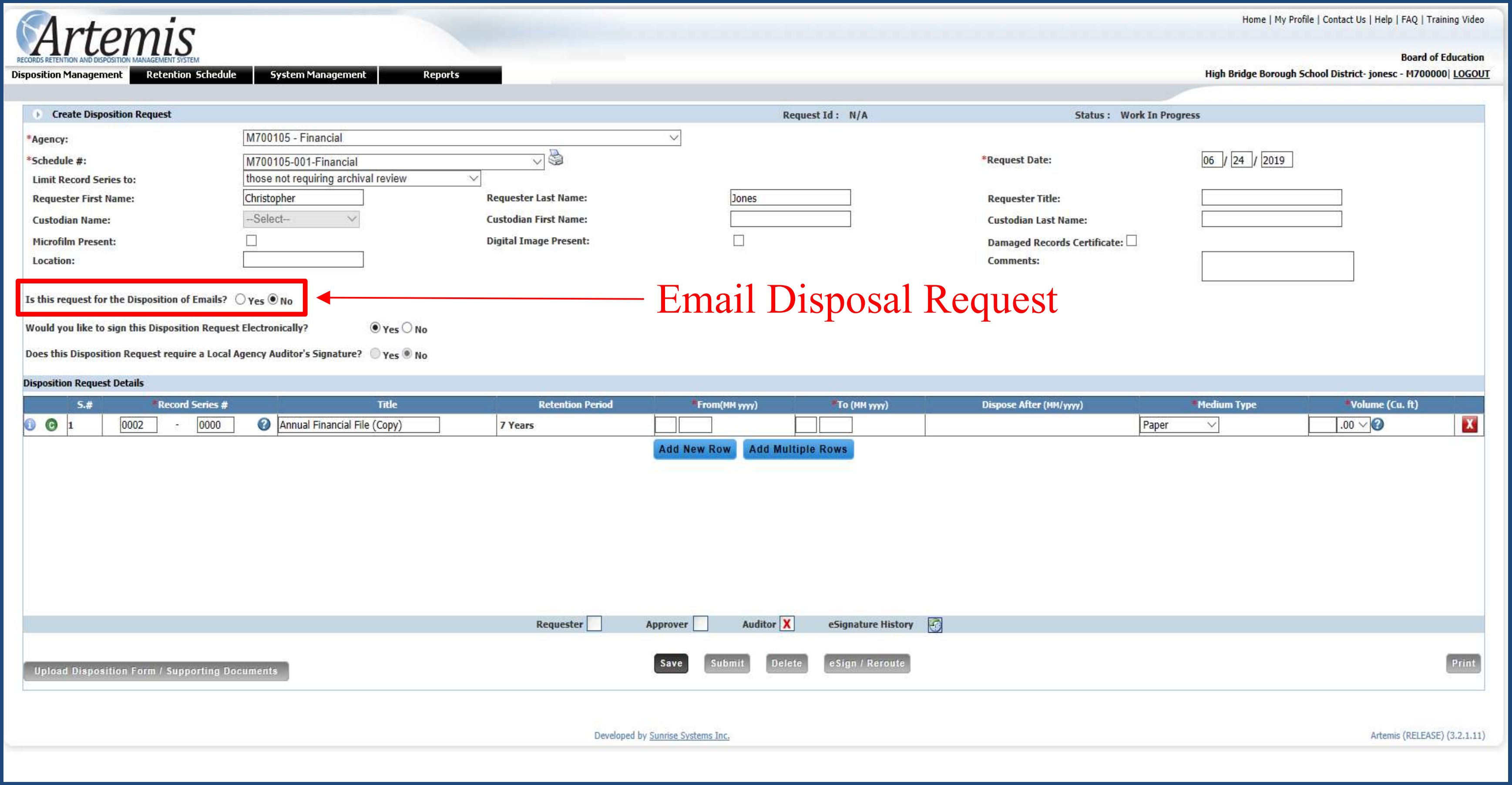
- Mitigates OPRA Liabilities
- Removes Legal Liabilities
- Removes Fiscal Liabilities
- Fosters Cost Effective Space -Saving
- Foster a Safe Workplace Environment
- Identifies Confidential Records
- Identifies Archival Records for Preservation

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 & Check Status - Pending, Approved, Denied,
- Produce Authorized Records Disposal Requests for OPRA Requests, and
- Create Reports - Records Retention & Disposal.

Records Disposal – Artemis & Email


Artemis
RECORDS RETENTION AND DISPOSITION MANAGEMENT SYSTEM
Disposition Management
Retention Schedule
System Management
Reports
Home | My Profile | Contact Us | Help | FAQ | Training Video
Add New Row
Add Multiple Rows
Upload Disposition Form / Supporting Documents
Save
Submit
Delete
eSign / Reroute
Print

Board of Education

High Bridge Borough School District- jonesc - M700000| LOGOUT

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

*Agency:	M700105 - Financial				
*Schedule #:	M700105-001-Financial			*Request Date:	06 / 24 / 2019
Limit Record Series to:	those not requiring archival review				
Requester First Name:	Christopher	Requester Last Name:	Jones	Requester Title:	
Custodian Name:	--Select--	Custodian First Name:		Custodian Last Name:	
Microfilm Present:	□	Digital Image Present:	□	Damaged Records Certificate: □	
Location:				Comments:	

Is this request for the Disposition of Emails? ○ Yes ● No

Email Disposal Request

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

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

Disposition Request Details

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

Requester □ Approver □ Auditor ☒ eSignature History

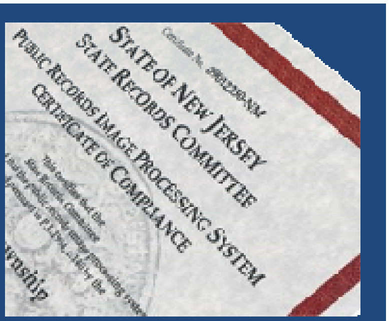
Developed by Sunrise Systems Inc.

Artemis (RELEASE) (3.2.1.11)

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

Records and Information Management Alternatives

Records and Information Management Storage Alternative – Imaging



State of New Jersey
State Records Committee
Public Records Image Processing System
Certificate of Compliance

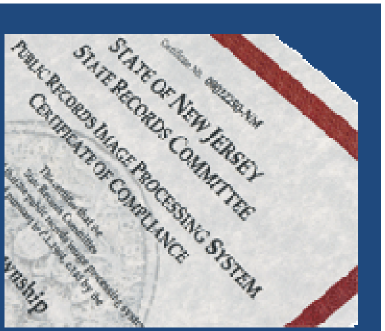
As per PL 1994, c. 140, the State of New Jersey allows for the replacement of hardcopy public records with digital images. The State Records Committee and Records Management Services issue initial imaging system certification to an agency, for an in-house or outsourced imaging application, and annual imaging system certification renewals.

The basic documents required for obtaining Imaging Certification from the State Records Committee and Records Management Services include:

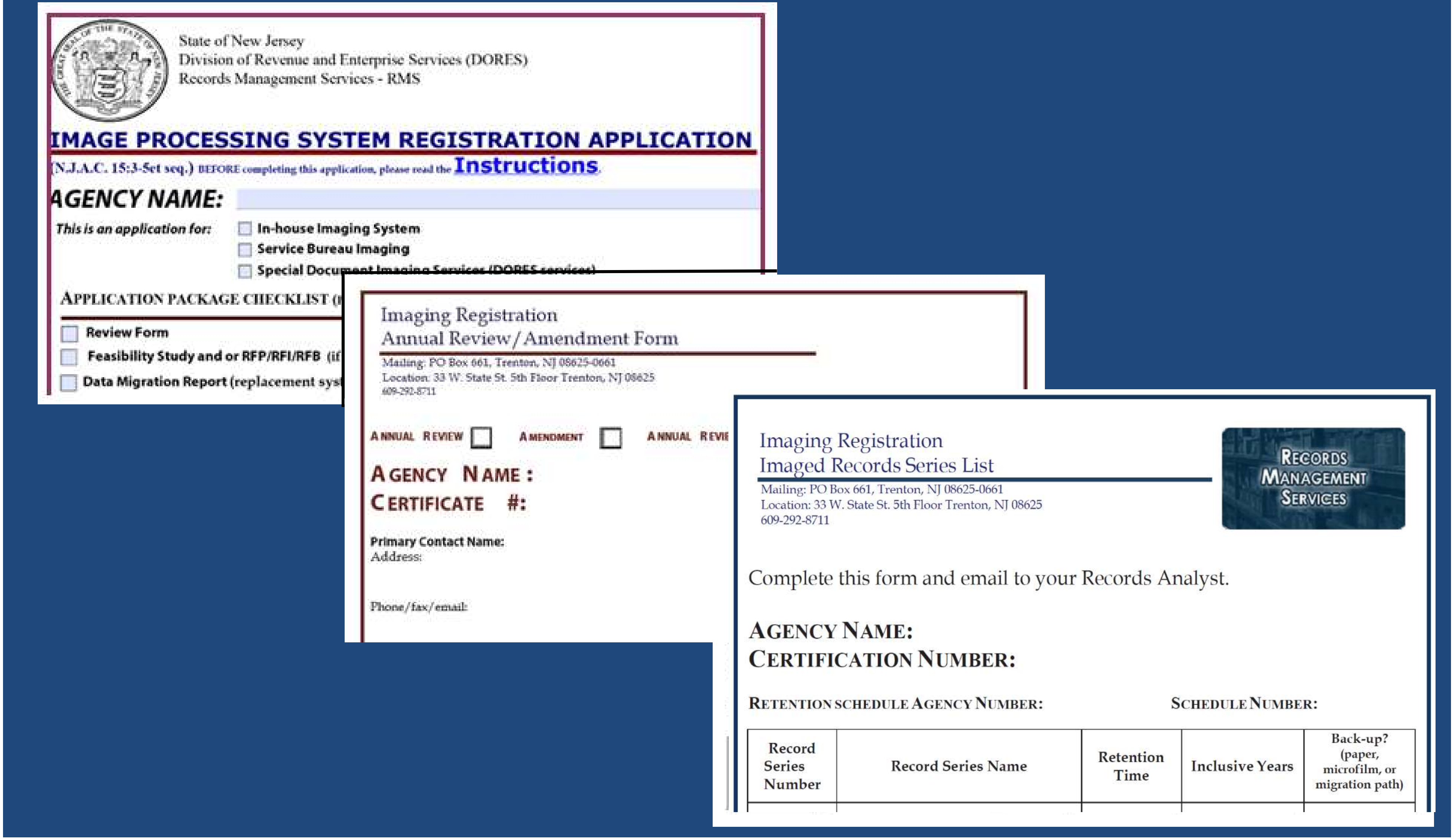
- *Image Processing System Registration Application* includes required documents such as:
  - Scanning Policy and Procedures
  - Disaster Prevention and Recovery
  - Data Migration Path
  - Feasibility Study
  - RFP/RFI/RFB
  - Vendor Detail
  - Imaged Records Series List

- *Annual Review/Amendment* includes required documents such as:
  - Scanning Policy and Procedures
  - Disaster Prevention and Recovery
  - Data Migration Path
  - Imaged Records Series List

Records and Information Management – Imaging continued



STATE OF NEW JERSEY
STATE RECORDS COMMITTEE
PUBLIC RECORDS IMAGE PROCESSING SYSTEM
CERTIFICATE OF COMPLIANCE



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 (

□ Review Form
□ Feasibility Study and or RFP/RFI/RFB (if
□ Data Migration Report (replacement syst

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 REVIE

AGENCY NAME:
CERTIFICATE #:

Primary Contact Name:
Address:

Phone/fax/email:

Imaging Registration
Imaged Records Series List

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

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)

Records Management Guidelines for Remote Work Settings

Records Management Guidelines for Remote Work Settings

As government agencies strive to address the challenges posed by the COVID-19 pandemic, social distancing continues to be a prominent factor in combating the spread of the virus. In this connection, many agencies promote expanded remote work programs -- working from home and other off-site locations, to reduce the number of employees in traditional office spaces. This increases the number of remote locations in which public records are received, produced, stored, distributed and used. By way of background, State law defines a public record as being any information that a public agency generates or receives in the transaction of its official duties. This is true regardless of the medium used to store the information (for example, electronic devices, paper or microfilm).

Public employees who receive, generate or store public records while working in remote settings have an obligation to manage these records properly. This means that they must be attentive to records retention requirements, basic information security measures, public records access provisions like the Open Public Records Act (OPRA) and any applicable access restrictions in the case of records that are classified as sensitive, confidential or private. This document is designed to provide government employees with quick and practical guidelines for managing public records in remote settings. While not comprehensive, the guidelines touch upon practical actions that employees can take to ensure they are following a basic records management regime in remote work settings.

Key Contacts The contact for the records management topics covered below is the New Jersey Division of Revenue and Enterprise Services' Records Management Services Unit (RMS): 609-777-1020 or 609-292-8711. Guidance on preservation of permanent and historical records can be obtained from the State Archives: 609-633-8304 or 609-292-6260. Organizational Sources of Support and Guidance Employees should look to their executive management teams for overall guidance on records management responsibilities. In addition, depending upon the structure of the government agency, the following functions may be able to provide guidance on records management and related topics:

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

Records Management Guidelines for Remote Work Settings

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

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

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

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

Records Management Guidelines for Remote Work Settings

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

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

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

7. Employ basic security measures to protect personal home computing facilities that connect to work systems. Protecting home computing facilities (for example, lap top computers and routers) helps to keep both your private information and public records safe from unauthorized access, use, dissemination and/or destruction. The National Security Agency (NSA) publishes useful guidelines for protecting your home computing facilities. Some of the NSA's recommended actions include:

Records Management Guidelines for Remote Work Settings

7. continued.

a. Keeping your operating system up to date.

b. Using up to date security software including firewall, anti-malware, anti-virus, anti- phishing and safe browsing software.

c. Disconnecting external storage and printing devices when not in use.

d. Turning off computing devices when not in use.

e. Using strong, unique and hard-to-guess passwords on your computing devices and Internet router.

f. Keeping your browser software up to date.

g. Limiting the use of the Administrator account on your home computer(s) by creating and using a non-Administrator account for daily activities (the Administrator account gives elevated privileges to system resources and malware can use these privileges to compromise your computer).

h. Practicing safe online behavior – for example:

i. Do not use open, unprotected networks such as those found in hotels and public spaces.

ii. Do not log in from overseas locations without the express approval of your agency.

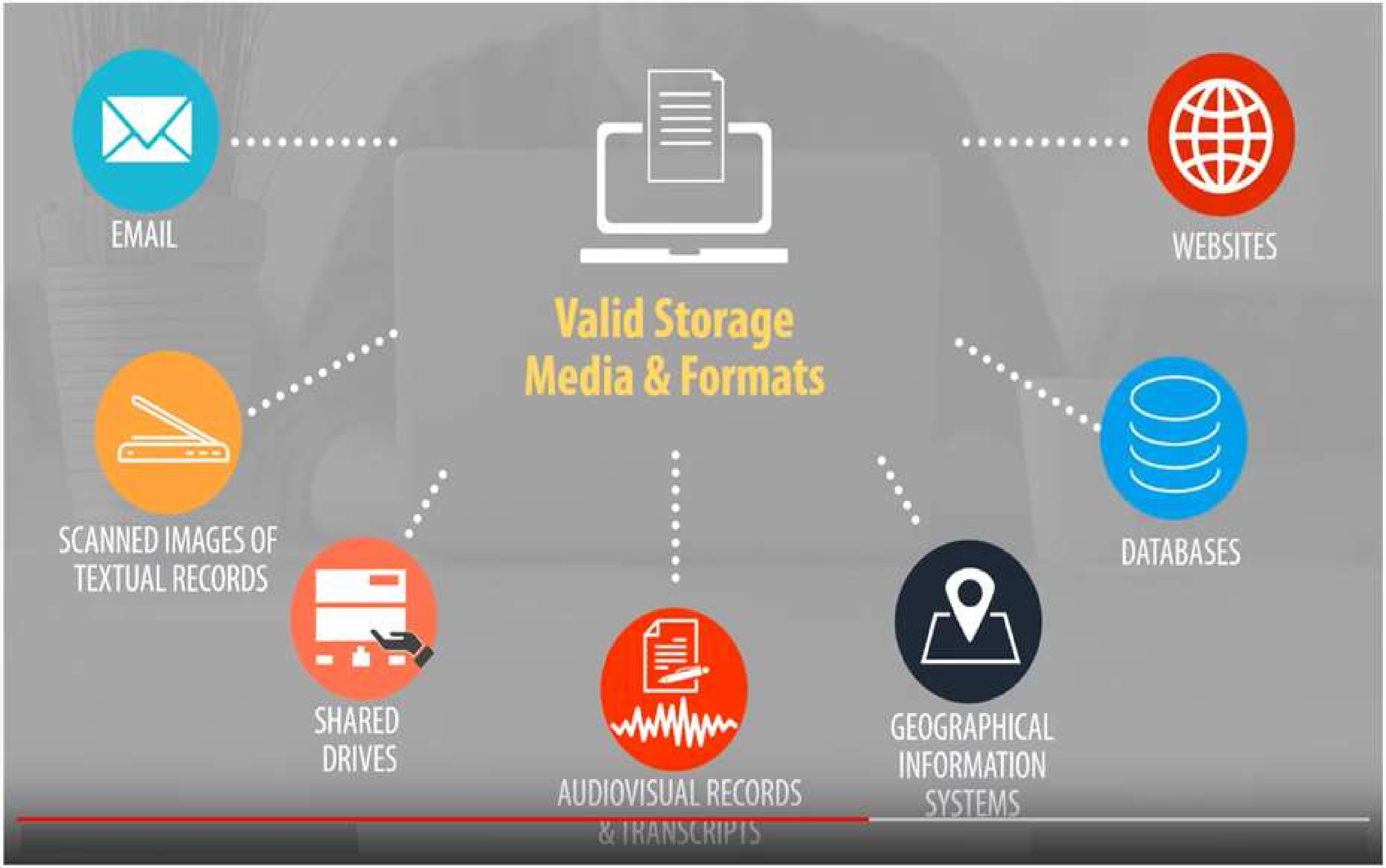
iii. Do not open attachments or links in unsolicited emails;

iv. Do not open emails from unknown sources or emails that look suspicious; v. Verify unfamiliar web sites by searching for them via an Internet search engine (before visiting them); and vi. Do not visit sites with known security or reputational issues.

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

ELECTRONIC RECORDS

Electronic Records


EMAIL
Valid Storage Media & Formats
WEBSITES
SCANNED IMAGES OF TEXTUAL RECORDS
DATABASES
SHARED DRIVES
AUDIOVISUAL RECORDS & TRANSCRIPTS
GEOGRAPHICAL INFORMATION SYSTEMS

Electronic Records Storage

Fixed (Stand Alone) Storage

- **Disk Backup** – quick access and can hold large amounts of data, can be used for disaster recovery if the server is placed offsite.

Virtual Storage

- **Cloud-based Computing** – 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

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.

Cloud-based
Storage

Guidelines for Cloud-based Records Storage

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

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

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

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

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

Guidelines for Guidelines for Cloud-based Records Storage continued

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

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

The contact for the records management topics covered below is the New Jersey Division of Revenue and Enterprise Services' Records Management Services Unit (RMS): 609-777-1020 or 609-292-8711.

Guidance on preservation of permanent and historical records can be obtained from the State Archives: 609-633-8304 or 609-292-6260 Guidelines

Guidelines for Guidelines for Cloud-based Records Storage continued

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

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

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

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

This can be somewhat complicated. Cloud facilities store a wide variety of records using various file formats including electronic mail, electronic documents (for instance, word processing and spreadsheet formats), presentations, social media posts, chats/text messages, audio-visual sessions and databases. In many cases, a direct mapping of Cloud storage content to records series will prove challenging. This has been the case historically for electronic mail and databases. For concepts on electronic mail retention scheduling see the State Records Manual and the Municipal General Schedule M100000/0013, item 0800-0000 - 0800-0001. For additional concepts on how to approach retention scheduling of electronic mail, databases and unstructured content see the State General Schedule G100000/011, items 2200-0000 – 22160000. Contact RMS for guidance on electronic records management.

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

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

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

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

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

Guidelines for Guidelines for Cloud-based Records Storage continued

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

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

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

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

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

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

Note that while the guidance in this area focuses on preventing the unauthorized deletion/destruction of public records, the agency should endeavor to apply records retention schedules to Cloud-based records and regularly dispose of records that are eligible for disposition. Failure to do so leads to over-retention and exposes the agency to risks of increased storage costs and costs associated with retrieving and producing records that might otherwise have been disposed of legally.

Guidelines for Guidelines for Cloud-based Records Storage continued

7. Institute data/content management protections.

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

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

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

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

Guidelines for Guidelines for Cloud-based Records Storage continued

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

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

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

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

Guidelines for Guidelines for Cloud-based Records Storage continued

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

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

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

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

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

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

Following are examples of service levels that relate to the records management considerations covered in items 1-11 above, along with other common and potentially useful service levels pertaining to service availability, performance and breach protocols. It is important to note that DORES is providing these examples for illustrative purposes only. Work with your procurement, information security, information technology and legal advisors when developing formal service levels. The examples do not constitute an exhaustive list of Cloud service levels. Examples of Records Management-related and Other Common Cloud Service Levels The contractor shall provide a system/service that meets the following service levels:

- 99.99% system availability (uptime) between the hours of <start hour> am and <end hour> pm Monday through Friday.
- 99.99 uptime Saturday – Sunday, from <start hour> a.m. to <end hour> p.m.
- All unexpected downtime during the above hours must be reported immediately to <agency contact name and contact information> .
- Scheduled maintenance and down time must be performed during off hours – that is, hours that fall outside of the production time frames cited above and contractor must give at least one week’s notice of these maintenance events to <agency contact name and contact information>.
- Response time to end user entries or records access requests shall not exceed an average of <list time segment – for example, in milliseconds or seconds>. For purposes of this engagement, response time means the elapsed time from receipt of a client request at the contractor’s server(s) through to response received by <agency name>’s network.

Guidelines for Guidelines for Cloud-based Records Storage continued

• Facilities must ensure the logical and physical segregation of <agency name>'s data and records from other organizations' data and records and provide for the transfer of same to the <agency name>'s <list alternate storage facilities owned by or affiliated with the agency>, in whole or in part, upon demand. (**Note: Procurement, budgetary or other constraints may require the agency to place its data/records in shared storage spaces in the Cloud instead of segregated spaces as envisioned in this service level. For guidance on operating in shared multi-tenant environments, see the State-wide Information Security Manual, page 167.)

• All data and records stored in the Cloud facility must be within the 48 contiguous United States of America; contractor must disclose the precise location(s) of <agency names>'s State data/records.

• Cloud storage facility must allow <agency name> to classify stored records in accordance with specific record series found in <list approved records retention schedules that apply to the agency>.

• Contractor's system must enable tracking of all data and records in the Cloud facility from creation/receipt through to authorized deletion/destruction or transfer (life-cycle management) and include logs that show actions taken on data and records throughout their life cycles. Systems logs must be made available to <agency name> upon request.

• Contractor must ensure metadata is captured and made accessible for all data and records. The minimum metadata requirements are <list the required metadata elements>.

Guidelines for Guidelines for Cloud-based Records Storage continued

- Contractor may not delete/destroy any data/records without the express authorization of the agency's < list name and contact information for the agency's records management representative>. When <agency name> authorizes records deletion/destruction, contractor must securely delete/destroy the targeted records by obliterating them or otherwise rendering them permanently inaccessible and unreadable and provide written confirmation of the deletion/destruction.

- Contractor may not modify or transfer any records without <agency name>'s consent.

- Contractor must document and execute back-up and restoration plans for all data/records stored pursuant to this contract.

- Contractor's systems must include redundancy and fail-over capabilities that assure continued compliance with the previously stated uptime service levels in the event of a system or facility failure (operational continuity).

- Contractor must implement and maintain a disaster recovery program for all facilities that store <agency name>'s records, which ensures return to operation in 24 hours following a disaster, with the data recovery point at no more than <list the time frame – in hours, calendar days, business days, etc.>.

Guidelines for Guidelines for Cloud-based Records Storage continued

• Contractor's Cloud system/services must provide functions that allow <agency name> to implement electronic discovery in response to OPRA requests, audits, subpoenas and investigations. The required steps are identification, preservation, collection, processing, review, analysis, production and presentation of targeted records.[4]

• Cloud facility must use/support de-facto standard and non-proprietary file formats. At a minimum, the platform must use/support the following file formats: <list the file formats>. • Cloud facility must achieve compliance with <list the required compliance regime(s) – for example, State-wide Information Security Manual, SOC 2, FedRAMP, SafeGuards, etc.> and maintain said compliance for the length of the contractual engagement.

• Contractor must have a documented information breach protocol to be used in the event of theft or unauthorized access, transfer, destruction or defacement of public records classified as sensitive, confidential or private.

• Contractor must provide for the transfer of the following records to <list the computing facilities to which the records are to be transferred>: <list records to be transferred>. Said transfer shall occur <list the timetable(s) for the transfer(s)>.

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

Guidelines for Guidelines for Cloud-based Records Storage continued

- Upon contract termination, per the instructions of <agency name>, contractor must transfer all data/records residing on its platform to a designated storage location in a file format(s) specified by <agency name>.

Following the complete and successful transfer of all data/records, contractor must securely delete/destroy the targeted records from its platform, including all back-up data/records, by obliterating them or otherwise rendering them permanently inaccessible and unreadable. Contractor must provide written confirmation of the deletion/destruction.

The contact for the records management topics covered above is the New Jersey Division of Revenue and Enterprise Services' Records Management Services Unit (RMS): 609-777-1020 or 609-292-8711.

Guidance on preservation of permanent and historical records can be obtained from the State Archives: 609-633-8304 or 609-292-6260 Guidelines

Guidelines for Using Cloud-based Collaboration and Remote (Live) Conferencing Platforms

Guidelines for Using Cloud-based Collaboration and Remote (Live) Conferencing Platforms

Following are guidelines designed to assist New Jersey public agencies using cloud-based collaboration and remote video conferencing platforms. These platforms allow organizations to receive, create, store, access and share electronic records and information through the use of third-party facilities like Microsoft's Office 365 and Google's G Suite. Examples of standalone conferencing platforms include GoToMeeting and Zoom.

The Division of Revenue and Enterprise Services (DORES) is providing these guidelines because more public agencies are planning for safe and secure use of these platforms in the face of the COVID-19 pandemic and the continuing trend toward remote work (telework).

Guidelines

1. Only install platforms that are approved by your information and technology officials. Installation of unapproved software exposes the organization to information security risks.

2. Consult with your information and technology officials regarding the required security settings for remote video conferencing sessions. These settings revolve around controlling participation, muting/unmuting and removing participants, enabling/disabling chat, screen sharing and annotation features and locking sessions.

3. In using a cloud-based collaboration and remote conferencing platform, use a password that adheres to the organization's policy on passwords.

4. Open meetings only to those whose participation is necessary for accomplishing the meeting's objectives and double-check to make sure that you have selected the correct invitees.

5. While away from your office, use only safe Internet carriers (avoid using hotel, coffee shop or unsecured wireless access points).

6. Use agency-owned hardware whenever possible.

Guidelines for Using Cloud-based Collaboration and Remote (Live) Conferencing Platforms continued

7. If using a personal device, keep it current with patches, updates and the latest software versions. If you are using an agency-issued device, make sure you connect it to the agency's network at least once a month to ensure it receives all required patches, updates and software versions.

8. Know which laws and regulations pertain to the subject matter being posted, discussed, displayed or shared. For example, you may be dealing with tax, personal health, personally identifiable and/or proprietary information/records. Take steps to prevent the display of, sharing and/or disclosure of such information to unauthorized parties. If you are not certain that a connection or platform is secure, do not display, share or disclose such information by remote means until you can obtain access to a secure connection or platform.

9. Do not store tax, personal health, personally identifiable and/or proprietary information/records in the Cloud unless you are cleared to do so by your records and information technology officials. If you are not cleared to store this content in the Cloud, store it on the agency's on-premises platform – for example, on shared drives or image and content management systems that your agency controls directly. Note that in order to file information/records on your on-premises platform from a remote location, you will need to have software that allows you to access your on-site computing systems. This is usually accomplished through remote desk top software or via virtual private networks (VPN). Consult with your information technology officials regarding your options here.

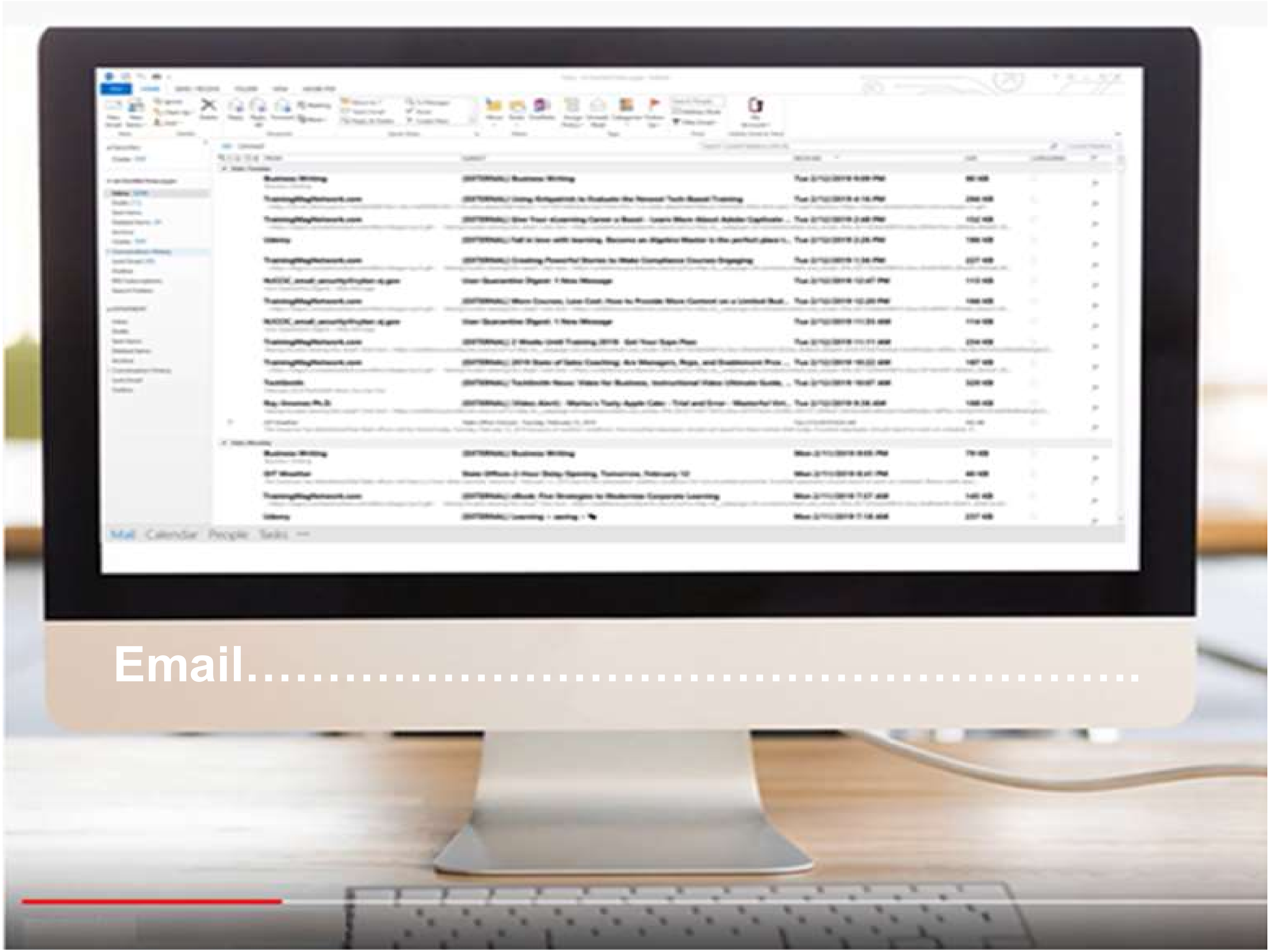
Guidelines for Using Cloud-based Collaboration and Remote (Live) Conferencing Platforms continued

10. Do not record audio-video sessions that deal with sensitive or confidential information unless cleared to do so by your records and information technology officials. Also, disable or temporarily shut off voice activated devices (for example, Alexa, Google and Siri) prior to participating in confidential voice or video calls.

11. Remember that records/information created and stored on collaboration/online conferencing platforms are public records, and therefore are subject the State's public records retention/disposition law and Open Public Records Act. Contact the Division of Revenue and Enterprise Services (DORES), Records Management for guidance on retention requirements for such records/information. (DORES Records Management Services - 609-777-1020 or 609-292-8711).

12. Be mindful that any public body meetings that you conduct via remote conferencing will be subject to the State's various open public meeting (OPM) laws, and that all requisite OPM actions and procedures apply.

13. When participating in a collaborative dialogue or a remote meeting initiated and/or hosted by a third party, be sure to adhere to guidelines 7-11 above: a. Do not disclose confidential/sensitive information/records to unauthorized parties; b. Do not record or store confidential/sensitive information on cloud-platforms unless authorized to do so; c. Seek guidance from DORES Records Management Services on how to comply with records retention requirements; and d. Adhere to OPM requirements where applicable.



Email……………………………………………………

Email

e-mail

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

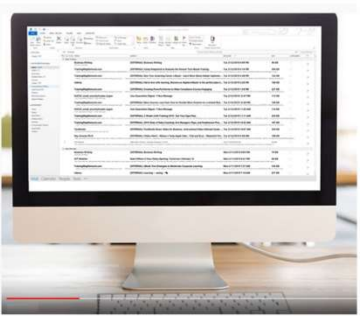
2. a message sent by e-mail: Send me an e-mail on the idea.

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

Also, E-mail, email.

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

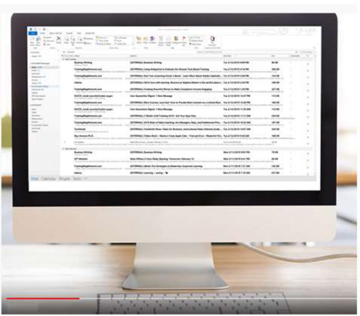
Email continued



What About Email?
Is it *Really* a Public Record?
Do I Have to Retain it?
Is it Discoverable?

- Email is a Public Record.
- Email may be Discoverable if in your Physical Custody - even AFTER you have received permission to destroy it from DORES-RMS.
- Email may be Accessible under OPRA.
- Email may be Disclosed in a Court of Law.
- Email may be Disclosed through e-Discovery.
- Email must be placed on a Records Retention Schedule.
- Email may *not* be destroyed without prior ARTEMIS authorization.

Email - Management, Retention & Disposal



Agency Email Management

- The Agency should consult the General Schedule for the Retention and Disposition of Email records.

- The Agency should maintain an Email System that includes Central Storage and Management for *all* Agency Emails - these Emails are to be kept separate from their copies residing in the users' Inbox.

- The Agency should adopt polices for E-Mail and Internet usage with associated employee training.

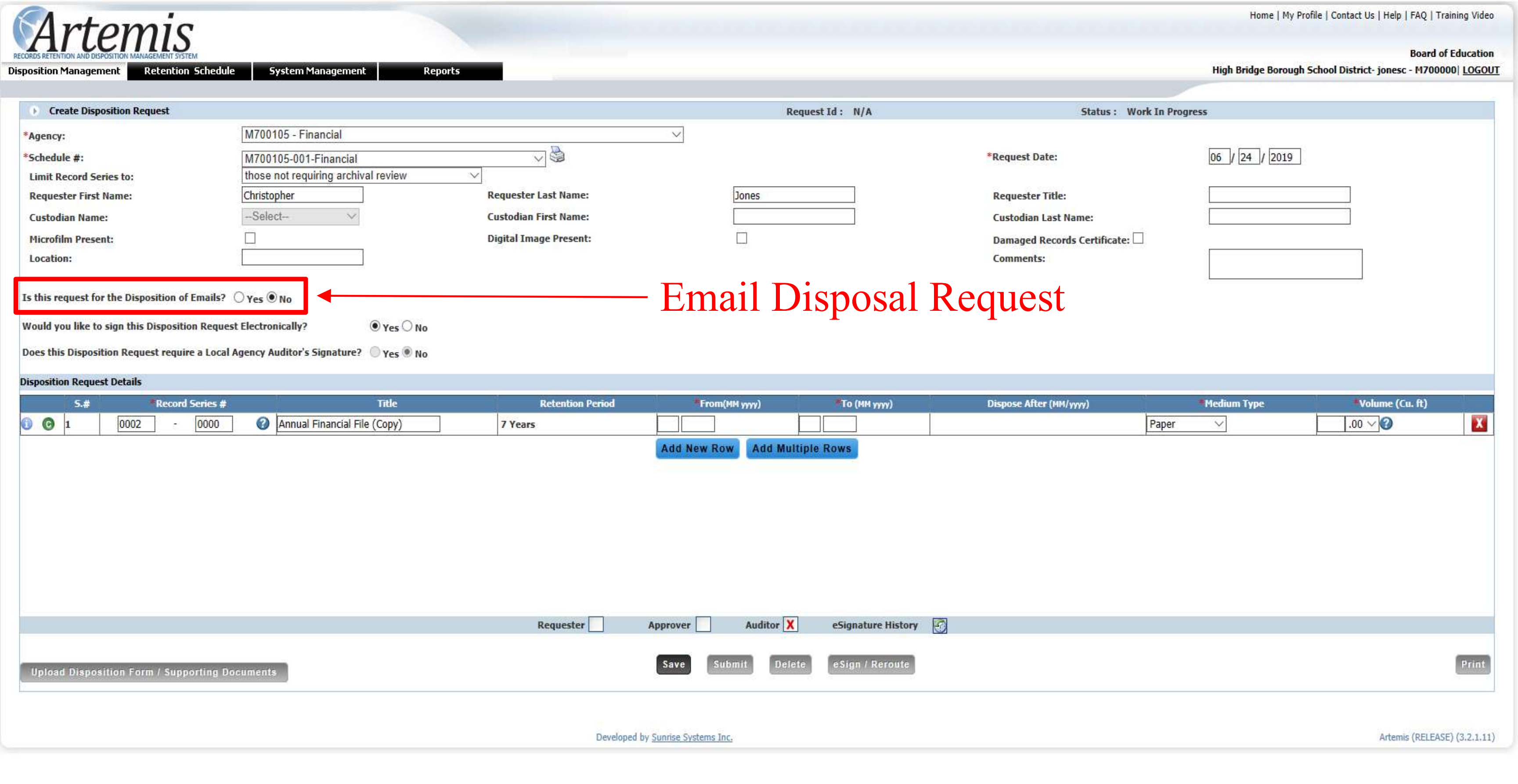
- The Agency's Email System should have Security Controls that guard against unauthorized access, use, modification, dissemination, disclosure and/or destruction.

- The Agency's Email System should have provisions for the administration of **"litigation holds"**.

- The Agency's Email System should also include back-up and Disaster Recovery Services for the restoration of Email.

- Only *authorized* Agency IT and/or Records Management Staff should control the management, retention and disposition of Email records the Email System. **Individual users should not be able to access or delete email records from the Email Central Storage/Management System**.

Email - Retention & Disposal in ARTEMIS


Artemis
RECORDS RETENTION AND DISPOSITION MANAGEMENT SYSTEM
Disposition Management
Retention Schedule
System Management
Reports
Home | My Profile | Contact Us | Help | FAQ | Training Video
Add New Row
Add Multiple Rows
Upload Disposition Form / Supporting Documents
Save
Submit
Delete
eSign / Reroute
Print

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

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

*Agency: M700105 - Financial
*Schedule #: M700105-001-Financial
*Request Date: 06 / 24 / 2019
Limit Record Series to: those not requiring archival review
Requester First Name: Christopher
Requester Last Name: Jones
Requester Title:
Custodian Name: --Select--
Custodian First Name:
Custodian Last Name:
Microfilm Present: □
Digital Image Present: □
Damaged Records Certificate: □
Location:
Comments:

Is this request for the Disposition of Emails? ○ Yes ● No

Email Disposal Request

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

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

Disposition Request Details

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

Requester □ Approver □ Auditor ☒ eSignature History

Developed by Sunrise Systems Inc.

Artemis (RELEASE) (3.2.1.11)

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

SOCIAL MEDIA
MONOPOLY
Mashable
Technorati
COLLECT $200
WI-FI
IPHONE
HTC EVO
DROID
IMAC
YOU'VE BEEN BACK-TRACED

Social Media

Social Media: interactive communication via web-based and mobile technology.

- Social Media Is Global, Immediate and Accessible.

- Social Media Is Not Private.

- Social Media Is Public and directives should be established regarding content, language, subject matter, etc.

- Social Media can be altered and used a portal for Cyberattack, which presents a real concern for an agency to release public information.

- Social Media is subject to the same Records Retention, Disposition, Access; Intellectual Property; OPRA, and Legal Rules of Evidence and e-Discovery concerns like e-mail, instant messaging, blogs, wikis, pod casts, metadata, or website content.

- An agency should consult with Records Management Services for guidance in developing a *Social Media Policy*. Social Media is similar to digitally-borne or website records. On your own website, you have control and can print hardcopy and protect it. With Social Media, you cannot control it and it can be altered or removed .

- 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.

Guidelines on Retention Scheduling Public Records on Social Media Platforms

Guidelines on Retention Scheduling Public Records on Social Media Platforms

Introduction

These guidelines include suggested action steps for creating retention/disposition policies for public records created and stored via social media services like Facebook, Twitter, LinkedIn, YouTube, wikis and other Internet-based platforms. Social media services involve various forms of content, including text, images, audio and video recordings. Usually, private firms provide and manage the platforms used to deliver social media services. This factor, combined with the dynamic, rich and complex make-up of the records involved, makes retention scheduling of social media a challenge. Nonetheless, public agencies can begin to deal with the retention scheduling challenge by executing the recommended action steps.

Applicability of Public Records Law

The foundation for this document is the legal imperative expressed in the State's public records law (N.J.S.A. 47:3 et seq.). That is, irrespective of medium, all records that are generated and received during governmental operations in New Jersey are public records and subject to the State's records management and archival requirements. Records generated and received via social media services and stored on social media platforms are therefore subject to the State's public records law.

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

Audience

Generally, these guidelines are designed for professionals who work in records and information management capacities and who have some familiarity with the State's records management program as described in the State Records Manual. However, generalist managers and administrative support staff may also find the guidelines useful.

Note on Scope

This document covers retention scheduling only[1]. It does not cover the more encompassing topic of social media policies and procedures. The New Jersey Records Manual contains an outline on how the State's Department of the Treasury approached the development of an encompassing social media policy/procedural regime. Readers interested in developing similar regimes for their agencies may find the outline helpful.

Note on Scope

This document covers retention scheduling only[1]. It does not cover the more encompassing topic of social media policies and procedures. The New Jersey Records Manual contains an outline on how the State's Department of the Treasury approached the development of an encompassing social media policy/procedural regime. Readers interested in developing similar regimes for their agencies may find the outline helpful.

[1] The approaches to retention scheduling, storage and disposition of social media discussed in this document are largely based on guidelines and standards published by the National Archives and Records Administration *(Best Practices for the Capture of Social Media Records*) and the New South Wales Archives and Records agency (Strategies for Managing Social Media Records). Be aware that some of the technical references in these publications may be dated or can become so quickly. However, the core concepts about value assessments and content capture, storage and retention/disposition are likely to be valid for the foreseeable future. Finally, The Sedona Conference provides invaluable information on this topic. It guided this document's commentary on the legal context of social media use/management (*Primer on Social Media, Second Edition*. (2018). The Sedona Conference: Phoenix, AZ.)

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

Key Contacts

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

Action Steps

1. Inventory Social Media

Start the retention scheduling process by inventorying and documenting all the services and platforms employed by the agency – for example, accounts/sites using Facebook, Twitter, Tumblr, YouTube, Snapchat, Instagram, etc. Describe the content that resides on each platform and the organizational functions that each one addresses – for instance, dissemination of program-related information, constituent service channel, ideation and communal program development, etc.

2. Conduct a Value Assessment(s)

Based on the descriptions and functional purposes of the social media platforms, assign values to the content (records) they contain. Following are value dimensions that could be assigned to records stored on social media platforms. The value dimensions are tied to a simple range: low (records with little or no lasting retention value); medium (records with some short-term – less than 10 years, retention value); and high (records with greater than 10 years retention value).

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

Note that records may bridge or overlap the value dimensions. For example, a particular social media site may contain content that has both informational and planning and decision support/knowledge management values. If this occurs and the overlapping dimensions have different (higher/lower) values with respect to retention and disposition, the recommended policy decision would be to assign the higher value to the content.

Value dimensions a and b below are likely to be the two most common dimensions that agencies encounter.

a. Informational **(retention value – low)**. Social media platforms can be used for broadcasting and one-way (organization to stakeholder) communications on routine matters. Content generated for such purposes would likely not have any lasting value, and therefore be classified as routine/non-sensitive in nature. Usually, the original, official broadcast messages are kept in separate storage areas (paper files, file shares, collaboration sites and/or agencies records/content management systems).

b.

General Information Exchange **(retention value - low to medium)**. Social media can augment informational postings by opening channels for two-way constituent service and communications. For instance, social media may serve as conduits for constituent commentary and information sharing (posts and tags) regarding information broadcast by the agency. Content produced in this category can include exchanges such as general feedback, question/answer streams, ratings, voting, likes/dislikes, etc. Such content may also have secondary uses such as operational research on the effectiveness and efficiency of communications campaigns.

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

c. Transactional **(retention value - low to medium)**. Social media can be parts of an agency's business processes and service delivery models. While perhaps there may not be a significant use case at this juncture of social media's technical and operational evolution, one could envision potential applications here – for example, delivery of digital content such as reports and other public documents and work order entry and tracking.

d. Operational/Management Control **(retention value - low to medium)**. This form of content relates to various internal (intra-agency) activities such as employee feedback/suggestions, information exchange/knowledge building, policy/procedure dissemination, publication of performance levels, etc. This type of content can correspond with and complement management control by carrying messages and commentary about program outcomes, operational controls and organizational service levels. Management control-related content is likely to have some enduring value beyond its immediate uses, principally as input for the next category, planning and decision support/knowledge management.

e. Planning and Decision Support/Knowledge Management **(retention value - medium to high)**. Here, content aids executives and specialized staff (technologists, public information officers, legal advisors, budget analysts, etc.) who develop plans and rules that guide the actions of the entire organization from a long term or strategic perspective. In this context, social media can contain valuable information including intra-agency and external discussions and information on a wide range of topics including: economic trends; policy research; constituent sentiment; legal issue; evolving products/technologies that impact agency operations; prevailing political trends; and changes in societal perspectives. Social media also may support collaborative efforts aimed at idea development and product or service innovations via feedback from individual citizens, organizational actors and various other stakeholders.

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

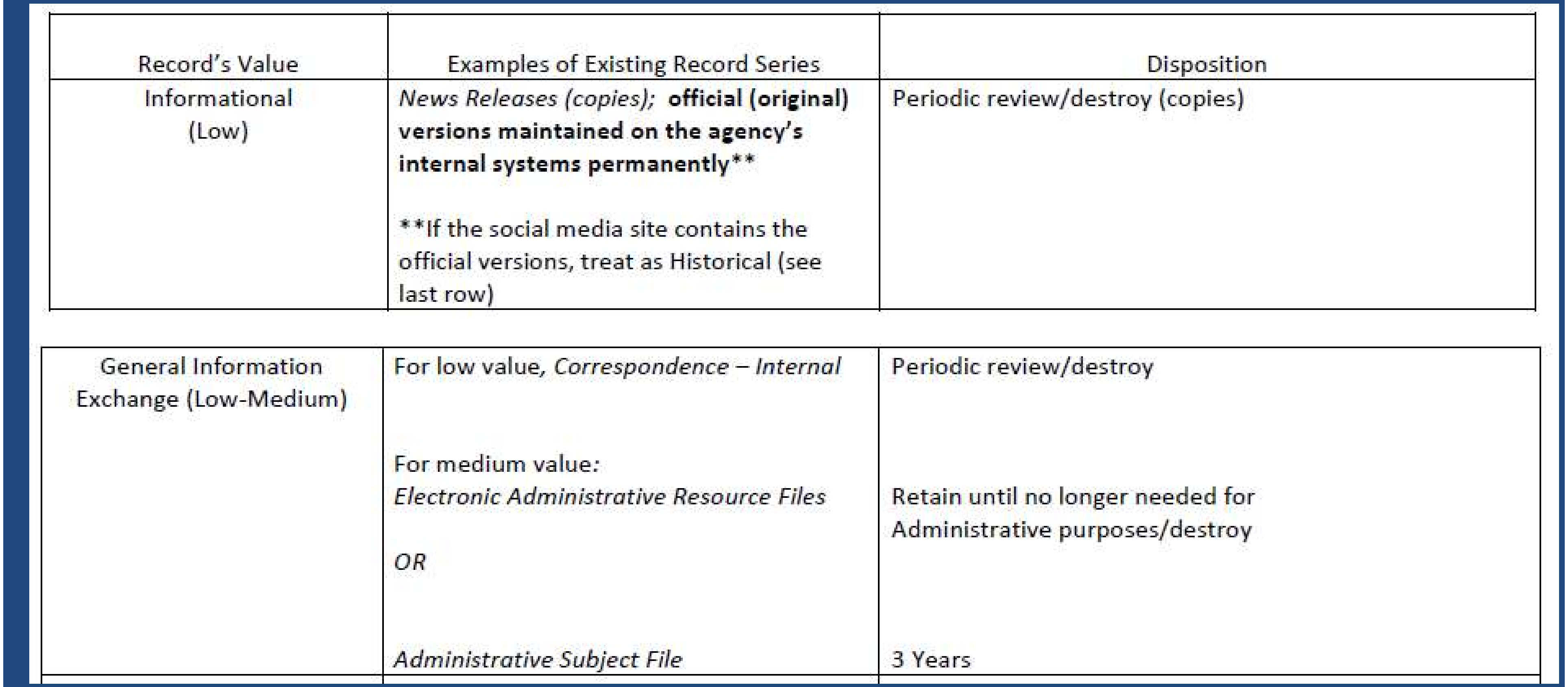
f. Legal/Compliance **(retention value – high)**. This is an encompassing category which, *depending on the agency's mission*, may envelop all the prior categories. It relates to the management of content, in all forms, for adherence to statutory and regulatory record-keeping requirements. Agencies that employ social media platforms in tightly regulated contexts should be aware that legal, contractual and rules-based requirements may attach to the contents generated by and stored on the platforms. Agencies may be compelled to produce this social media content in discovery processes associated with litigation, audits and internal investigations.

g. Historical **(retention value - high)**. This dimension is likely to grow in importance as time progresses, especially in governmental contexts. Historical content holds long-term or permanent research value. It serves to preserve our intellectual heritage and to document important social, political, economic and cultural developments, and thus has enduring relevance. Over time, some portion of the social media content space will document significant events, developments and/or trends in aspect of human development, and/or record time- and context-bound perceptions and attitudes about significant human endeavors. This may be especially true in relation to the current COVID-19 pandemic.

3. Assign Retention and Disposition Policies to Social Media Records
Based on the value assessments conducted in Action Step 2, assign retention and disposition polices to all social media records that the agency generates and stores. This may be done by creating new agency-specific records retention schedule items (record series) or using existing records series.

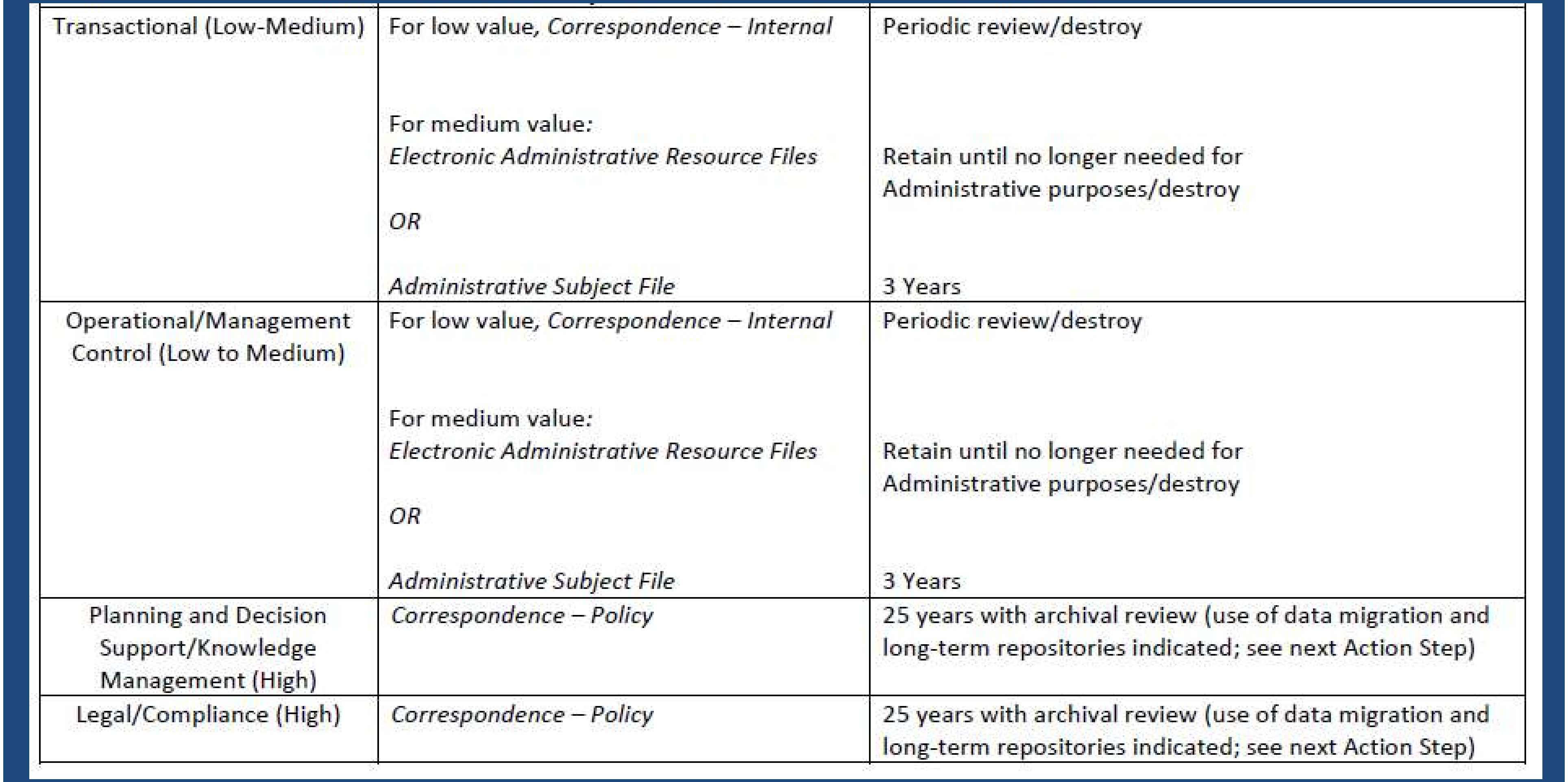
Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

Following are suggestions for use of existing general record series and disposition policies that align with the value dimensions discussed in Action Step 2.



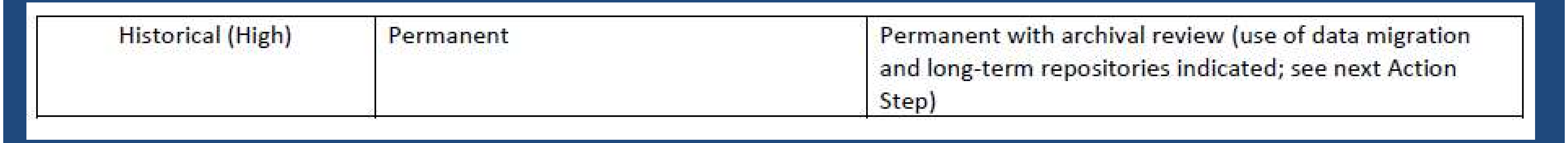
Record's Value	Examples of Existing Record Series	Disposition
Informational (Low)	*News Releases (copies);* **official (original) versions maintained on the agency's internal systems permanently**** **If the social media site contains the official versions, treat as Historical (see last row)	Periodic review/destroy (copies)
General Information Exchange (Low-Medium)	For low value, *Correspondence – Internal* For medium value: *Electronic Administrative Resource Files* *OR* *Administrative Subject File*	Periodic review/destroy Retain until no longer needed for Administrative purposes/destroy 3 Years

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued



Transactional (Low-Medium)	For low value, *Correspondence – Internal* For medium value: *Electronic Administrative Resource Files* *OR* *Administrative Subject File*	Periodic review/destroy Retain until no longer needed for Administrative purposes/destroy 3 Years
Operational/Management Control (Low to Medium)	For low value, *Correspondence – Internal* For medium value: *Electronic Administrative Resource Files* *OR* *Administrative Subject File*	Periodic review/destroy Retain until no longer needed for Administrative purposes/destroy 3 Years
Planning and Decision Support/Knowledge Management (High)	*Correspondence – Policy*	25 years with archival review (use of data migration and long-term repositories indicated; see next Action Step)
Legal/Compliance (High)	*Correspondence – Policy*	25 years with archival review (use of data migration and long-term repositories indicated; see next Action Step)

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued



Historical (High)	Permanent	Permanent with archival review (use of data migration and long-term repositories indicated; see next Action Step)

4.Choose Modes of Storage for Social Media Records

It is most common for agencies to use third party social media services and platforms that are publicly facing and that use a variety of electronic storage formats that can evolve rapidly. Also, third party service providers may offer varying levels of quality and storage capacities that could change over time. This can make the underlying storage technologies and service levels for the agency’s social media program uncertain and unstable. In this connection, consider the following storage options.

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

a. **Implement an *archiving* tool that allows for the scheduled extraction and migration of social media content to an agency-owned or controlled trusted digital repository.**[2] This is the preferred approach. A trusted digital repository enables the agency to store digital records, including social media records, in formats that assure access, use and analysis of the records for the entire length of their retention periods. [3] This functionality is critical for long-term and permanent records. **However, for ease of administration, agencies may wish to include short-term records in these repositories as well.**The trusted digital repository can be an agency owned computer storage facility and/or a Cloud-based platform, either of which meets or exceeds the requirements listed in the RMS Cloud storage guidelines (State Records Manual, page 145). [4] For long-term or permanent storage requirements, the repository should use file formats that are compatible with long-term/permanent storage.[5] Once records are **successfully migrated** to the trusted digital repository, the agency may delete the migrated content from the site.

[2] In this context, the term *archiving tool* refers to a specific form of software and does not inherently imply or equate to long-term retention of content in the State Archives or any other repository of permanent digital records.

[3] The Research Library Group/Online Computer Library Center (RLG/OCLC) provides a formal, encompassing definition of trusted digital repository in its publication entitled *Trusted Digital Repositories: Attributes and Responsibilities.* As noted in the narrative, while trusted digital repositories focus on long-term and permanent storage, for purposes of this guideline, short-term records may also be included for ease of administration.

[4] The Cloud storage guidelines are relevant to this discussion because many of the requirements listed for Cloud platforms center on capabilities that go to the ability of *any* repository to address long-term records storage and access. The RLG/OCLC publication cited in the previous footnote also provides valuable information on these and other key characteristics, as does the OCLC's publication entitled *Trustworthy Repositories Audit & Certification: Criteria and Checklist*.

[5] The National Archives' guidelines on file formats for transfer of permanent records and metadata for transferred files may prove helpful in determining file format and meta data requirements for trusted digital repositories.

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued

b. If the agency's social media site(s) contain records with medium to long-term value (for purposes of this guideline, retention for2 to 10 years), and the procurement of an archiving tool is not possible, migrate the content periodically to a trusted digital repository via importation of tested back-ups or through the use of data export/ import applications. Otherwise, copy (cut and paste) content to the repository. This *snippet* approach is not a best practice but may be used if there are no other options available to the agency.

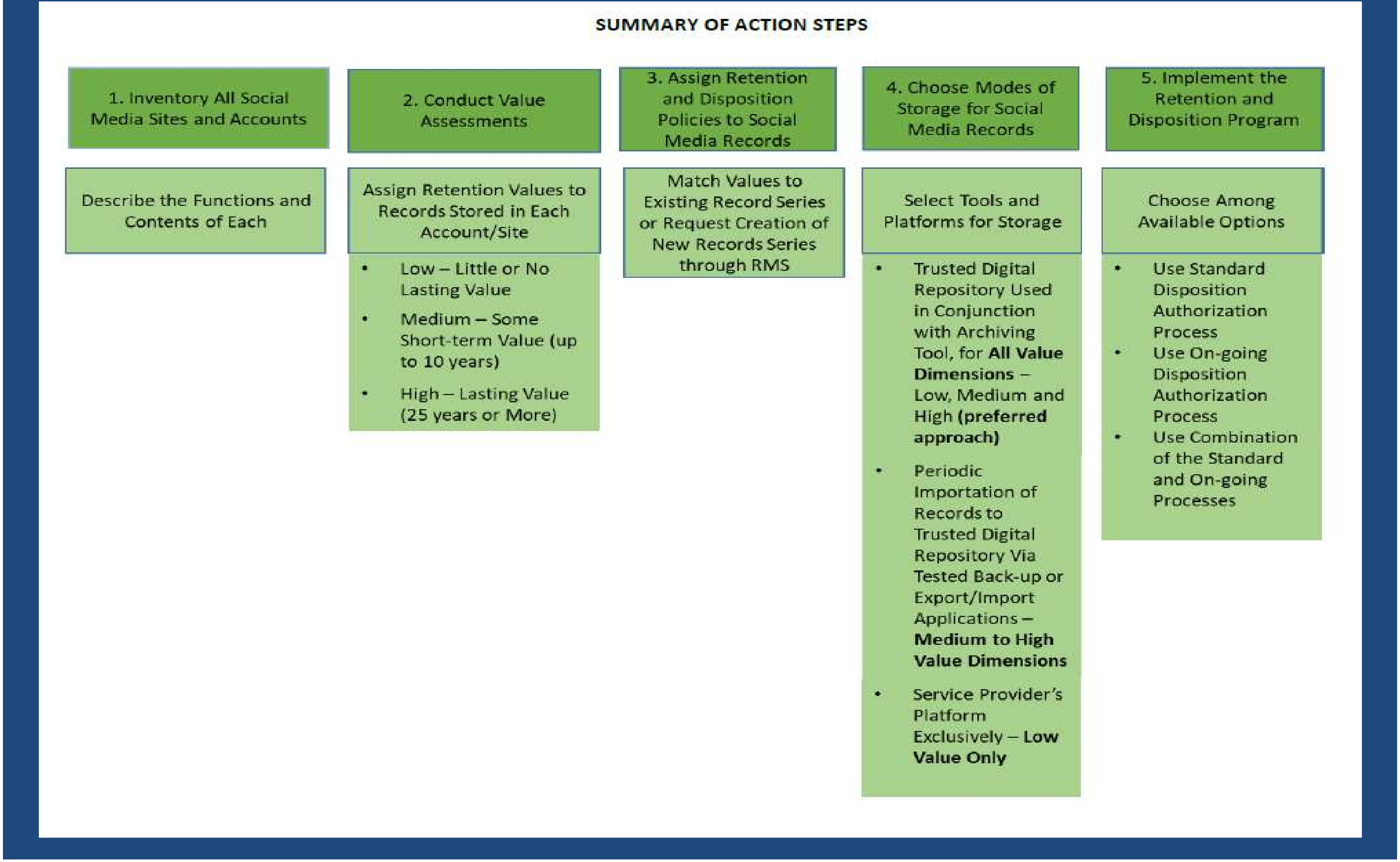
c. If it is not possible to procure an archiving tool, **and the agency's records need to be retained for short time frames (for purposes of these guidelines, no more than 2 years)**, consider relying on the platform used by the social media service provider exclusively. Ensure that the provider has back-up/recovery tools in place to guard against data loss, or that there are data import/export applications that can be used to make accessible copies of the records. Be sure to test the back-up/recovery tools and export/import applications to ensure that lost or damaged content can be restored.

5.Implement the Retention and Disposition Program

Choose to conduct the program by:

a. The standard disposition authorization process (State Records Manual, pages 10 – 13)
b. The on-going disposition authorization process (contact RMS for assistance in setting up an on-going authorization)
c. A combination of the processes for different sites

Guidelines on Retention Scheduling Public Records on Social Media Platforms continued



SUMMARY OF ACTION STEPS

1. Inventory All Social Media Sites and Accounts

Describe the Functions and Contents of Each

2. Conduct Value Assessments

Assign Retention Values to Records Stored in Each Account/Site

- Low – Little or No Lasting Value
- Medium – Some Short-term Value (up to 10 years)
- High – Lasting Value (25 years or More)

3. Assign Retention and Disposition Policies to Social Media Records

Match Values to Existing Record Series or Request Creation of New Records Series through RMS

4. Choose Modes of Storage for Social Media Records

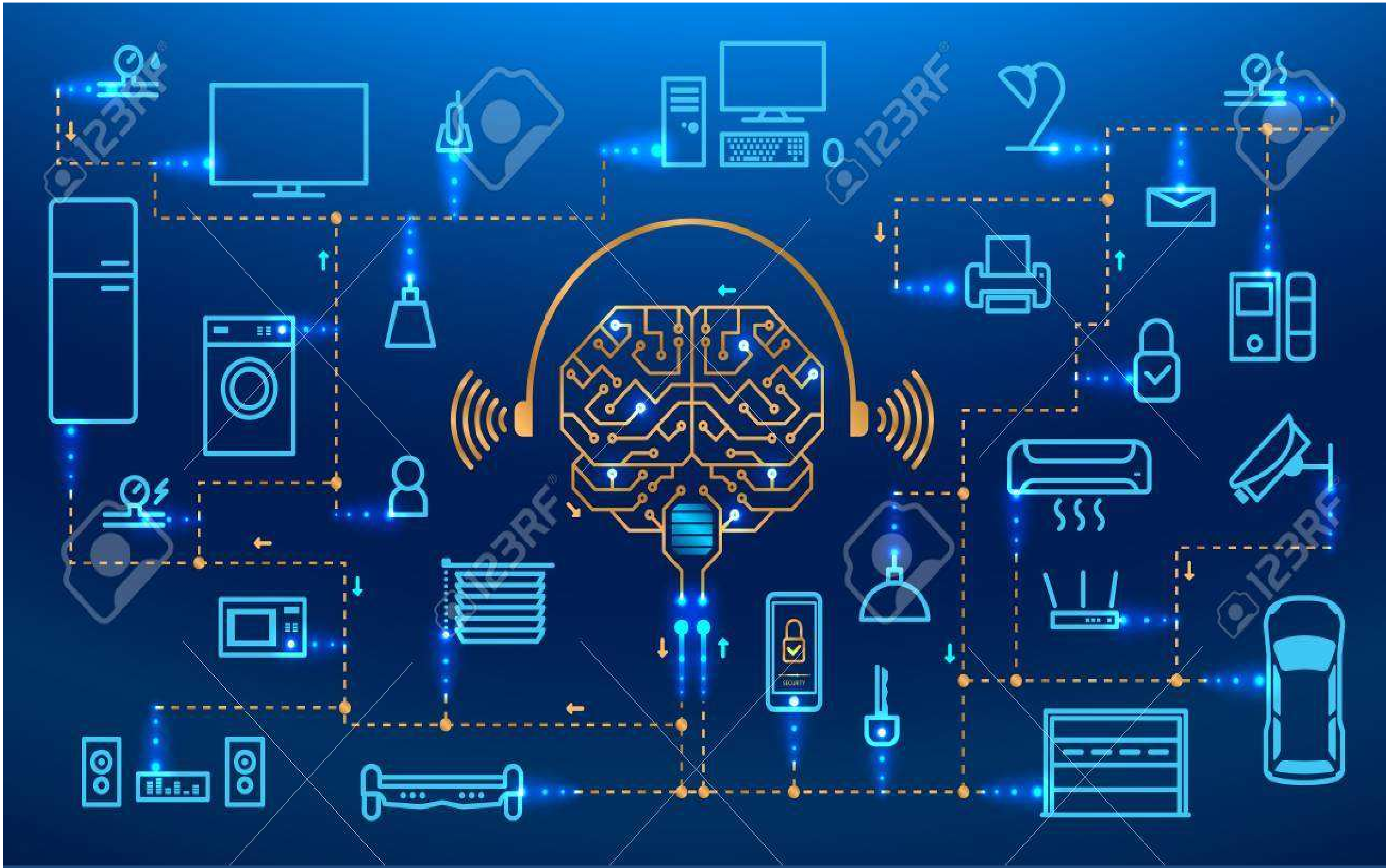
Select Tools and Platforms for Storage

- Trusted Digital Repository Used in Conjunction with Archiving Tool, for **All Value Dimensions** – Low, Medium and High **(preferred approach)**
- Periodic Importation of Records to Trusted Digital Repository Via Tested Back-up or Export/Import Applications – **Medium to High Value Dimensions**
- Service Provider's Platform Exclusively – **Low Value Only**

5. Implement the Retention and Disposition Program

Choose Among Available Options

- Use Standard Disposition Authorization Process
- Use On-going Disposition Authorization Process
- Use Combination of the Standard and On-going Processes



The World Wide Web and the Internet of Things (IoT)

The World Wide Web and the Internet of Things (IoT)

The World Wide Web via the Internet of Things or the Internet, is how government operates with other government agencies, business and industry, finance, healthcare, education, etc. The Web is comprised of three (3) different strata:

Surface Web

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

Deep Web

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

Dark Web

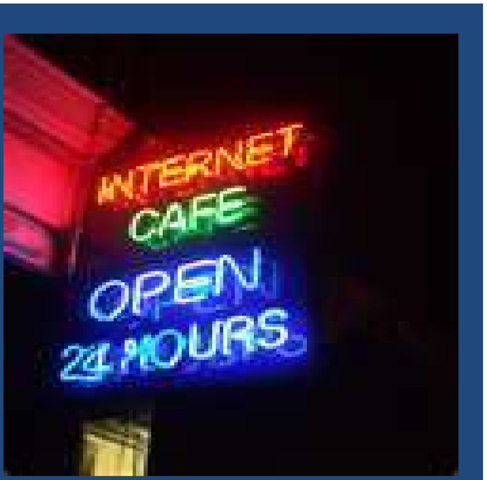
The encrypted part of the Internet that refers to alleged *questionable* content that is not easily reached and requires the multi-layered Tor software for access.

The World Wide Web and the Internet of Things - Perspectives

Due to its ever-changing content and structure, an agency should maintain documentation regarding their website. These records reflect hardware, software, Metadata, content and their respective areas of concern:

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

The World Wide Web and the Internet of Things - Records



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.

Security - Information Technology

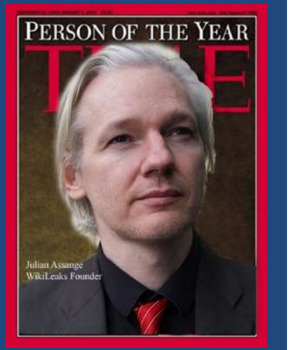
Security - Information Technology

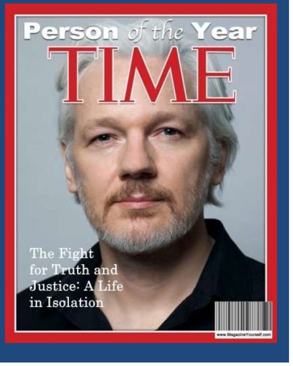
Government uses Information Technology (IT), Networking, Mobile Computing, Telecommunications, Email, the Cloud and Social Media in its normal course of business of receiving, processing & distributing data and information.

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

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

Pers
Julian Assange
WikiLeaks
TIME
Do You Want to Know a Secret?
TIME
Wikileaks: How is it Organized ?





Security – Types of Cyber Attack

TYPES OF CYBER ATTACK --- --- --- --- --- --- --- --- --- --- --- ---

UNINTENTIONAL: INTERNAL and/or EXTERNAL ACTIONS

The Accidental Access or Release of information or its Premature, Unauthorized or Inadvertent disposal, Misconfiguration, Insecure Interfaces and APIs, etc.

INTENTIONAL, DELIBERATATE: INTERNAL and/or EXTERNAL ACTIONS

Advance persistent threats, Zero Day threats, overt/covert cyber hacking from a foreign national with deliberate intent to influence and or disrupt a government activity or action, man-made disasters, social engineering, cyberespionage/cyberspies, Insider Threat, mining, data theft and modification, root enablers, Brute-Force attack, Doxing, Point of Sale (POS) malware, biocyber-intrusions, cyberthreats, cyberterrorists, cyberthieves, cyberwarriors, cyberhacktivists, internal and external Sabotage, data user attack, WannaCry Ransomeware, botnets, botnet bitcoin sales via the Dark Web, Exhaustive Master Key Search attack, Data Leakage overlay attack, drop box malware, spyware, network eavesdropping, data modification, identity falsification, password attacks, denial of service attacks, man-in-the-middle monitoring attack, botnets; zero-day threat, compromised key attack, keylogger, exploits, exploit kits, backdoor, sniffer attack, application software layer attack, unpatched software attack, trojans, worms, Phishing, spearphishing, whaling, advanced persistent threats, root malware, malware, jailbreak, drive by downloads, typosquatting, wiper, Denial of Service (DoS), Distributed Denial of Service (DDoS), spoofing, lax or delayed software patches, malvertising, rogue software, cross-platform malware, mobile malware, metamorphic and polymorphic malware, pineapple, surveillanceware, Hacking, Identity Theft, CEO Fraud/BEC, threatening sources (gadflies, competitors, third parties, activists, hackers, criminals, terrorists), Fake News, B0r0nt0k Ransomware, Trojan Panda Banker / Zeus Panda, Cloud Vulnerability, AI-Enhanced Cyberthreats, AI Fuzzing, Machine Learning Poisoning, Smart Contract Hacking, Social Engineering Attacks, Deepfake, theft of intellectual property, theft of equipment or information account hijacking, Online Harassment, Cyberstalking, Invasion of Privacy, information extortion, etc.

Security – Types of Cyber Attack continued

Types of Cyber Security Threats

Phishing — Phishing attacks, in which carefully targeted digital messages are transmitted to fool people into clicking on a link that can then install malware or expose sensitive data, are becoming more sophisticated. Employees at most organizations are more aware of the dangers of email phishing or of clicking on suspicious-looking links, hackers are upping the using machine learning to much more quickly craft and distribute convincing fake messages in the hopes that recipients will unwittingly compromise their organization's networks and systems. Such attacks enable hackers to steal user logins, credit card credentials and other types of personal financial information, as well as gain access to private databases.

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

Cryptojacking — The cryptocurrency movement also affects cyber security in other ways. For example, cryptojacking is a trend that involves cyber criminals hijacking third-party home or work computers to "mine" for cryptocurrency. Because mining for cryptocurrency (like Bitcoin, for example) requires immense amounts of computer processing power, hackers can make money by secretly piggybacking on someone else's systems. For government, cryptojacked systems can cause serious performance issues and costly down time as IT works to track down and resolve the issue.

Security – Types of 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.

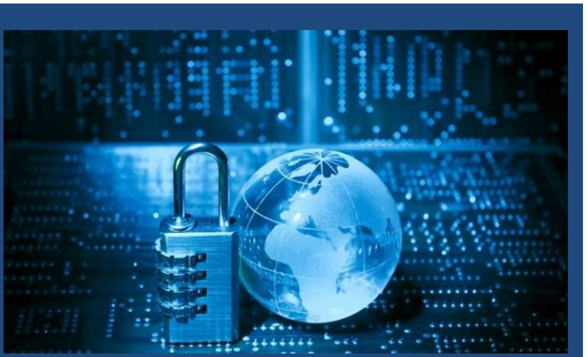
State-Sponsored Attacks — Beyond hackers looking to make a profit through stealing individual and corporate data, entire nation states are now using their cyber skills to infiltrate other governments and perform attacks on critical infrastructure. Cyber crime today is a major threat for private sector, individuals, government and the nation as a whole.

IoT Attacks — The Internet of Things is becoming more ubiquitous by the day (the number of devices connected to the IoT is expected to reach almost 31 billion by 2020). It includes laptops and tablets, routers, webcams, household appliances, smart watches, medical devices, manufacturing equipment, automobiles and even home security systems. However, this also means greater risk, making IoT networks more vulnerable to cyber invasions and infections.

Smart Medical Devices and Electronic Medical Records (EMRs) — As Health Care adapts to the digital age, there are real concerns about privacy, safety and cyber security. While hospitals and medical facilities are still electronically converting hardcopy patient medical records online and converging their electronic records systems, hackers are exploiting the many vulnerabilities in their security defenses, making them prime targets due to the sensitive information they contain.

Third Parties (Vendors, Contractors, Partners) — Third parties such as vendors and contractors pose a huge risk to corporations, the majority of which have no secure system or dedicated team in place to manage these third-party employees.

Security – IT Safeguard Measures



IT Measures must be taken to safeguard informational and areas susceptible to Cyber Attack: Web/Internet applications; desktops; mobile devices; the Cloud; Network-connected devices; Communication lines; Hardware, System and Application Software; Metadata and Data; Records and Reports; Email; Social Media; Internet- and Web-based documents, etc.

Basic IT Safeguard Measures should be implemented to include:

- Routine backups and Migration of Legacy Information and Records,
- Update antiquated hardware and system software with: built-in Security, Firewall/System/Network Segmentation, Cyber-Tracking, Data Loss Prevention, Anti-Virus, Spam, Malware and Ransomware,
- Develop and routinely update data encryption policies, employee passwords and facility passwords and access level codes,
- Regulate that all government computing including mobile, must be conducted on specific government-issued devices that only agency-authorized apps are to be downloaded on agency computing and mobile devices,
- Identify Agency Data and System vulnerable access points - including email, websites and social media,
- Implement Intrusion Prevention and Detection Systems,
- Update, update and update!

The Plan:

- Vital Records
- Disaster Prevention & Recovery
- Business Continuity

Vital Records

Vital Records are the records essential to meet operational responsibilities under emergency or disaster conditions. An Agency needs to ask itself:

> "What records are absolutely crucial to operations and can hardcopy, digital or electronic backups be produced if they are lost in a disaster?"

Conduct a Risk Analysis by evaluating the potential hazards to electronic records:

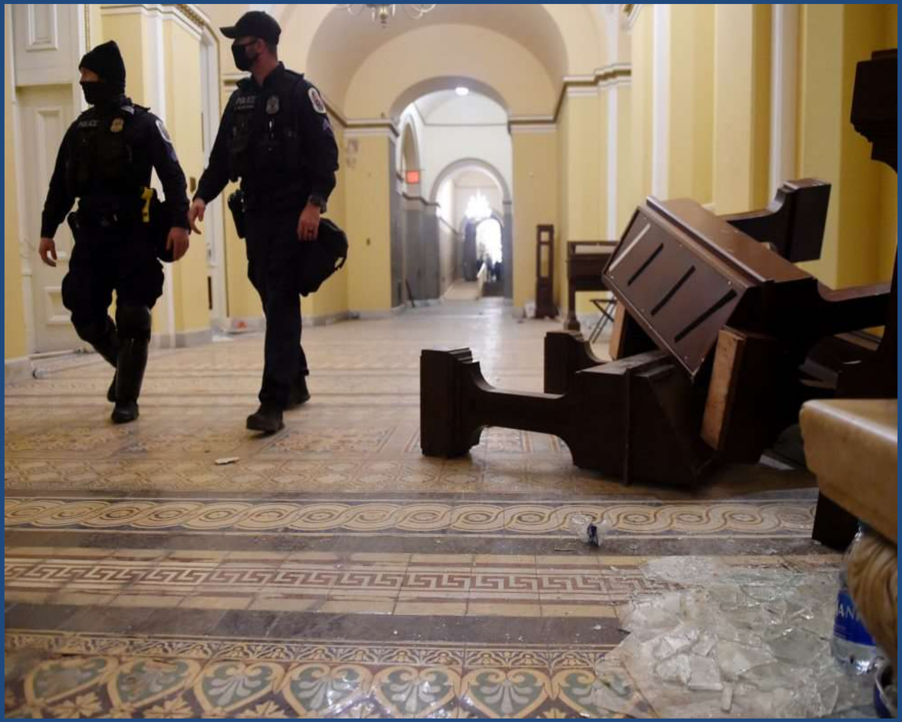
- Natural & Environmental
- Human inflicted
- Facility related

Determine electronic records protection methods:

- Appropriate Agency protection measures
- Measures may vary by type of record

Identify Vital Records:

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



Disaster Prevention and Recovery & Business Continuity

Procedures and operations before and after a disaster, that identify essential personnel, equipment, and alternate space if a closing of a facility is deemed necessary in order to resume services to an agency. A *Disaster Prevention and Recovery Plan* and a *Business Continuity Plan* are the key elements to safe and successful operations.

Disaster Prevention & Recovery

- Mitigates Loss of Records and Information
- Protects Electronic Records, Hardware and Software

Business Continuity

- To resume operations quickly and efficiently
- To ensure the normal flow of business
- Foster continued business relations and credibility and reputation

Notre Dame Cathedral
Paris, France April 15, 2019

Disaster Prevention and Recovery & Business Continuity – Information Technology

The Objective

To mitigate the amount of damage and associated costs (i.e., lost revenue, wages, labor, employee morale, customer goodwill, marketing opportunities; incurred bank fees and legal penalties; and bad publicity from Planned and/or Unplanned Downtime) and to protect information and resume information technology services to agencies after a disaster.

Planned Downtime

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

Unplanned Downtime

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

Contains

Disaster Prevention and Recovery Plan, Standards, and Guidelines; Security Policy and Procedures; Client Network Installation and De-installation data; and supporting documentation. The Disaster Prevention and Recover Plan is to be used in conjunction with an agency's Business Continuity Plan.

Disaster Prevention and Recovery & Business Continuity – The Plan

What to do *before* something goes wrong.

Establish

- *Disaster Prevention and Recovery* and *Business Continuity Plans.*
- Vendors Lists for Disaster Recovery Services and Supplies, System Hardware and Software and Electronic Disaster.
- Disaster Recovery Team - Records Management, IT and Custodian of Public Record .
- Agency Chain of Command.
- Data Center Hot & Cold Sites Identify Information Technology Staff.
- Alternate Operations Site for Agency Staff, PCs, Records.

Identify

- Hardware, Software (models and versions) and Data.
- Agency Vital Records.
- Potential Recovery Costs – Hardware, Software, Supplies, Technology Supplies, etc.
- Necessary Emergency Supplies.

Retain

- Disaster Prevention and Recovery and Business Continuity Plans - copies in safe and accessible Offsite Locations and with *every* Disaster Recovery Team Member.

Revise

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

The Future of Digital Information …

Synthetic DNA to Store Digital Information

ARCH MISSION

Cape Canaveral, Florida, April 15, 2019

The Arch Mission Foundation & the State of Israel's *"The Lunar Library - Spaceil2019's Beresheet Lander"* crashed onto the Moon's surface with a Lunar Library of dime-sized analog disks containing 30 Million Pages of Digital Information of Human History.

The space craft was destroyed but the disks of digital information are believed to have survived and are able to last "ions" to be available for future space exploration.

The Arch Mission Foundation, a non-profit organization whose goal is to create "redundant repositories" of humankind knowledge around the Solar System and the Earth. The Foundation has launched three missions and a fourth proposed –

- The FOUNDATION Library (SpaceX, 2018)
- The LEO Library (SpaceChain, 2018)
- The Lunar Library I (SpaceIL, 2019)
- The Lunar Library II (Astrobotic, 2021) – is the next slated Mission.

Swiss Lab Creates Synthetic DNA to Store & Reproduce Digital Information - in a Plastic Bunny Rabbit

FOR IMMEDIATE RELEASE

ZURICH, SWITZERLAND - DECEMBER 2019 - The Swiss-based Lab, ETH has developed a reproducible plastic bunny rabbit using a DNA sequencer and a 3D printer. The lab coated biological DNA with Silica to produce Synthetic DNA and infused it into a white, plastic bunny rabbit figurine. This resulted in the bunny's DNA information - size and shape and makeup - being stored for millions of years and able to reproduced more identical plastic bunny rabbits faster than real ones.

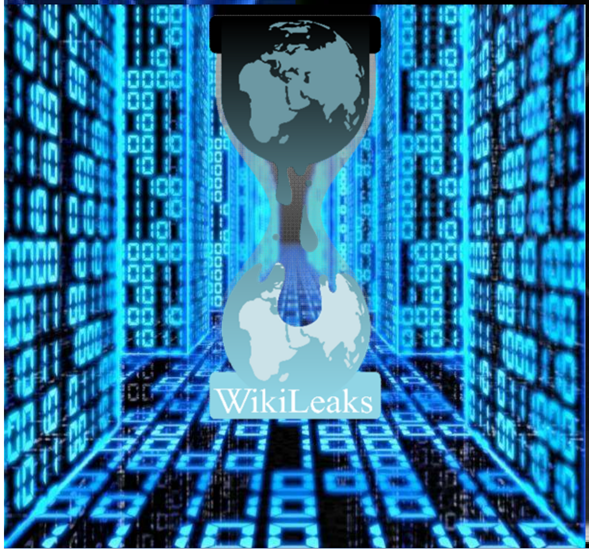
Bunnies today, tomorrow…the carrot patch and beyond.

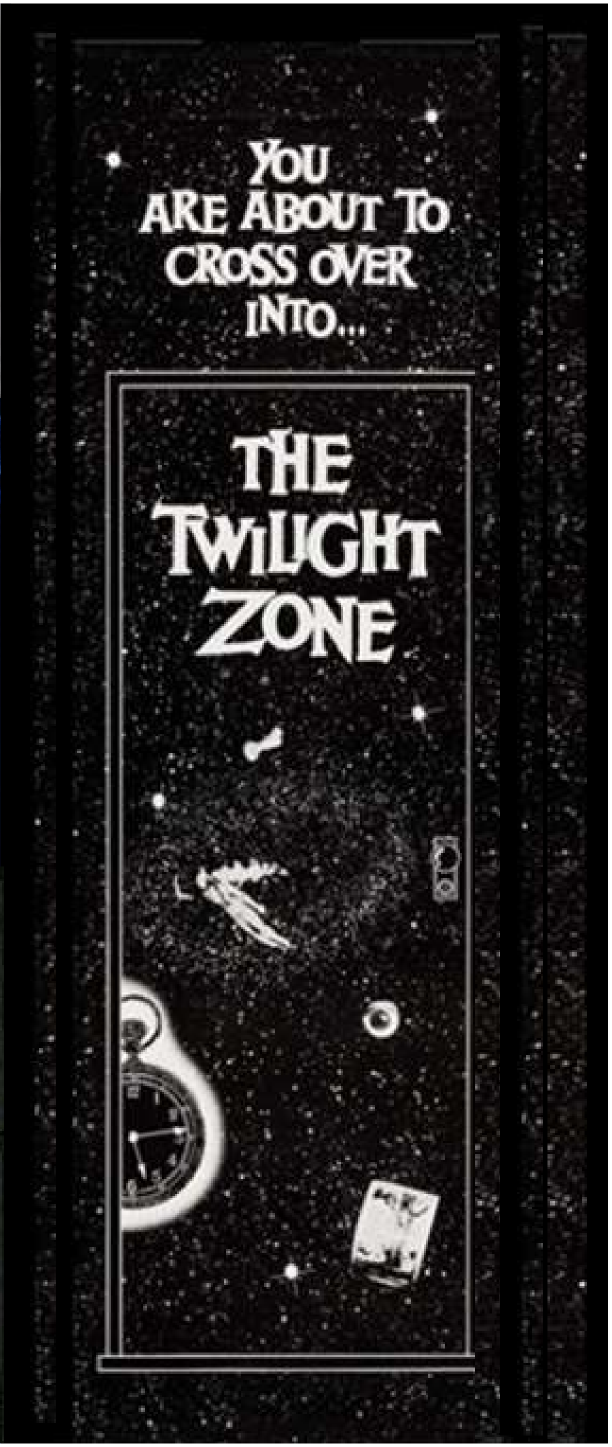
# # #

What’s Next???

TOP- SECRET
CONFIDENTIAL

thymine
deoxyribose
guanine
adenine


WikiLeaks


YOU ARE ABOUT TO CROSS OVER INTO...
THE TWILIGHT ZONE

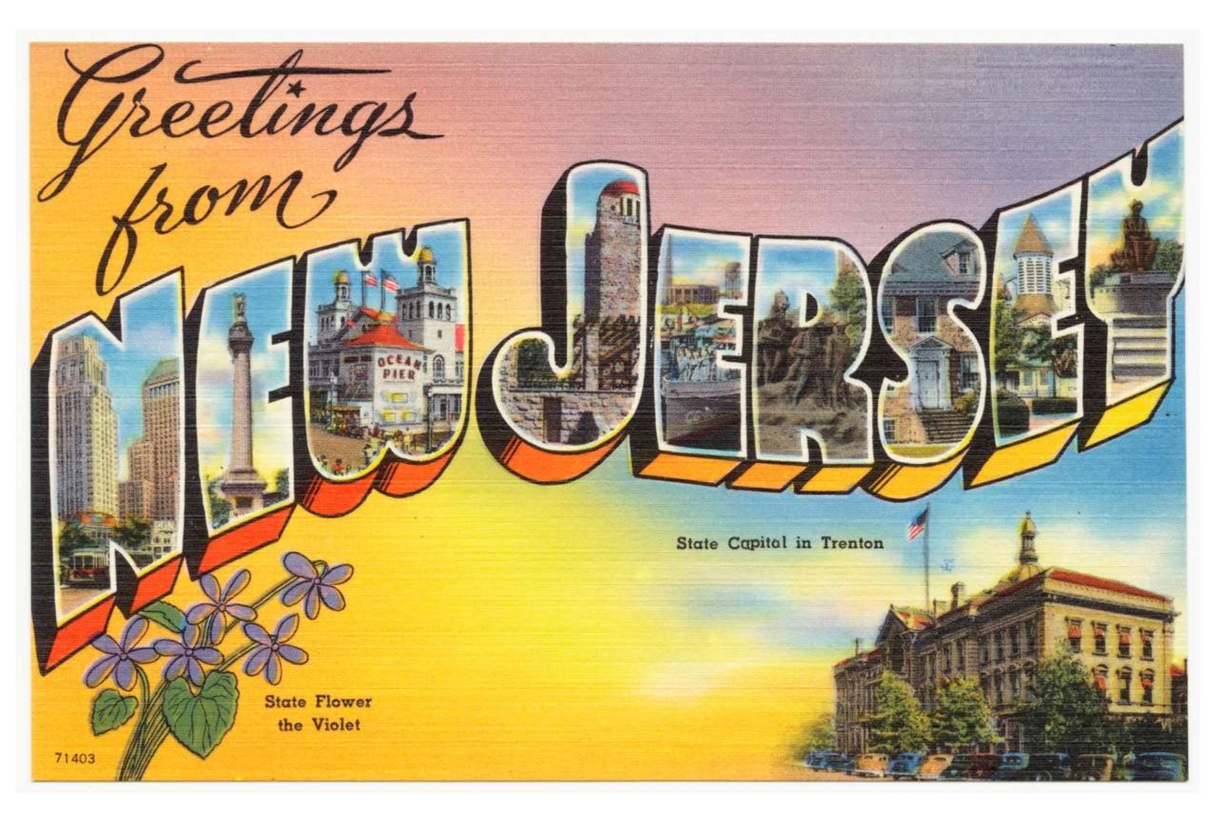
A final thought…

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.“

- Warren Buffett

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

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


Greetings from
NEW JERSEY
OCEAN PIER
State Capital in Trenton
State Flower the Violet
71403

Thank you.