Records and Information Management in the Age of e-Government

Karen A. Perry

Records Analyst

Department of the Treasury
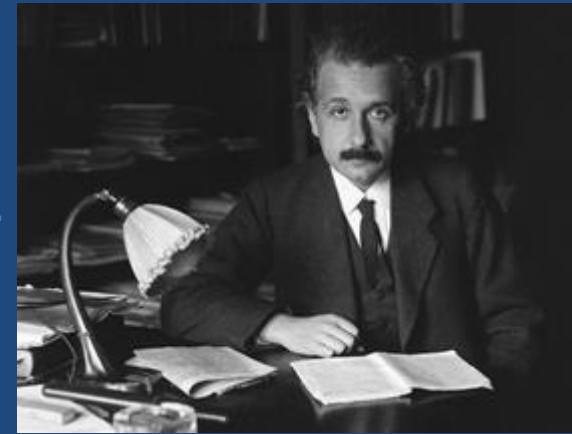
Division of Revenue and Enterprise Services

Records Management Services

Records and Information Management in the Age of e-Government

According to Albert Einstein and the *Laws of Physics*, *nothing* can exist in a vacuum … and Government is no exception.

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

- Traditionally, their Constituency Base were: Federal Agencies; Government Agencies from other States; Private Sector; Financial Institutions; the Media and the Public at Large. Interactions with these constituents usually resulted in the exchange of varying amounts of public information in hardcopy, electronic and/or digital format.
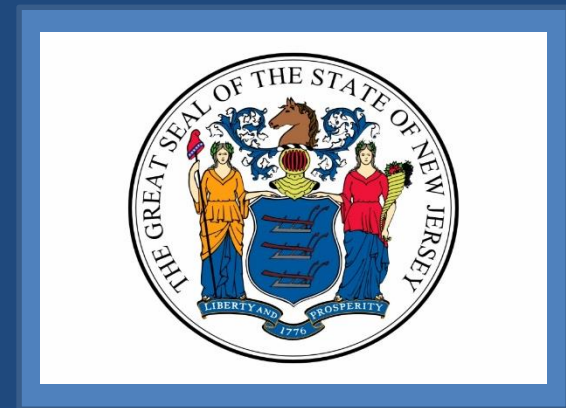
Today, Public Agencies in New Jersey have a Constituency Base that has expanded to include the International Arena resulting in a global exchange of even larger quantities of public information now being transmitted and stored via the Internet and Social Media and the Cloud, compounding the concerns for Security, Regulatory Compliance, Access, Retention, Preservation and Disposition.

Destruction of Public Records Act (PL 1953, c. 410) – The State Records Committee
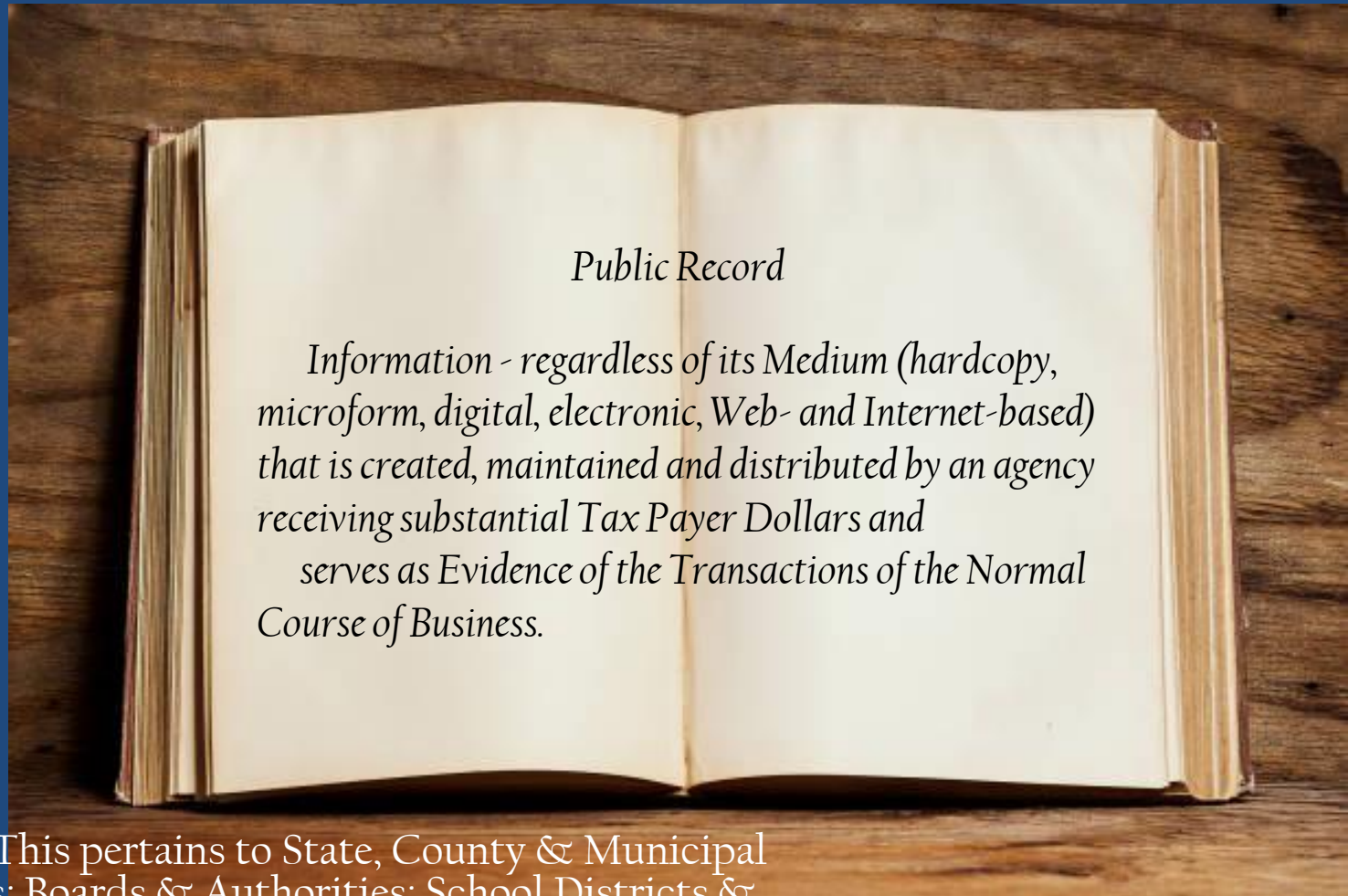
State Records Committee

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

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

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

Public Record

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

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

Destruction of Public Records Act (PL 1953, c. 410) – Public Records Retention and Disposal

Records Retention and Disposition

- <u>Records Retention Schedules</u> must be created for all public records maintained by all New Jersey Public Agencies.

- <u>Request and Authorization for Records Disposal</u> must be submitted to obtain authorization *before* the Public Records of these Agencies can be disposed.

Records and Information Management (RIM)

- Documents an Agency's History
- Federal & State Litigation and e-Discovery Support
- Federal & State Audit and Program Review Compliance
- Federal & State Regulatory Compliance
- Fosters OPRA Public Records Access

Records Inventory

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

- How and where it is physically stored
- Volume
- Classification
- Retention Periods as per the Records Retention Schedule
- Disposition
- Applicable Regulations and Codes

Records Retention – Records Retention Schedules

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

Records Retention Schedules address:

- Vital Records
- Legal, Fiscal, & Administrative Value
- Records Retention
- Historical Records
- Confidentiality
- Final Disposition: Permanent, Archives, or Disposal

Records Retention - ARTEMIS

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

ARTEMIS enables users to:

- Search the General Records Retention Schedule and the Agency-specific Records Retention Schedules,

- Create online, electronic Records Disposal Requests for their public records and check their status - Pending, Approved, Denied,

- Produce Authorized Records Disposal Requests for OPRA Records Requests, and

- Create and View Records Retention and Disposal Reports.

Records Retention – ARTEMIS Online Records Retention Schedule

Records Retention Schedule

Records Retention – Hardcopy Records Retention Schedule Report Generated in ARTEMIS

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	Total Retention Period	Minimum Period in Agency	Disposition	Citation
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, disposal authorization *before* records can be destroyed. The authorization:

- Removes OPRA, Legal, and Fiscal Liabilities
- Cost Effective
- Safety
- Identifies a Confidential and Archival Records for Preservation

Records Disposal - ARTEMIS

Records Retention and Disposition Management System (ARTEMIS)

- Search and View Records Retention Schedules and Disposition time periods.
- Create, View, Update, and Submit Disposition Requests.
- Update Disposition Status for agency

Records Disposal – ARTEMIS Request & Authorization

Online Records Disposition Request

Records Preservation & Conservation

- <u>Preservation</u>: preventative maintenance of Active, Inactive, Permanent and Historical Records

- <u>Conservation</u>: "corrective surgery" to records - should be performed by qualified Document Conservationists.

Records Storage - Classifications

- Active Records
  On-site storage

- Inactive Records
  Off-site storage in Government or Commercial Storage

- Historical Records
  A Depository Agreement should be established for the protection of Historical Records.
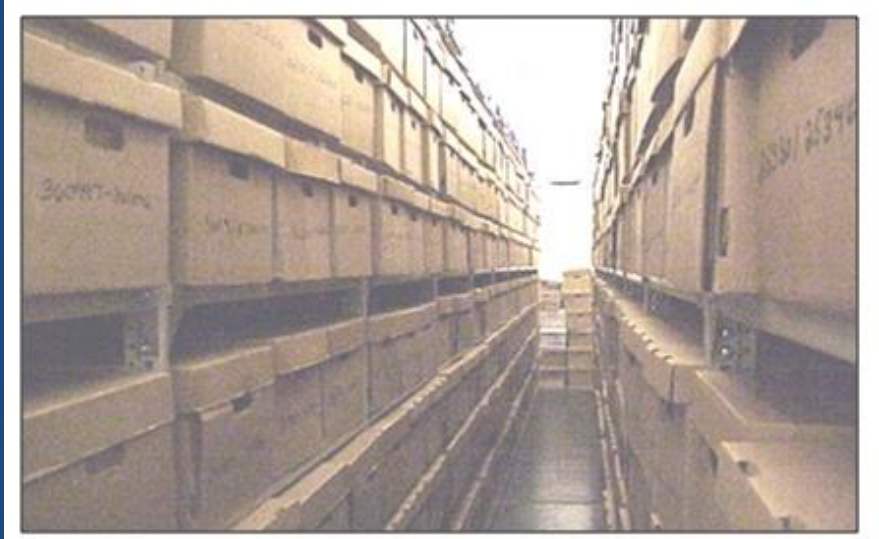
Records Storage – Offsite Facility

A *Records Transfer Request Form* must be used to document the transaction and the *Records Retention Schedule* is used to determine the storage time periods - otherwise unnecessary storage fees could be incurred if records are stored beyond their legal retention period and could be destroyed.

Records and Information Management (RIM) Alternatives

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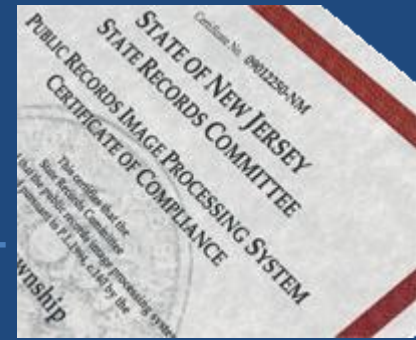
As per PL 1994, c. 140, the State of New Jersey allows for the replacement of hardcopy public records with digital images. The State Records Committee and Records Management Services issue initial imaging system certification to an agency, for an in-house or outsourced imaging application, and annual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

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
- ☐ Data Migration Report (replacement sy

Imaging Registration
Annual Review/Amendment Form

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

ANNUAL REVIEW ☐   AMENDMENT ☐   ANNUAL

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: 2300 Stuyvesant Avenue, Trenton, NJ 08625
609-530-3200

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)

Electronic Records Storage

Fixed (Stand Alone) Storage

•<u>Disk backup</u> – quick access and can hold large amounts of data, can be used for disaster recovery if the server is placed offsite.

Virtual Storage

•<u>Cloud computing</u> – 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 and does not have to be installed per PC. 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

<u>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.</u>

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, <u>and</u> 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.

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

Email - Disposition

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

Email Disposal Request

Social Media

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

- IT IS: global, immediate and accessible.
- IT IS <u>NOT</u>: Private. It is PUBLIC and directives should be established regarding content - language, subject matter, etc.

- It can be used a portal for <u>Cyberattack</u>. Also, it can be <u>altered,</u> which presents a real concern for an agency to release public information.

- Because of this, 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 <u>Disclaimer</u> 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.

The World Wide Web and the Internet of Things

The World Wide Web and the Internet of Things

The World Wide Web via the Internet of Things (IoT) 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 .

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 and content and their respective areas of concern:

- <u>IT Perspective</u> - reflects website creation, maintenance, and growth

- <u>Intellectual Property & Historical Perspective</u> - digitally-born documents if not printed to hardcopy could be lost forever

- <u>Legal Perspective</u> - records needed for Litigation, Legal Rules of Evidence, and e-Discovery

- <u>Financial Perspective</u> - records needed for a Local, State and/or Federal Audit

- <u>Records Management & Access Perspective</u> - 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.

Note: 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

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 <u>Operational Efficiencies</u>, it can also create the potential for <u>Internal & External Operational Vulnerabilities</u> 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

Security – Types of Cyber Attack

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

<u>UNINTENTIONAL</u>:   INTERNAL and/or EXTERNAL ACTIONS

 Accidental access or release of information or its premature, unauthorized or inadvertent disposal.

<u>INTENTIONAL, DELIBERATATE</u>:   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, cyber-intrusions, cyberthreats, cyberterrorists, cyberthieves, cyberwarriors, cyberhacktivists, internal and external sabotage, data mining, data theft and modification, root enablers, Brute-Force attack, Doxing, Point of Sale (POS) malware, browser attack, WannaCry Ransomeware, botnets, botnet bitcoin sales via the Dark Web, Exhaustive Master Key Search attack, ransomware, 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 and identity theft with questionable, CEO Fraud/BEC, threatening sources (gadflies, competitors, third parties, activists, hackers, criminals, terrorists), Fake News, etc.

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.

These basic IT Measures should 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, and

- Implement Intrusion Prevention and Detection Systems.

Vital Records

Records essential to meet operational responsibilities under emergency or disaster conditions. An Agency needs to ask:

"What records are absolutely crucial to operations and can they be recreated from hardcopy , digital, electronic or microfilmed backups if the originals are lost in a disaster?"

Conduct a Risk Analysis by evaluating potential hazards to records:

- Natural & Environmental
- Human inflicted
- Facility related

Determine records protection methods:

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

Identify Vital Records:

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

Disaster Prevention and Recovery & Business Continuity

Procedures and operations <u>before and after</u> a disaster, that identify essential personnel, equipment, and alternate space if a closing of a facility is deemed necessary in order to resume Information Technology 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 - Water is the single most significant culprit in a records disaster
- Protects Vital and Historical Records
- Protects Electronic Records, Hardware, & Software

Business Continuity

- To resume operations quickly and efficiently
- To ensure the normal flow of business

Seaside Heights, NJ – October 2012
Seaside Heights, NJ – September 2013

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, etc. Necessary Information Technology Supplies.
- Necessary Emergency Supplies.

Retain
- Disaster Prevention and Recovery and Business Continuity Plans - copies in safe and accessible Offsite Locations.

A Final Thought, With Some Common Sense…
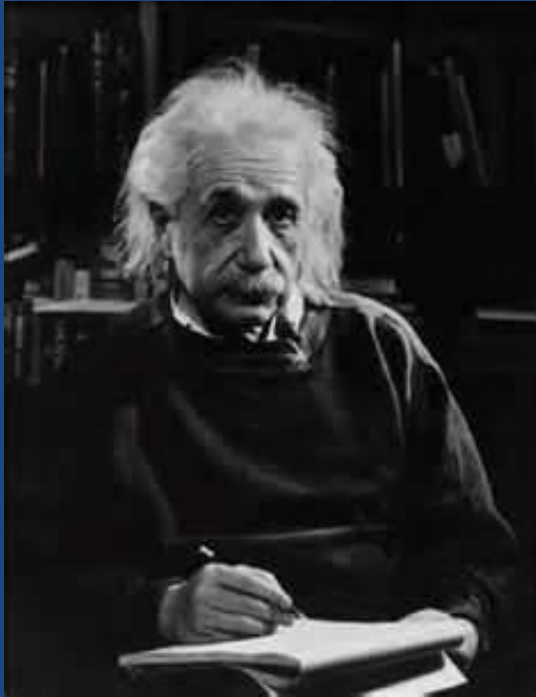
"It has become appallingly obvious that our technology has exceeded our humanity."

Albert Einstein

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

RECORDS MANAGEMENT SERVICES

PO Box 661 Trenton, NJ 08625

Phone 609-777-1020

Thank you.