New Jersey Division of Revenue and Enterprise Services

Records Management Guidelines for Remote Work Settings

11/2020

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

GUIDELINES

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.

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 (HIPPA).

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:
   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.