Destroying Electronic Records

The records retention and disposition schedules provide authority for agencies to destroy public records once they have fulfilled their prescribed retention period. Records should be disposed of in a timely manner once the retention expires. The destruction of all public records must be documented and reported to the Library of Virginia through the submission of a Certificate of Records Destruction (RM-3 Form), as required by the Virginia Public Records Act (Code of Virginia § 42.1-86.1).

I. When can electronic records be destroyed?

The retention period of records, electronic or otherwise, depends on the content of the record rather than the format. Electronic records may fall into various record series with various retention requirements, depending on the information they contain. There is no single retention requirement for electronic records.

To determine the retention period, consult the records retention and disposition schedules: https://www.lva.virginia.gov/agencies/records/retention.asp

Consider whether the electronic records may be non-records as defined by the Virginia Public Records Act (Code of Virginia § 42.1-77). If the electronic records are duplicative or do not pertain to public business, they may be non-records. Non-records may be destroyed at any time, and the destruction should not be reported to LVA.

II. When can backups or duplicates of electronic records be destroyed?

It is advisable and common practice to create regular backups of electronic records, whether stored on-premise or in the cloud, that can be recovered if the original records are lost. Backups of electronic records created for recovery purposes are duplicative of the official records and therefore may be considered duplicative non-records.

Other duplicates of official records can also be considered non-records. For example, attached files sent via email might be duplicative if the official version is stored elsewhere on the agency's recordkeeping system. The proliferation of duplicates can create risk and liability for an agency. Avoid the proliferation of duplicates by sharing access to the official records and working collaboratively on them, rather than sharing and working on multiple versions.

As non-records, backups and duplicates may be destroyed at any time, and the destruction should not be reported to LVA via the Certificate of Records Destruction (RM-3 form). However, backups and duplicates of official records should be destroyed before or at the same time as the official records are destroyed; otherwise, the duplicates may be subject to discovery. If backups are maintained by a vendor, coordinate with the vendor to ensure backups are destroyed.

III. Where can I find the Certificate of Records Destruction (RM-3 Form)?

The Certificate of Records Destruction (RM-3 form) is an online form available on the Records Management Forms page on the LVA website: https://www.lva.virginia.gov/agencies/records/forms.asp

Underneath the RM-3 form, you will also find links to the following resources:

- RM-3 Preparation Instructions (pdf) (videos)
  - The PDF instructions provide detailed information on each step of the RM-3 form process.
  - The videos provide walkthroughs for each step of the RM-3 form process.
- Reporting Destruction Tip Sheet (pdf)
  - The tip sheet provides a few essential facts about destruction requirements and the RM-3 form.
- Volume Equivalency Table (pdf)
  - The table provides the volume (in cubic feet) of common records storage containers.
- In-Progress Dashboard
  - The dashboard allows anyone to monitor the status of a submitted RM-3 form. It shows where the form is in the approval process and the date it was last active.
- Completed Form Search
  - The search tool, available on the LVA website, allows anyone to search for and review the details of completed RM-3 forms. Users can search for RM-3 forms using many criteria, including specific agency information or specific information about the records.

IV. Why should electronic records be routinely destroyed?

The Library of Virginia recommends evaluating electronic records on a regular basis as part of an agency's routine file-cleanup process. Frequency of destruction (monthly, annually, etc.) may vary depending on the agency; the most important thing is that destruction occurs on a regular and consistent basis in order to minimize backlogs and establish a pattern of defensible disposition.

During the file cleanup, destroy electronic records that have fulfilled their retention requirements according to the retention schedules. At the same time, agencies should evaluate whether active web and social media records need to be migrated to another format to prevent obsolescence.

V. How do I determine the volume of electronic records being destroyed?

The volume of electronic records being destroyed must be reported in bytes (e.g., kilobytes, megabytes, gigabytes, terabytes, etc.). The volume should be as accurate as possible but may be an estimate. For many electronic records, the volume can be viewed within the file properties. If you are unable to determine the volume, consult IT staff or a vendor (if applicable) for assistance.

Byte conversions:
1 kilobyte (KB) = 1000 bytes
1 megabyte (MB) = 1000 kilobytes (KB)
1 gigabyte (GB) = 1000 megabytes (MB)
1 terabytes (TB) = 1000 gigabytes (GB)

VI. How do I destroy electronic records?

LVA recommends consulting IT staff or a vendor (if applicable) for assistance in destroying confidential electronic records.

Electronic records are either destroyed confidentially or non-confidentially, depending on the sensitivity of the content. To determine which method is required, consult the “disposition method” column of the retention and disposition schedules.

If the disposition method is Confidential Destruction, or the records are known to contain sensitive content, then they should be destroyed in a way that the information is not recoverable. Merely deleting confidential files is not sufficient, as the files can still be recovered following deletion.

Common confidential destruction methods include:

- Overwriting
- Electronic shredding or incineration
- Degaussing (for magnetic media)
- Physical destruction of storage device

If the disposition method is Non-Confidential Destruction and the records do not contain sensitive information, then the records may be simply deleted (by hitting the Delete key), or the storage device may be sent to a landfill or recycling center.

VII. How do I destroy electronic records when the current database system doesn’t allow for destruction?

If an agency’s existing system is not capable of destroying records, consider the following options:

(1) Retrofit the system to make disposition possible
(2) Migrate all records to a new system that meets requirements
(3) If the current system does not allow for migration, wait until all the records in the system have fulfilled their retention requirements, then dispose of all records within the system

VIII. How do I report the destruction of records that are destroyed automatically?

Some agencies have implemented systems that automatically purge records, e.g., audiovisual recordings, after a pre-determined period of time and, typically, on a daily basis. If the recordings document government business, then they are likely public records and are subject to retention and destruction-reporting requirements. Although not in strict compliance with the Public Records Act, reporting the destruction of already-purged records increases the defensibility of the destruction.

Some systems provide logs or reports of automated destruction which can be used to report destruction to LVA. Other systems do not provide logs, and therefore destruction is challenging to accurately report. For systems that do not provide logs, the LVA recommends following the below steps to estimate the file size of the records subject to destruction:

(1) Select a window of time for which destruction will be reported (monthly, quarterly, etc.)
(2) With the help of internal IT or the system’s supplier/integrator, determine the estimated file size (in bytes) for a data set that spans the same length of the reporting window.
(3) Following the end of the window, report the destruction using the RM-3.

For ongoing destruction reporting of the same records series, the same steps can be taken to estimate file size, or the same estimate can be reported at regular intervals until there is reason to believe the volume has changed (e.g., additional recording equipment has been implemented).