**17 VAC 15-120-10. Definitions.**

The following words and terms when used in this chapter shall have the following meanings unless the context clearly indicates otherwise:

"Electronic record" means records created or stored by electronic means, including but not limited to, computer files and optically scanned files on tapes, disks, CD-ROMs or internal memory.

"Erasure" means to remove electronic information so that it cannot be retrieved from the media on which the information is stored.

"Hardcopy record" means a paper record.

"Redaction" means the process of editing existing printed documents to delete or obliterate information.

"Shredding" means destroying paper records by mechanical cutting. Straight cut shredders cut in one direction only, cross cut shredders cut in two directions, 90 degrees from the other.

**17VAC15-120-20. Purpose.**

To prevent the misuse of personal information it is the obligation of the owners of public records to protect the social security numbers that may be contained in public records. Any public records, irregardless of media, that contain social security numbers have to be destroyed in a confidential manner. These records are to be shredded, made electronically inaccessible or erased so as to make the social security numbers unreadable or undecipherable by any means.

**17VAC15-120-30. Procedures.**

A. Paper Records. There are several accepted methods to destroy paper records containing social security numbers. The method used is determined by the amount of records that need to be destroyed as well as availability of funds and resources. Care must be taken to ensure that until the records are destroyed they are protected from accidental or unapproved access. The acceptable methods of hardcopy destruction are as follows:

1. Shredding involves the use of a mechanical cutter to cut the paper in such a way as to render the document unreadable. There are two forms of acceptable shredders:

a. Cross-cut shredders that reduce sheets of paper into thin strips that when mixed with other shreds cannot be easily recreated into the original document. The strips shall not exceed 3/8 inches in width.

b. Cross-cut shredders that use two sets of cutters set at right angles to each which reduces the paper to a confetti-like substance. This provides maximum protection for privacy protected documents.

2. Use of a commercial shredder. Commercial shredders must be either of the two acceptable types outlined above.

Whether the custodian of the records has the shredding done onsite or offsite a certificate of destruction which lists what records have been destroyed, the date of destruction and who did the shredding is required.

If the shredding is done offsite locked bins are required to protect the records prior to shredding. The company doing the shredding must be bonded.

The agency contracting for the shredding must determine how long after the bins are picked up the contents are shredded and require that the bins are secured until they are shredded. It is the agency's responsibility to protect the social security numbers on the records they collect.

B. Electronic records. Unlike a paper record where it can be visibly determined if the document is unreadable, electronic records require special handling to make information unreadable. Merely using the computer delete key does not actually delete the record. Only the pointer to that information is deleted. It can easily be re-indexed using easily available off the shelf programs. The decentralization of computer based information also results in information being stored on multiple computers, on back-up tapes and portable media.

Processes to protect and destroy social security numbers in electronic format and stored on information or recordkeeping systems must be established.

1. Security. Access to information containing social security information must be restricted to those with a need to know or use. Security parameters of information systems must be established to restrict access to data to only the employees who need this information. If the information system is connected to the Internet it must be protected by a firewall.

2. Control. Limit the number of places where social security numbers are stored in info systems, and limit the locations within each system. Limit the amount of information that is retained on local computers; identify back-up tapes and what is done with them.

3. Records retention. Determine if the social security numbers are required. Determine if the records are covered by a records retention schedule and that the retention schedules are being followed.

4. Destruction. When the records retention has expired and the information needs to be destroyed choose an appropriate method to protect the social security numbers.

a. Files stored on a personal computer must not only be deleted but also overwritten to prevent the information from being reconstructed. Shredder programs are

available that overwrite the data with meaningless data multiple times to totally obliterate the original data. A shredder program must be used to overwrite social security numbers in public records.

b. Back-up tapes must be overwritten at the same time as all other copies are destroyed. These tapes should not be held longer than the retention period for the information retained on them.

c. Data containing social security numbers on floppy disks, tapes and other magnetic storage devices also must be overwritten.

(1.) These materials can be shredded in a shredder to insure that the information is totally destroyed or the materials may be exposed to a powerful magnetic field several times to disrupt the information.

(2.) If magnetic media is used the data must be reviewed to insure that the social security numbers are not retrievable

d. CD-ROMs should be physically broken, into several pieces, to be rendered unusable.

e. When disposing of computers that contain social security numbers or other privacy-protected information care should be taken to protect the information stored in the computers. The hard drives must be wiped clean and inspected to make sure no privacy-protected data remains. It may be necessary to remove the hard drive and dispose of it separately. To assure maximum protection the hard drive can be physically damaged by drilling to prevent it from being used again.

C. Redaction.

1. Hard copy records. Hard copy redaction involves using opaque material to mask off or obliterate the protected information. A permanent ink marker or similar material can be used to mark out the information so that it cannot be viewed; the image may have to be marked out on both sides of the document to prevent image bleed through.

2. Electronic documents. Commercial off the shelf redaction programs are available to accomplish electronically what is done physically with hard copy documents. These programs allow access to redacted documents while retaining un-redacted electronic documents to authorized individuals; this is acceptable as long as only authorized persons have access to the un-redacted information.