

MEDIA SANITIZATION AND DISPOSAL STANDARD

See Also:

RCW [43.105.450](#) Office of Cybersecurity
RCW [43.105.054](#) OCIO Governance

RCW [43.105.020](#) (22) "State agency"
RCW [43.105.205](#) (3) Higher Ed

1. Agencies must establish formal storage [media](#) sanitization and disposal procedures to render the stored data unusable, whether the storage media is reused or destroyed. At a minimum, agencies must:

- a. Ensure that users and custodians of information are aware of its sensitivity and the basic requirements for media sanitization and secure disposal for in accordance with applicable standards and policies. This includes but is not limited to hard drives, solid state drives, removable drives, mobile devices, scanners, copiers, printers, paper copies, and pictures.
- b. Ensure staff responsible for data disposal are trained in records retention requirements and to perform and attest to media sanitization functions. Agencies may use service providers for destruction purposes provided that the information remains secure until the destruction is completed. The service providers must follow this standard. Agencies must ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the information classification standards.
- c. Ensure that media sanitization and disposal documentation is protected against unauthorized access.
- d. Ensure media containing information is protected against unauthorized access, misuse, or corruption from the time it is removed from operational status to the time it is sanitized or disposed, whether within the agency or outside the agency's physical boundaries.

2. Agencies must select from three types of sanitization methods: clear, purge, and physical destruction. For more detail refer to Appendix A of [NIST 800-88](#).

The following table depicts the three types of sanitization methods and the impact of each method.

Sanitization Method	Appropriate Use	Description
Clear	If the media will be reused and will not be leaving the entity's control.	Clearing information is a level of media sanitization that would protect the confidentiality of information. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities.

Sanitization Method	Appropriate Use	Description
Purge	If the media will be reused and leaving the entity's control.	Protects confidentiality of information against an attack through either degaussing or a three-pass wiping procedure compliant with NIST 800-88 .
Physical Destruction	If the media will not be reused at all.	Intent is to destroy the media. Physical destruction may be accomplished by shredding, pulverization or other means that ensure the media can never be re-used. Disposal of physically destroyed media must be conducted in accordance with the Responsible Recycling (R2) standard , the e-Stewards Standard , or some other environmentally responsible way.

3. Agencies must work with the Information Owner to select the sanitization method based on the categorization of the data stored on that media.

- a. Category 1 – Public Information
 - i. If this media will be reused and will not leave agency control, this media must be cleared.
 - ii. If this media will be reused and will leave agency control, this media must be purged.
- b. Category 2 – Sensitive Information
 - i. If this media will be reused and will not leave agency control, this media must be cleared.
 - ii. If this media will be reused and will leave agency control, this media must be purged.
 - iii. If this media will not be reused, it must be destroyed.
- c. Category 3 – Confidential Information
 - i. If this media will be reused and will not leave agency control, the media can be cleared.
 - ii. If this media will be reused and will leave agency control, the media must be purged.
 - iii. If this media will not be reused, it must be destroyed.
- d. Category 4 – Confidential Information Requiring Special Handling
 - i. If this media will be reused and will not leave agency control, the media can be cleared.
 - ii. If this media will be reused and will leave agency control, the media must be sanitized per the special handling requirements commensurate with category 4 data.
 - iii. If this media will not be reused, it must be destroyed.

4. Agencies must maintain records that document all media disposal activities and protect them from unauthorized access. Records for disposed media must include:

- a. Information about the media (type, serial number, other unique identifiers).
 - b. The category of data contained on the media.
 - c. The destination of the media (if known).
 - d. The date the media was sanitized.
 - e. The person performing the activity.
 - f. The method used to render all data unusable (e.g. software tool used or physical destruction of the media).
 - g. The signature of the person responsible for ensuring that all data on the storage media has been rendered unusable.
5. **Agencies must test at least 10% of its sanitized media to assure that proper protection is maintained.**

REFERENCES

1. [NIST 800-88](#)
2. [State Government Records Retention Schedules - WA State Archives - WA Secretary of State](#)
3. [Definition of Terms Used in OCIO Policies](#)
4. [Guidance – Certificate of Sanitization](#)
5. [Responsible Recycling \(R2\) standard](#)
6. [What's the e-Stewards Standard? - e-Stewards](#)

CONTACTS

- For questions about this policy, please contact the [WaTech Policy Mailbox](#).
- For technical security questions or to submit risk assessments, please contact the [WaTech Risk Management Mailbox](#)
- To request a Design Review, please contact sdr@watech.wa.gov.

