How Do You Stop Accidental Data Loss?

Rich Kissel, NIST

Does your organization have systematic procedures to remove sensitive data from obsolete equipment, or is cleanup and disposal of old gear a somewhat *ad hoc* process, as it is in many places? Careless disposal of data storage hardware has led to costly and embarrassing incidents for organizations that discovered too late their inadequate control over media sanitization. Here's an approach to developing a sound process, or for reviewing your sanitization procedures (Kissel et al., Guidelines for Media Sanitization).

Before defining a sanitization process, we need to consider what is meant by "removing sensitive data".

- Clear - Read/Write or Reset commands to the storage device to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques.
- Purge - A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- Destroy - A method of sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Information on an organization's storage devices will have differing levels of confidentiality, and it's important to understand what types of data may be stored on the device to decide the most effective ways to preserve the confidentiality of the data. The risk decision should include the potential consequence of disclosure of information retrievable from the media, the cost of information retrieval and its efficacy, and the cost of sanitization and its efficacy. Additionally, the length of time the data will remain sensitive should also be considered. These values may vary between different environments. Organizations can use Figure 1 to assist in making sanitization decisions that are commensurate with the confidentiality of information on their media. Once organizations decide what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.

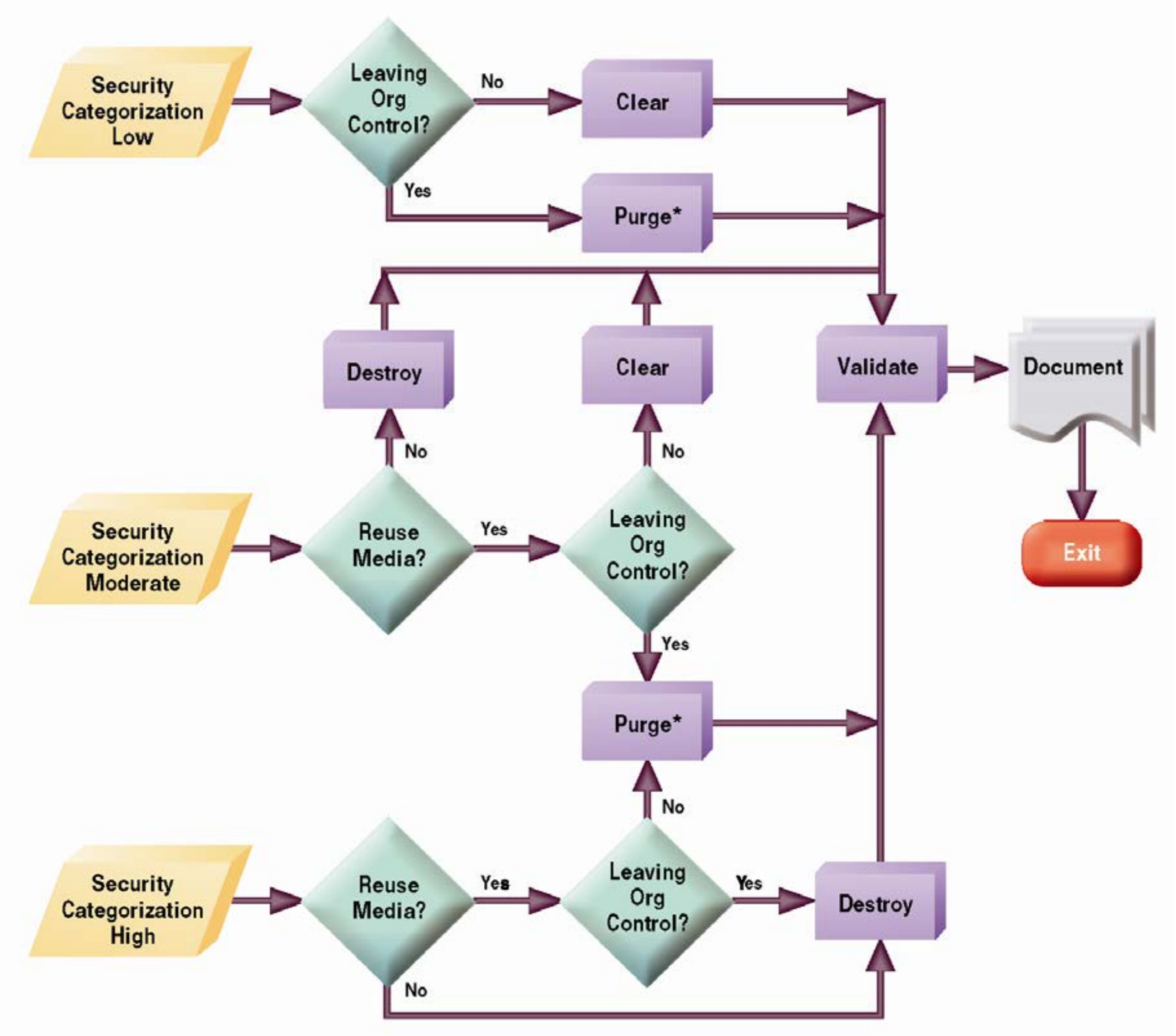

Figure 1. Proper control over media sanitization and disposal involves a series of decisions.

4.1 Information Decisions in the System Life Cycle

Methods to conduct media sanitization should be identified and developed long before arriving at the Disposal phase in the system life cycle. One of the key decisions that will affect the ability to conduct sanitization is choosing what media are going to be used in the system. System owners must understand early on that this decision affects the types of resources needed for sanitization throughout the rest of the system life cycle.

An organization may ask a product vendor for assistance in identifying storage media that may contain sensitive data. This information is typically documented in a ‘statement of volatility’. The statement may be used to support decisions about which equipment to purchase, based on the ease or difficulty of sanitization. For example, the increasing availability of rapidly applicable techniques, such as Cryptographic Erase, provides opportunities for organizations to reduce the risk of inadvertent disclosure by combining sanitization technologies and techniques. For example, an organization could choose to apply Cryptographic Erase at a user’s desktop before removing the media to send it to be ‘formally’ sanitized at the sanitization facility, in order to reduce risk and exposure.

4.2 Determining Security Categorization

Early in the system life cycle the security categorization for the system’s confidentiality will be determined based on information sensitivity, regulations, contractual requirements, and applicable laws. This security categorization is often revisited and revalidated throughout the system’s life, and any necessary changes to the confidentiality category can be made. Once the security categorization is completed, the system owner can then design a sanitization process that will ensure adequate protection of the system’s information.

4.3 Reusing Media

A key decision on sanitization is whether the media are planned for reuse or recycle. Some forms of media are often reused to conserve an organization’s resources. If media are not intended for reuse either within or outside an organization due to damage or other reason, the simplest and most cost-effective method of control may be Destroy.

4.4 Control of Media

A factor influencing an organizational sanitization decision is who has control and access to the media. This aspect must be considered when media leaves organizational control. Media control may be transferred when media are returned from a leasing agreement or are being donated or resold to be reused outside the organization. For example, media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organization are considered to be out of organizational control.

4.5 Data Protection Level

Even within an organization, varying data protection policies may be established. For instance, a company may have an engineering department and a sales department. The sales personnel may not have a need for access to the detailed proprietary technical data such as source code and schematics, and the engineers may not have a need to access the private information of the company's customers. Both might be within the same confidentiality categorization, but contextually different and with different internal and external rules regarding necessary controls.

4.6 Sanitization and Disposal Decision

Once an organization completes an assessment of its system confidentiality, determines the need for information sanitization, appropriate time frames for sanitization, and the types of media used and the media disposition, an effective, risk-based decision can be made on the appropriate and needed level of sanitization. Upon completion of sanitization decision making, the organization should record the decision and ensure that a process and proper resources are in place to support these decisions. This process is often the most difficult piece of the media sanitization process because it includes not only the act of sanitization but also the validation: capturing decisions and actions, identifying resources, and having critical interfaces with key officials.

4.7 Verification Methods

While not obvious at first, verifying the selected information sanitization and Disposal process is an essential step in maintaining confidentiality. Two types of verification should be considered. The first is verification every time sanitization is applied. The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action. If sampling is done after full verification in cases of low risk tolerance then a separate validation tool than the one used in the original verification should be used.

4.7.1 Verifying Equipment

Verification of the sanitization process is not the only assurance required by the organization. If the organization is using sanitization tools (e.g., a degausser or a dedicated workstation), then equipment calibration, as well as equipment testing, and scheduled maintenance, is also needed.

4.7.2 Verifying Personnel Competencies

Another key element is the potential training needs and current expertise of personnel conducting the sanitization. Organizations should ensure that equipment operators are competent to perform sanitization functions.

4.7.3 Verifying Sanitization Results

Verification should ensure that the Target Data was effectively sanitized. When supported by the device interface (such as an ATA or SCSI hard drive or solid state drive), the highest level of assurance of effective sanitization (outside of a laboratory) is typically achieved by a full reading of all accessible areas to verify that the expected sanitized value is in all addressable locations (where the device is in an operational state following sanitization so that data can be read and written through the native interface). A full verification should be performed if time and external factors permit.

Cryptographic Erase has different verification considerations than procedures such as rewriting or block erasing, because the contents of the physical media, following Cryptographic Erase may not be known and therefore cannot be compared to a given value. When Cryptographic Erase is leveraged, there are multiple options for verification, and each uses a quick review of a subset of the media. Each involves a selection of pseudorandom locations to be sampled from across the media

As part of the sanitization process, in addition to the verification performed on each piece of media following the sanitization operation, a subset of media items should be selected at random for secondary verification using a separate validation tool. The secondary validation tool should be from a separate developer. For the secondary validation, a full validation should be performed. At least 20% of sanitized media (by number of media items sanitized) should be verified. The secondary validation provides assurance that the primary operation is working as expected.

4.8 Documentation

Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized, recording bar codes or other identifying information. The decision regarding whether to complete a certificate of media disposition and how much data to record depends on the confidentiality level of the data on the media. For a large number of devices with data of very low confidentiality, an organization may choose not to complete the certificate.

When fully completed, the certificate should record at least the following details:

- Manufacturer
- Model
- Serial Number
- Organizationally Assigned Media or Property Number (if applicable)
- Media Type (ie magnetic, flash, hybrid, etc.)
- Media Source (ie. user or computer the media came from)
- Method Used (ie. degauss, overwrite, block erase, crypto erase, etc.)
- Pre-Sanitization Confidentiality Level Sanitization Description (Clear, Purge, Damage, Destruct)
- Tool Used (including version)
- Verification Method (ie. full, quick sampling, etc.)
- Post-Sanitization Confidentiality Level
- If known, post-sanitization destination
- Personnel conducting the sanitization
- Data Backup (ie. if data was backed up, and if so, where)

Conclusions

Media sanitization is one of the most neglected, yet critically important, aspects of information security. Using the outline in this article, organizations can develop an effective and cost-efficient approach to the problem, helping to ensure that sensitive information is protected.

References

R. Kissel, M. Scholl, S. Skolochenki, X. Li, Guidelines for Media Sanitization, Revision 1, National Institute of Standards and Technology, Sept. 2012.

Acknowledgments

Any mention of commercial products or reference to commercial organizations is for information only; it doesn’t imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.