

## Kansas Information Technology Executive Council Security Council

### Media Sanitization Best Practice Whitepaper

This paper defines media sanitization and how it fits into an overall security program; it's based on the National Institute of Standards and Technology Special Publication 800-88 (NIST SP 800-88).

#### Media Sanitization

When electronic media is repurposed or retired, it's the responsibility of the data owner—the representative of the responsible organization—to ensure the data currently or previously stored on that media is not easily accessible.

Media sanitization is another control, or safeguard, that should be implemented in accordance with risk management principles and incorporated into local information technology security policies. Reasonable assurance varies based on the sensitivity of the information and the retrieval methods most likely to be used by an attacker. The method used depends on the reward or value derived from obtaining the data versus the work factor and costs associated with available retrieval resources.

#### Guidelines for Media Sanitization

According to the NIST Guidelines for Media Sanitization, there are four sanitization processes (Scholl et al, 2006)—disposal, clearing, purging, and destruction.

**Disposal** – The process of disposal essentially consists of tossing the media in a dumpster with no attempt to hinder or prevent the recovery of data. This also includes the reuse of disks, tape, or memory without taking steps to protect information that may have been stored during previous operational use. It's acceptable to follow a simple disposal process when the data stored on the media is classified as "public". In other words, the release of the information will not cause harm to the organization, its employees, its shareholders, or its customers.

**Clearing** – Clearing requires taking steps to prevent the recovery of data through a keyboard attack. As we've seen, this requires more than deleting files. At least a single overwrite of the writable areas of the media must be completed. A single overwrite significantly increases the effort, or work factor, required to recover information. Not only does the attacker need physical access to the media, but recovery requires the use of lab-based tools. Clearing is acceptable when release of the information stored would cause only moderate harm to the organization, its employees, its shareholders, or its customers.

**Purging** – Purging is necessary when the compromise of the information stored on the media will result in serious--and possibly unrecoverable--harm to the organization, its employees, its shareholders, or its customers. Data is overwritten at a minimum of 3 times to increase the work factor of lab-attack attempts to a level that exceeds the data's value to the attacker. It should be noted that some Federal entities require more passes. Ideally, all remnant data is removed.

**Destroying** – Purging is a good way to retain media you wish to reuse. However, the best process for ensuring the irretrievability of highly sensitive data is to destroy the media. During the destruction process, media is reduced to a state in which both keyboard and lab attack attempts are impossible.

Again, the process you select depends on the sensitivity of your information and the potential impact on your organization if the information is compromised. Below is a list of approved resources for different methods of performing media sanitization.

Reuse:

<http://www.killdisk.com/> Magnetic Storage HDDs - PC/Intel compatible processors

<http://www.superscrubber.com/> Magnetic Storage HDDs - Apple Mac machines

Destruction:

[http://www.nsa.gov/ia/government/MDG/NSA\\_CSS-EPL-02-01.pdf](http://www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-02-01.pdf) - NSA/CSS Evaluated Products List (EPL) for High Security Crosscut paper Shredders, Annex A to NSA/CSS 02-01, version M, dated: April 2005

[http://www.nsa.gov/ia/government/MDG/NSA\\_CSS-EPL-02-02.pdf](http://www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-02-02.pdf) - NSA Evaluated High-Security Disintegrators, Annex A to NSA/CSS 02-02, version F, dated: April 2005

[http://www.nsa.gov/ia/government/MDG/NSA\\_CSS-EPL-04-02.pdf](http://www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-04-02.pdf) - Optical Media Destruction Devices, Annex A to NSA/CSS 04-02, version B, Date: 30 September 2005

[http://www.nsa.gov/ia/government/MDG/NSA\\_CSS-EPL-9-12.PDF](http://www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-9-12.PDF) - Degausser Approved Products List - Annex A to NSA/CSS Manual 130-2, version B, dated: May 2005”

[http://www.nsa.gov/ia/government/MDG/NSA\\_CSS-EPL-04-01.pdf](http://www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-04-01.pdf) – Punched Tape Destruction Devices – Annex A to NSA/CSS 04-01 29 July 2005

#### Works Cited

- NCSC (1991). *A guide to understanding data remanence in automated information systems*. Retrieved January 14, 2008 from <http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-025.2.txt>
- Scholl, M., Kissel, R., Skolochenko, S., & Li, X. (2006, February). *Guidelines for media sanitization (NIST SP 800-88, Public Draft)*. Retrieved January 14, 2008 from [http://csrc.nist.gov/publications/drafts/DRAFT-sp800-88-Feb3\\_2006.pdf](http://csrc.nist.gov/publications/drafts/DRAFT-sp800-88-Feb3_2006.pdf)
- Olzak, Tom (June 2006). *Fundamentals of Storage Media Sanitization*. Retrieved January 14, 2008 from [http://adventuresinsecurity.com/Papers/Fundamentals\\_of\\_Media\\_Sanitization.pdf](http://adventuresinsecurity.com/Papers/Fundamentals_of_Media_Sanitization.pdf)