Media Sanitization and Disposal Policy
Kansas State University

December 14, 2008, *revised April 29, 2009*

Table of Contents

.010 Purpose

The purpose of this policy is to protect University Data from unauthorized disclosure. This policy defines the requirements for ensuring University Data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools – even data from files that were deleted long ago or a hard drive that was reformatted. Failure to properly purge data in these circumstances may result in unauthorized access to University Data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

.020 Scope

This policy applies to all university colleges, departments, administrative units, and affiliated organizations.

.030 Effective Date

This policy will be effective upon approval by the Computing Executive Committee [*replace with date after CEC approval*].

.040 Authority

The state of Kansas *Enterprise Media Sanitization and Disposal Policy* requires all state agencies, including Regents' institutions, to "establish policies and procedures for the sanitization of all media including hard copy and electronic." It also instructs Regents' institutions to use "the guidelines contained in NIST Special Publication 800-88 or an approved established industry best practice for higher education technical environments or institutions."

The Health Insurance Portability and Accountability Act of 1996 specifies requirements for disposal, media reuse, and accountability for electronic protected health information.

The Internal Revenue Service (IRS) Publication #175, *Tax Information Security for Federal, State, and Local Agencies and Other Entities*, specifies security controls for protecting the confidentiality of Federal Tax Information that includes media reuse and disposal.

.050 Policy

To prevent unauthorized disclosure of University Data, media leaving control of the responsible department and destined for reuse or disposal must have all University Data purged in a manner that renders the data unrecoverable.

Media that will be reused within the department should likewise have all University Data purged to prevent unauthorized disclosure.

Media containing University Data authorized for transfer to individuals or organizations outside the University are exempt.

.060 Definitions

A. *Affiliated Organization* - any organization associated with the University that uses university information technology resources to create, access, store or manage University Data to perform their business functions.

B. *Confidential Data* – Highly sensitive University Data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. See K-State's *Data Classification and Security Policy* for an expanded definition and examples.

C. *DeGaussing* – demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded. ~~disposed~~.

D. *Disintegration* – A physically destructive method of sanitizing data; the act of separating into component parts.

E. *HIPAA* – Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.

F. *Incineration* – A physically destructive method of sanitizing media; the act of burning completely to ashes.

G. *Internal Data* – University Data intended for internal University business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. See K-State's *Data Classification and Security Policy* for an expanded definition and examples.

H. *Media* – material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.

I. *Media sanitization* – the process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

J. *Public Data* – University Data explicitly or implicitly approved for distribution to the public without restriction. See K-State's *Data Classification and Security Policy* for an expanded definition and examples.

K. *Pulverization* – A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

L. *Purging* – a media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

M. *University Data* – Any data related to Kansas State University ("University") functions that are a) stored on University information technology systems, b) maintained by K-State faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

.070 Roles and Responsibilities

The local department is responsible for ensuring that University Data are properly removed or destroyed from media before it leaves the control of the department for reuse or disposal.

.080 Implementation Procedures

While the primary purpose of this policy is to protect non-public University Data (e.g., data classified either internal or confidential), it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient and cost effective to purge *all* University Data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside the University, all University Data must be purged from the media before giving it to the third party.

Specific instructions for different types of media and regulations follow.

A. *Electronic Storage Media (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, etc.)*

1. If purging is done by overwriting the data, the *entire media/device* must be overwritten with a minimum of three passes.

2. Equipment that can store University Data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the University should have all data storage devices removed before disposition. If the equipment leaving University control must retain the data storage devices, all University Data must be properly purged.

3. The only acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, or incineration.

4. Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.

B. *Paper-Based Media*

1. Any paper-based or other hard copy media containing ~~internal or~~ confidential University Data must be shredded with a cross-cut shredder before disposal or transferred to an

authorized third party contracted by the University for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (~1/32”x1/5”). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the institution, an affiliated organization, or an individual. The maximum particle size for media containing internal data is ~~of~~ 2x15 mm (~1/16”x3/5”).

2. Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

C. *Optical Media (e.g., CDs and DVDs)*

Optical media containing internal or confidential University Data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

D. *Smartphones, Personal Digital Assistants (PDAs), and other handheld devices*

Mobile devices like Smartphones (e.g., Blackberry or Treo), PDAs, MP3 players, and even regular cell phones store information and often contain personal or other sensitive information. Any University Data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.

E. *Other Media Types*

For other media and additional guidelines, refer to National Institute of Standards and Technology (NIST) Special Publication 800-88, table A-1 “Media Sanitization Decision Matrix,” in Appendix A, *Minimum Sanitization Recommendations for Media Containing Data*.

F. *Export controls*

Media containing University Data in equipment that will be reused outside the United States must comply with export laws and regulations according to K-State’s Export Control Program.

G. *Electronic Protected Health Information*

K-State units responsible for electronic protected health information covered by HIPAA must also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, *Physical Safeguards*, part (d), (1) & (2).

H. *Federal Tax Information*

K-State units handling Federal Tax Information must also have media sanitization and disposal policies and procedures in accordance with IRS Publication #175, *Tax Information Security for Federal, State, and Local Agencies and Other Entities.*

I. *More Information*

For more information about media sanitization and disposal, including suggested software tools for purging hard drives and other K-State-specific resources and procedures, see K-State’s Media Sanitization and Disposal web site (www.k-state.edu/infotech/security/media).

.090 Related Laws, Regulations, or Policies

A. *Enterprise Media Sanitization and Disposal Policy*, state of Kansas IT Executive Council (ITEC) Information Technology Policy 9400 – January 2009 (www.da.ks.gov/itec/Documents/ITECITPolicy7900.htm)

B. K-State *Data Classification and Security Policy* – January 2009 (insert URL when it's available in the PPM)

C. *Guidelines for Media Sanitization*, NIST Special Publication 800-88 (csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)

D. K-State export control program (urco.k-state.edu/ECPOverview.html)

E. Chapter 6510, "Property Management", in K-State's Policy and Procedures Manual (www.k-state.edu/policies/ppm/6510.html)

F. HIPAA Final Security Rules, Section 164.310, *Physical Safeguards,* part (d), (1) & (2)

G. IRS Publication #175, *Tax Information Security for Federal, State, and Local Agencies and Other Entities.* February 2007. (www.irs.gov/pub/irs-pdf/p1075.pdf)

.100 Questions/Waivers

The Vice Provost for Information Technology Services (VP ITS) is responsible for this policy. The VP ITS or designee must approve any exception to this policy. Questions related to the policy should be directed to the Chief Information Security Officer.

Note on where to publish this policy in K-State's PPM

This policy needs to replace or be referred to by section .085 "Disposal of Computers", chapter 6510 "Property Management" of K-State's Policies and Procedures Manual (www.k-state.edu/policies/ppm/6510.html#.085 Disposal of Computers), which currently states:

> It is the responsibility of the department to ensure that all sensitive information is removed from the computer, before it is disposed of by the department after local disposition has been authorized.
>
> In order to maximize the value of the computer and at the same time ensure compliance with software license agreements, it is important that the department owns a transferable license for any operating system that is left on the surplus computer and it is the only copy.

The first paragraph should be replaced by a reference to this policy. The second paragraph should be revised as follows:

> If a surplus computer is to be transferred to another entity for continued use, the license(s) for any software remaining on the computer, such as the operating system, must be transferable to the receiving department in order to maximize the value of the computer and ensure compliance with software license agreements. The transferring department is responsible for making sure no other copies are retained unless allowed by license agreements.

Disposal of equipment and media and removing sensitive data from them before disposal is addressed in both the "Physical and Environmental Security" and "Communications and Operations Management" sections of the ISO/IEC 27001:2005 IT security standard. I recommend this policy be grouped with the new K-State Physical Security policy and referenced in a future "Communications and Operations Management" security policy.