DATA DESTRUCTION & SANITIZATION POLICY

POLICY# OTECH-POL2019-006

FRANK L.G. LUJAN, JR. – CHIEF TECHNOLOGY OFFICER
OFFICE OF TECHNOLOGY, GOVERNMENT OF GUAM
Otech.guam.gov

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

JULY 19, 2019

Contents

Overview

Policy Number:	OTECH-POL2019-006
Title:	Data Destruction and Sanitization Policy
Purpose:	To provide proper procedures for disposal and disposition of surplus computer hardware and other storage media.
Authority:	5 GCA Chapter 1 Office of the Governor § 12.106 (f)
Publication Date:	July 19, 2019
Policy Approval:	Frank L.G. Lujan, Jr. Chief Technology Officer
Target Audience:	All OTECH employees, contractors, vendors and third parties. **The intended recipients of this policy also include all entities under the authority of the Office of Technology, pursuant to 5 GCA Chapter 1 Office of the Governor § 12.102**
Contact Details:	**Office of Technology** 211 Aspinall Avenue Hagatna, Guam 96910 O: 671.635.4500 F: 671.472.9508 otech.guam.gov

Revision History

Date of Change	Responsible	Summary of Change
December 2017	OTECH Systems Support	Draft policy
February, March 2019	OTECH Systems Support	Update policy and format
July 2019	OTECH Data Processing Manager and CTO	Review, approve and disseminate policy

Introduction

Proper disposal and disposition of surplus computer hardware and other storage media manages risks of security breach and inappropriate information disclosure. Broadly, exposure to an Agency takes the form of:

- **Violation of Software License Agreements** – Most software is licensed for use on either a single computer system, to a single person, or to an organization. Typically, licenses are not transferable. Even when licenses are transferable, there are generally specific requirements that must be met in order to effect a transfer. Allowing a third party access to licensed software without proper transfer of the license may be a breach of the license agreement, and may subject the state or the recipient of the software to claims and/or damages.
- **Unauthorized Release of Confidential Information or Personally Identifiable Information (PII)** – Allowing an unauthorized person access to Confidential Information or PII can subject an Agency to claims for damages.

This policy is designed to address proper disposal procedures for Confidential Information and/or PII from an Agency surplus assets prior to their disposal. Proper sanitization and disposal procedures are key to ensuring data privacy and license compliance.

Policy

The Office of Technology (OTECH) understands that Agencies regularly store sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media reach end of life, sensitive information on surplus equipment and media must be properly destroyed or otherwise made unreadable to protect Confidential Information or Personally Identifiable Information (PII).

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled and managed by the Office of Technology. Data remains present on any type of storage device (whether fixed or removable) even after a disk is “formatted”, power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the media removes information in such a way that the data recovery using common techniques or analysis is greatly reduced or prevented.

Procedures

All Government of Guam issued computer desktops, laptops, hard drives, and portable media must be processed through the Office of Technology for proper disposal. Paper and hard copy records shall be disposed of in a secure manner as specified by the respective Agency’s archiving and destruction policy.

Types of Sanitization

In accordance with NIST SP 800-88 Rev.1, three primary actions can be taken to sanitize media – Clear, Purge and Destroy.

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge** applies physical or logical techniques that render Target Data[i] recovery infeasible using state of the art laboratory techniques.
- **Destroy** renders Target Data recovery infeasible using state of the are laboratory techniques and results in the subsequent inability to use the media for storage of data.

The NIST SP 800-88 Rev.1 guideline insinuates that the terms "clear" and "purge" are interchangeable. It is determined that, in this document, "clearing" satisfies NIST's guidance for "purging."

Selection & Methods

The following tables are used to select the sanitization method whose thoroughness corresponds to the security category of the information on the storage device to the device's future use.

Sanitization Method – Low or Moderate Impact Level

Security Impact Level: **LOW or MODERATE**		Acceptable Sanitization Methods	
		Clear	**Destroy**
Future Control of the Storage Device	Repurposed or Reissued **(under OTECH control)**	YES	N/A
	Repurposed or Reissued **(not under OTECH control)**	YES	N/A
	Discarded **(not under anyone's control)**	NO	YES

Sanitization Method – High Impact Level

Security Impact Level: **HIGH**		Acceptable Sanitization Methods	
		Clear	**Destroy**
Future Control of the Storage Device	Repurposed or Reissued **(under OTECH control)**	YES	N/A
	Repurposed or Reissued **(not under OTECH control)**	NO	YES
	Discarded **(not under anyone's control)**	NO	YES

The following tables are used to determine the device's appropriate mechanisms to carry out the information sanitization and disposition methods.

1.1 Hand-held Devices

Type of Hand-Held Device	**Clear** mechanisms	**Destroy** mechanisms
Cell Phones	• Delete all information manually (This includes the call history and all phone numbers) • Perform a full reset (Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.)	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility
Personal Digital Assistants (PDAs)	• Delete all information manually • Perform a full reset (Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.)	• Shred • Pulverize • Incinerate it in a licensed facility

1.2 Networking Devices

Type of Networking Device	**Clear** mechanisms	**Destroy** mechanisms
Routers (any type)	• Perform a full reset (Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.)	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility

1.3 Magnetic Disks

Type of Magnetic Disk	**Clear** mechanisms	**Destroy** mechanisms
ATA Hard Drives	• Purge with agency-approved and validated purge techniques or tools	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility
USB Removable Storage (Pen drives, thumb drives, flash drives, memory sticks, or USB-powered hard drives)	• Purge with agency-approved and validated purge techniques or tools	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility
Zip Disks	• Overwrite the entire medium using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Incinerate it in licensed facility

SCSI Drives	• Overwrite the entire medium using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility

1.4. Magnetic Tapes

Type of Magnetic Tape	**Clear** mechanisms	**Destroy** mechanisms
Tapes	• Overwrite the tape	• Incinerate the tapes in a licensed facility • Remove magnetic strips from encasing and shred

1.5 Optical Drives

Type of Memory	**Clear** mechanisms	**Destroy** mechanisms
CDs	• Use the **Destroy** mechanisms	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility
DVDs	• Use the **Destroy** mechanisms	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility

1.6 Memory

Type of Memory	**Clear** mechanisms	**Destroy** mechanisms
Compact Flash Drives, SD	• Overwrite the entire medium using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility

RAM	• Purge the DRAM as follows:
	  ○ Power it off
	  ○ Remove the battery (if there is one)
	• Perform a full chip purge as described in the manufacturer's data sheets
	• Overwrite the entire medium using agency-approved and validated
		• Shred
		• Disintegrate
		• Pulverize
		• Incinerate it in a licensed facility

	overwriting technologies, methods, and tools • Use Destroy mechanisms	
Flash Cards	• Overwrite the entire medium using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Disintegrate • Pulverize

1.7 Magnetic Cards

Type of Magnetic Card	**Clear** mechanisms	**Destroy** mechanisms
Magnetic Cards	• Overwrite the entire media using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Incinerate it in licensed facility

1.8 Other Equipment

Type of Equipment	**Clear** mechanisms	**Destroy** mechanisms
Copy Machines	• Perform a full reset (Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.)	• Shred • Disintegrate • Pulverize • Incinerate it in licensed facility
Fax Machines	• Perform a full reset (Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.)	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility

Approved Sanitization Tools

OTECH has approved the use of the following tools:

Product Name	**Website**
Secure Erase	http://cmrr.ucsd.edu/people/Hughes/secure-erase.html
Wipe Drive Enterprise	https://www.whitecanyon.com

Roles & Responsibilities

Responsibilities for data destruction and sanitization are as follow:

Role	Responsibility
OTECH Chief Technology Officer (CTO)	• Overall responsibility for promulgating the data destruction and sanitization policy • Overall responsibility for ensuring that organizational or local sanitization requirements follow the guidelines of this document • Overall responsibility for reviewing and updating this policy on an annual or as needed basis
Agency Heads (i.e. Directors, Chiefs, etc.)	• Overall responsibility for ensuring that adequate resources are applied to the information security program and ensuring program success • Overall responsibility for ensuring that the resources are allocated to correctly identify types and locations of information and to ensure that resources are allocated to properly sanitize the information • Ensure that maintenance or contractual agreements are in place and are efficient in protecting the confidentiality of their respective Agency's system media and information commensurate with the impact of disclosure of such information on the organization • Adhere to the license terms and agreements for software on a computer that is being transferred to another Agency or surveyed. • Overall responsibility for determining if the data is security-sensitive and method of data destruction or sanitization • Overall responsibility to ensure that all their respective employees, third party vendors, contractors and visitors comply with this policy • Ensure this policy is updated on an annual or as needed basis • Support the OTECH CTO with new security implementations and protocols pertaining to this policy • Report any violation of this policy directly to OTECH resource in a timely manner

[i] Target Data – the data subject to the sanitization technique (NIST SP 800-88 Revision 1, Guidelines for Media Sanitization - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)