Policy & Procedure No. 7.005

Nunez Community College

Title: Data Sanitization Policy

Effective Date: 11-9-2018

Last Revision Date: 2014-2015
Cancellation:

Department/Office: Information Technology

PURPOSE

In accordance with DOA OIT Policy-Data Sanitization IT POL 1-04 and LCTCS sanitization policies, Nunez has created this policy to ensure all discarded devices (be it surplus or other means) have been properly wiped of critical college data.

SCOPE

Any electronic device or media owned, managed, leased or utilized by Nunez Community College with the ability to store, process, or transmit Internal, Confidential, or Restricted Data. Examples include, but not limited to, Hard Drives, CDs, Backup Tapes, USB Drives, Smart Phones, Tablets, Fax Machines, Routers, Firewalls, VOIP Handsets, Network Storage Devices, and Printers.

The following requirements should also be referenced when specifying Data Sanitization requirements for contracted Partners or Service Providers storing or processing State Data.

POLICY

PROCEDURE FOR SANITZATION OF DATA FROM COMPUTER STORAGE MEDIA

SERVERS AND WORK STATIONS: all obsolete workstations and servers will have their hard drives wiped utilizing Derrik's Boot and Nuke to ensure that sensitive data is completely unrecoverable. Boot and Nuke utilizes a deletion process in which all spaces on the hard drive are overwritten with random characters. Three passes are made on the hard drive's spaces to ensure that the data is completely destroyed. Hard drive that have been identified as having held financial data will be first wiped with Boot and Nuke and then removed from the computer before disposal of the system. These, and any hard drives in which the software fails to wipe the data successfully, will be destroyed by physical means.

Definitions:

Tape Media: Retired tape media will be destroyed by incineration.

Optical Media: Optical media, such as CD/DVD Rom discs will be destroyed via physical means. Flash drives that are no longer functional will be destroyed by physical means.

Once a device has been properly sanitized, documentation containing the following sanitization codes is provided to the property office and a copy maintained in the IT office once the device has been turned over to property for surplus purposes:

Office Equipment	**ND**	N/A	**No Data**	Reusable
HDD, SSD	**OWS**	Overwrite	**Success**	Reusable
Facsimile, Office Equipment, Network Device, Mobile Device	**MRS**	Reset	**Success**	Reusable
RAM	**PRS**	Removed Power	**Success**	Reusable
HDD	**OWFD**	Overwrite	**Failure** – Marked for Degaussing	Not Reusable
HDD, SSD	**OWFMD**	Overwrite	**Failure** – Marked for Destruction	Not Reusable
Network Device, Mobile Device	**MRFMD**	Reset	**Failure** – Marked for Destruction	Not Reusable
Facsimile, Office Equipment, Network Device, Mobile Device, Magnetic Tape, ROM	**DS**	Destruction	**Success**	Not Reusable
HDD, SSD	**OWFDS**	Destruction	**Success**	Not Reusable
HDD, Magnetic Tape	**DGS**	Degaussed	**Success**	Not Reusable
Optical Media	**OMDS**	Destruction	**Success**	Not Reusable
Removable Media	**RMDS**	Destruction	**Success**	Not Reusable

X	Reviewing Council/Entity	Review Date	Effective Date
X	Office of Information Technology	10-2018	11-8-2018
X	College Compliance Committee	11-2018	11-8-2018

Policy Referenced: LCTCS Procedure for Sanitization of Data from Computer Storage Media

Distribution: Distributed Electronically via College's Internet 1-14-2019

Chancellor's Signature/Approval

SIGNATURE:_____ DATE: 11-15-2018
Tina M. Tinney, Ed.D.
Chancellor