NORTHERN
NEW MEXICO COLLEGE

Your school, your future.

Hardware Sanitization Policy

Purpose

The purpose of this policy is to protect the intellectual property of Northern New Mexico College and the confidentiality of personal information. It defines standards and procedures for the pre-disposal data sanitization of NNMC's hardware. This policy applies to, but is not limited to, all devices that fit the following device classifications:

- Portable and notebook computers running Windows, UNIX, Linux, or Mac OS operating systems.
- Workstations running Windows, UNIX, Linux, or Mac OS operating systems.

The following devices and storage media are not specifically addressed by the terms of this policy, but must be sanitized accordingly:

- Servers should be backed up and sanitized in accordance with vendor recommendations. If the vendor has not provided recommendations, servers can be sanitized as workstations.
- Mobile devices, such as PDAs and smart phones, must be destroyed by crushing, incineration, shredding, or melting prior to disposal.
- Removable storage media such as flash memory devices, floppy disks, optical CD and DVD media, tape, and other long-term storage media must be destroyed by incineration, shredding, or melting prior to disposal.

Scope

The policy applies to all hardware owned or leased by NNMC and capable of storing NNMC's intellectual property or information related to the privacy of NNMC's employees, clients, or suppliers.

Scenarios for Disposal

NNMC recognizes two different categories for the disposal of hardware:

1. Hardware transferred internally. Hardware may not require sanitization if it is transferred to another user within the same department. Hardware that is either transferred to a different department or to an employee with less authority must be sanitized as *hardware transferred externally*. End users may choose to sanitize personal information from hardware using a sanitization tool provided by the IT department.

2. Hardware transferred externally. All hardware transferred externally must be sanitized according to the methods defined in this policy. This scenario includes:

    a. Hardware transferred to the private ownership of employees.

b. Hardware donated to charitable organizations.

c. Hardware returned to a lessor.

d. Hardware returned to a vendor for servicing or maintenance.

e. Hardware released to an external agency for disposal.

Policy Statement on Sanitization

Consult with the IT department prior to disposing of any computer equipment. Jorge C. Lucero is the primary contact for sanitization issues. They will provide an approved sanitization tool and provide assistance in properly sanitizing the hardware. Department chairs or their designee must sign a certification that the equipment has been properly sanitized before it can be surplused, transferred, or donated. Copies of all certification statements should be maintained by IT staff.

Technical Guidance on Sanitization

Two different methods may be used to sanitize hardware.

1. Physical destruction. Hardware may be sanitized through crushing, shredding, incineration, or melting.

2. Digital sanitization. Deleting files is insufficient to sanitize hardware. A digital sanitization tool must be used. The tool must conform to the following standard[s]:

    a. RCMP TSSIT OPS-II (Royal Canadian Mounted Police Technical Security Standards for Information Technology, Appendix OPS-II).

    b. DoD 5220-22.M.

    c. The Gutman Wipe.

    d. Pseudo Number Random Generator PRNG Stream with eight passes.

Policy Non-Compliance

The Vice-President Finance, Chief Operating Officer, and the employee’s immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action, up to and including termination of employment.

Contacts

If you have any questions or concerns regarding this policy, or would like to report a policy violation, contact the following policy administrator(s):

- Jorge C. Lucero

Declaration of Understanding

I, [_______________], have read, understand, and agree to adhere to [company name]'s Hardware Sanitization Policy.

Name (Printed): ___________________________________

Name (Signed): ___________________________________

Today's Date: ___________________________________