Electronic Media Disposal

ROWAN UNIVERSITY POLICY

Title: Electronic Media Disposal Policy
Subject: Information Security
Policy No: ISO:2013:04
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Information Security Officer
Date Adopted: 07/01/2013
Last Revision: 09/15/2023
Last Review: 09/15/2023

I. PURPOSE

The purpose of this policy is to establish a standard for the proper disposal of media containing electronic data. The disposal procedures used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Information Security Officer shall implement and ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy in their respective areas as needed.

III. APPLICABILITY

This policy applies to all members of the Rowan community who access and use the University's electronic information and information systems. This policy, in addition to the Acceptable Use Policy, governs access and use of the University's electronic information and information systems originating from non-Rowan computers, including personal computers and other electronic devices. The access and use of electronic information provided by research and funding partners to Rowan is also governed by this policy.

The use of information systems acquired or created through use of University funds, including grant funds from contracts between the University and external funding sources (public and private), are covered by this policy. This includes University information systems that are leased or licensed for use by members of the Rowan community.

IV. DEFINITIONS

Refer to the Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy.

V. POLICY

1. All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.
    a. Approved Sanitization Methods

i. **Overwriting**: Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. S anitization is not complete until the three overwrite passes and a verification pass are completed.
ii. **Destruction of Electronic Media**: Destruction of electronic media is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the media such as a computer, tape reader, audio or video player.

b. Non-Approved Sanitization Methods

i. **Clearing Data:** Clearing data such as formatting or deleting information removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. Because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing media intended for disposal outside of the University.

2. Disposal of Hard Drives

a. Disposal of Hard Drives to Other Departments or outside the University

i. Prior to disposal, operable hard drives must be overwritten in accordance with the procedures in section V.2.a above. The owner must be able to certify that the hard drive was properly sanitized. Written certification should include the make, model, and serial number of the hard drive and the date that the procedure was performed. Equipment designated for surplus or other disposal must have a label affixed stating that the hard drive has been properly sanitized. The label should be a high visibility color that is easily recognizable.

b. Transfer of Hard Drives within a Department

i. Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. It is recommended that all electronic media be sanitized per section V.2.a above; however, since the media is remaining within the department, the hard drive may instead be formatted prior to transfer. Since, special recovery tools must be used by an individual to access the data erased by this method any attempt by an individual to access unauthorized data would be viewed as a conscious violation of Rowan University Information Security Policy and possibly regulatory statutes such as HIPAA, FERPA, GLBA, etc., depending on the nature of the data.

c. Sending a Hard Drive out for Repair or for Data Recovery

i. The vendor repairing or recovering data on the hard drive must have signed an appropriate Non-Disclosure Agreement, Business Associate Agreement and/or Security Contract Language with Rowan University, stating that they will take proper care of the data. Once data is recovered or the hard drive is repaired the original hard drive must be returned to the owner so that the owner can dispose of it per this policy for proper disposal of hard drives.

d. Repairing a Hard Drive Under Warranty

i. In the special situation where a hard drive under warranty has failed and the manufacturer requires that the failed disk drive be returned, an appropriate Non-Disclosure Agreement, Business Associate Agreement and/or Security Contract Language between the manufacturer and Rowan University must be in place before the drive can be shipped to the manufacturer. If the manufacturer will not sign the appropriate agreement, then the old drive must be properly destroyed and the owner of the system must cover any costs associated with purchasing a new drive.

e. Disposal of Damaged or Inoperable Hard Drives

i. The owner must first attempt to overwrite the hard drive in accordance with the procedures in section V.2.a above. If the hard drive cannot be overwritten, the hard drive must be disassembled and mechanically damaged so that it is not usable by a computer.

3. Disposal of Electronic Media Other Than Hard Drives

   a. Transfer of Electronic Media Other Than Hard Drives Within a Department

      i. Before electronic media is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be reformatted if the media type allows it or erased if formatting is not possible.

   b. Disposal of Electronic Media Outside the University

      i. All electronic media other than computer hard drives must be rendered unusable before leaving the University. Use of certified commercial disposal systems such as "Shred-it" is encouraged.

VII. NON-COMPLIANCE AND SANCTIONS

Violation of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school, and may subject the violator to penalties stipulated in applicable state and federal statutes.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer