Revision History

Version	Date
Sanitization and Disposal of Information Resources Policy, 1.0	29 July 2021

SANITIZATION AND DISPOSAL OF INFORMATION RESOURCES POLICY

I. Introduction

A large volume of Organizational Data is stored on Systems (as each such term is defined in the USEIC Data Protection Charter (the "Charter")) throughout USEIC. A substantial amount of such Data consists of Sensitive Data or Confidential Data. Unauthorized disclosure of such Data may expose the Organization to legal liability. Data sanitization is the deliberate and permanent removal of Organizational Data from an Information Resource. This Policy defines the appropriate sanitization and disposal methods to be used.

Capitalized terms used herein without definition are defined in the Charter.

II. Policy

Each System Owner, Data Owner, IT Custodian and User is responsible for determining if Sensitive Data is present on an Information Resource by, for example, periodically scanning the Information Resource using software provided by USEIC, and sanitizing all Information Resources with hard drives and Removable Media under his/her control prior to removal from the Organization in accordance with the following guidelines:

A. Non-Sensitive Data

Organizational Data other than Sensitive Data may be deleted and/or reformatted.

B. Sensitive Data

Sensitive Data must be sanitized or disposed of in a manner that leaves such Data fully unrecoverable. Except as provided below, this can be accomplished by using one of the following methods:

- Data deletion software provided by the Data Protection Officer (DPO);
- DPO-approved destruction hardware to physically render the Sensitive Data storage media inoperable, such as degaussing, shredding, pulverizing, or melting;
- Release of the Information Resource containing storage media to the DPO for destruction and disposal; or
- Release of the Information Resource containing storage media to a DPO-approved vendor.

C. Paper-Based Data

All paper based Sensitive Data or Confidential Data must be destroyed using cross-shredding or through a contract with a DPO-approved vendor.