Information
Inventory Tracking and Discarding of Computing Devices

Effective
July 23 2007

Number
ISO 016 v2 1

Applicability
This policy applies to all persons while conducting performing work teaching research or study activity or otherwise using university resources Scope Applicability also includes all facilities property data and equipment owned leased and or maintained by the University or affiliates

Administrative Authority
Vice President for Risk Audit and Compliance

Responsible Unit
Information Security Compliance Office
502-852-6692
isopol@louisville.edu

History
This policy is subject to change or termination by the University at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.
This policy will be reviewed annually to determine if the policy addresses University risk exposure and is in compliance with the applicable security regulations and University direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed per the Policy Management process.
Approved July 23, 2007 by the Compliance Oversight Council
Shirley C Willihnganz, Executive Vice President and University Provost, Chair of the Compliance Oversight Council
Revision Date(s):

1.0 / July 23, 2007 / Original Publication
1.1 / January 29, 2013 / Content Update
1.2 / September 26, 2013 / Content Review and URL Update
2.0 / March 8, 2016 / Content review/update and update to new template
2.1 / December 6, 2016 / Update Purchasing reference and links to Surplus
2.1 / August 13, 2018 / Grammar and punctuation updates
2.1 / June 23, 2022 / Update references and links
Reviewed Date(s): March 8, 2016, June 14, 2017, August 13, 2018; June 23, 2022

Categories

Statement:

Sensitive information must be permanently deleted from all computing devices and electronic media that is redeployed, transferred, sent to surplus, discarded, removed from service or that changes service and/or facilities.

Related Information:

NIST Media Sanitization Standards
Related inventory procedures: Inventory and Surplus

Reasoning:

Sensitive data must be protected from unauthorized access or disclosure throughout its entire lifecycle from origination to destruction. Electronic media and computing devices, regardless of their value, that contain sensitive information must be properly inventoried, tracked and secured at all times. Sensitive data must be properly eradicated upon destruction or redeployment.

Definitions:

Sensitive information: Information of a confidential or proprietary nature and other information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or University policy. This includes (but is not limited to) full name or first initial and last name and employee ID (in combination), identifiable medical and health records, grades and other enrollment information, credit card, bank account and other personal financial information, social security numbers, confidential or

proprietary research data, dates of birth (when combined with name, address and/or phone numbers), user IDs when combined with a password, etc. See Information Management and Classification Standard.

Computing Devices: Includes but is not limited to workstations, desktop computers, notebook computers, tablet computers, network enabled printers, scanners and multi-function devices, mobile devices, email/messaging devices, cell phones, removable hard drives, flash or "thumb" drives, etc. all hereafter referred to as "computing devices".

Electronic Media: Includes all electronic data storage devices funded as under Computing Devices above or other electronic data storage devices used to store UofL related data. Media includes but is not limited to removable and non-removable storage such as hard drives, CDs, DVDs, magnetic tape, removable disks (floppy, zip, cartridge systems, etc.) and flash memory devices.

ePHI: Electronic Protected Health Information - Health information maintained or transmitted in an electronic format that:

1. Identifies or could be used to identify an individual;
2. Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and
3. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of healthcare to an individual.

Responsibilities:

Policy Authority/Enforcement: The University's Information Security Officer (ISO) is responsible for the development, publication, modification and oversight of these policies and standards. The ISO works in conjunction with University Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

Policy Compliance: Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the University and/or action in accordance with local ordinances, state or federal laws.