pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Policy SEC-015

Name:	Data Sanitization
Effective Date:	September 2017
Category:	Security Domain
Version:	1.2

1. Purpose:

This policy provides direction for the removal of data from information technology (IT) systems, and IT Equipment and identifies specific procedures within the Department of Labor & Industry (L&I) to protect data and alert program areas of financial implications that may impact their budgets.

This policy provides direction for Office of Information Technology (OIT) staff to reduce the risk of data leakage or unauthorized data release. This policy also fulfills the requirements of Internal Revenue Service (IRS) Publication 1075 safeguards and requirements defined by the Social Security Administration (SSA). This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-3, MP-2, 4, 6, & SA-9 Per SP 800-53 R4. In addition, this policy identifies guidelines for the sanitization of data per NIST SP 800-88.

2. Background:

All data on hard drives and associated computing devices is confidential. The cleansing, or sanitization of computer devices and related storage media is a vital step in safeguarding data and ensuring that the inadvertent sharing of sensitive information does not occur.

Data remains present on any type of storage device (whether fixed or removable) even after a disc is "formatted," power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented.

Leaving data on an un-sanitized drive could represent an unauthorized release of confidential information that could result in fines, penalties, or litigation. Additionally, accessing data on an un-sanitized drive could represent a violation of L&I's Software License Agreements that could result in fines and penalties.

3. Scope:

This policy applies to all employees within all bureaus, divisions, boards, commissions, and councils within L&I. This includes any contracted employees in the service of L&I (hereinafter referred to collectively as "L&I Users").

4. Policy:

A. Planning

Paper, hard copy, and electronic records shall be disposed of in a secure manner as specified by the data owner, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and agency records retention plans.

L&I, Office of Information Technology Policy SEC-015

System owners (SO) shall identify and classify the data on their IT systems per APP-001 and SEC-000. The SO shall coordinate and document the assessment of data with the agency records coordinator.

The SO shall determine if failure to sanitize drives and media prior to transfers would represent an unauthorized release of confidential information, breach, or license agreement violation. The SO also shall assess the risks and report them to the agency information security officer (ISO).

The SO shall coordinate with the agency records coordinator and IT staff to ensure records are destroyed following all laws and controls including federal and state laws, and the records retention plan, including rules governing both the sanitization of media, and destruction of printed materials.

The SO shall treat all records containing personally identifiable information (PII), IRS or SSA data as confidential.

Any Commonwealth-related information, software, data, files, or programs discovered on any Commonwealth-provided computing device, is the property of the Commonwealth.

Program area staff shall retain at least one copy of each version of the application software used to create any archived data to ensure recovery.

Program area staff shall ensure that all critical information residing on an L&I User's storage drives has been copied to a durable and secure storage site, prior to the L&I User's last day of work with L&I and prior to replacing an L&I User's work computer or hard drive.

Program area staff shall ensure all printed material is printed, stored and destroyed in accordance with the specifications of the data owner.

B. Redeployed /Disposal of Computing Equipment

OIT shall reload the operating system and necessary programs on every workstation that is redeployed to another user within L&I.

L&I Users shall report to the agency ISO any information, software, data, files, or programs discovered on a commonwealth-provided computing device that they reasonably believe to be from a previous L&I User.

OIT shall report to the SO if sensitive, confidential, or PII is present on IT Equipment or IT systems.

OIT shall sanitize data from all IT Equipment and associated media prior to removal for decommissioning or disposal.

OIT shall sanitize all IT Equipment prior to transferring the equipment to an external entity for off-site maintenance or repairs.

OIT shall sanitize information system media prior to disposal, release out of organizational control, or release for reuse.

OIT shall employ sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

OIT shall track, document, and verify media sanitization and disposal actions.

OIT shall annually test sanitization equipment and procedures to verify correct performance.

OIT shall validate security controls are still functioning properly following maintenance or repair actions.

OIT shall protect IT systems, applications, and data storing media until destroyed or sanitized using approved equipment, techniques, and procedures.

OIT will review all contracts and proposals with providers of external information system services to comply with requirements and employ appropriate security controls in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.

OIT shall monitor security control compliance by external service providers.

OIT shall destroy any data storage device that cannot be cleansed using approved data cleansing software before the data storage device is either transferred to a new user, designated as IT-surplus, or returned to a lessor.

5. Responsibilities:

A. L&I User responsibilities:
- Comply with all L&I policies, management directives, and laws; and
- Report any violations of policies promptly to the ISO at LI, OIT-DLICISO.

B. L&I management responsibilities:
- Comply with all L&I policies and ensure L&I users comply with the policies; and
- Adhere to this policy and any published procedures regarding data cleansing.

A. References:

L&I Policy Definitions Document

APP-001 - Release of Protected Data

Data Sanitization of Workstations Hard Drives & Media

Disposal of L&I-Owned & Leased Workstations

SEC-000 - Security Planning Policy

ITP_SEC015 - Commonwealth of Pennsylvania Data Cleansing Policy

ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data

NIST SP 800-88 Guidelines for Media Sanitization

L&I, Office of Information Technology Policy SEC-015

B. Version Control:

Version	Date	Purpose
1.0	10/2006	Base document
1.1	08/2017	Format and Content Revision
1.2	04/2018	Updates to policy to accommodate SSA audit