

Information Technology Policy

Data Cleansing Policy

Number

ITP-SEC015

Effective Date

May 1, 2013

Category

Security

Supersedes

None

Contact

RA-ITCentral@pa.gov

Scheduled Review

July 2024

1. Purpose

This Information Technology Policy (ITP) establishes policy, responsibilities, and procedures for the sanitization and destruction of Commonwealth electronic media.

2. Scope

This ITP applies to all offices, departments, boards, commissions and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Policy

[Agency personnel](#) shall ensure that Commonwealth [electronic media](#) data is:

- Assessed by agency records manager's office;
- Securely erased; and
- Physically removed from state-owned, leased, and contractor-owned/leased devices containing agency data pursuant to law or court order and in accordance with the policies outlined in this ITP.

Agencies assume all responsibility for ensuring all electronic media has been [degaussed](#), wiped, or destroyed and removed from [electronic devices](#) prior to the decommissioning of assets. The Department of General Services (DGS), Bureau of Supplies & Surplus Operations is not responsible for any information loss or damage that may result from an agency's failure to follow the procedures outlined in this policy.

The DGS Bureau of Supplies & Surplus Operations will not accept any electronic

devices that contain electronic media, and any such devices will be rejected by DGS personnel. Refer to DGS procedures for electronic media handling referenced in section 3.2 below.

For records management guidance, refer to [Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program](#).

3.1 Cleansing of Electronic Media on Commonwealth-owned and Commonwealth-leased Electronic Devices

Prior to the disposal, surplus, or recycling of any Commonwealth-owned and -leased electronic devices, Agencies shall ensure the following steps are followed:

- 1. Degauss, wipe, or destroy electronic media.** All data residing on electronic media shall be cleansed in accordance with the [NIST Guidelines for Media Sanitization \(SP 800-88 Rev. 1\)](#) and securely erased by using one of the following methods:
 - Utilizing a National Security Agency (NSA) or Department of Defense (DoD) rated degausser, or
 - By performing a [DoD 5220.22-M](#) wipe, where data is overwritten using a three-pass approach.

Note: If using the wiping method to securely erase data, the status log shall be checked each time the process is completed to ensure that the entire disk wiping procedure finished successfully without any errors. Disk wiping is a time-consuming and labor-intensive process that demands high levels of quality control review by IT staff.

The agency is fully responsible and liable for taking the necessary measures to ensure that data is securely erased.

- 2. Store in a secure location.** The electronic media shall be stored in a secure location pending delivery or collection. For additional policy guidance on physical security procedures, refer to [ITP-SEC029, Physical Security Policy for IT Resources](#).

3.2 Surplus, Recycle, Package/Palletize

Agencies shall follow the [DGS State Surplus Property Program](#) procedures when recycling or surplusizing Commonwealth IT resources.

3.3 Reassignment of Commonwealth-owned Electronic Devices between Employees of the Agency

Prior to the reassignment of any Commonwealth-owned electronic devices between employees, Agencies shall ensure the following steps are followed:

- 1. Wipe the electronic media.** All data residing on electronic media is wiped by performing a [DoD 5220.22-M](#) wipe. Do not use a degausser for the reassignment of electronic devices.
- 2. Re-image the electronic media.** Once the electronic media has been wiped, use a backup image to reinstall the operating system and software applications.

Note: Special cases may exist that do not warrant a DoD [disk wipe](#) upon reassignment between employees of Commonwealth-owned electronic devices. In such cases, a Commonwealth department manager has the discretion to determine and request that the wipe procedure not be utilized. By allowing special-case discretion to management, the Commonwealth will be able to promote business efficiency and prevent unnecessary work from being done, while at the same time, not compromising its ability to maintain the confidentiality of its sensitive and private data.

3.4 Cleansing of Electronic Media on Electronic Devices owned by Contracted Resources and Used on Behalf of the Commonwealth

Electronic devices that are owned by a contracted resource and are used to perform work for the Commonwealth shall adhere to [ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data](#) to ensure the protection of any Commonwealth data on or transmitted through the device.

At the completion of a contracted resources' engagement, if any electronic devices owned by the contracted resource contain data in one of the classifications described in [ITP-INF015, Policy and Procedures for Identifying, Classifying and Categorizing Commonwealth Electronic Data](#) the electronic media utilized for the engagement shall be securely erased by the disk wiping method described in the following paragraph. This can be done by the contracted resource, a Commonwealth employee, or a verified third party; however, successful completion of this process is the contracted resources' responsibility and shall be verified by a Commonwealth employee.

All data residing on electronic media shall be wiped by performing a [DoD 5220.22-M](#) wipe. Do not use a degausser in this scenario.

If the contracted resource has a "Statement of Destroyed Materials" or similar policy/program, the agency will not be required to pay for the replacement of the destroyed electronic media. This policy recognizes that electronic media contains confidential, sensitive data and cannot be returned. The contracted resource will credit the Commonwealth as if the drive had been returned.

3.5 Failed Electronic Media

All electronic media that fails due to a physical malfunction or other reasons shall be destroyed if the media cannot be properly sanitized through degaussing or wiping. Methods of destruction include Disintegrate, Pulverize, Melt, Incinerate, or Shred which are detailed in [NIST SP 800-88 Rev. 1](#).

3.6 Chain of Custody

Agencies must submit [OPD-SEC015A, Commonwealth of Pennsylvania Chain of Custody Tracking Form](#) to accompany any equipment designated for DGS Surplus. This form must be completed and signed by the Agency personnel responsible for sanitizing the equipment. DGS will not accept equipment that is not accompanied by a signed Chain of Custody Tracking Form (OPD-SEC015A).

For all properly sanitized electronic media DGS accepts as surplus and ultimately disposes of, a date/time-stamped [Chain of Custody Tracking Form \(OPD-SEC015A\)](#)

will be returned to the agency signatory.

4. Responsibilities

4.1 Agencies shall:

Comply with the requirements as outlined in this ITP to ensure all electronic media has been properly cleansed prior to surplus, recycling, or disposal.

4.2 Agency Information Security Officer shall:

Determine which electronic media requires data cleansing.

4.3 Agency Records Management Office Representation shall:

Provide assistance to Agency IT personnel as needed in determining the content of electronic media prior to data cleansing.

4.4 Department of General Services shall:

Determine final disposition for electronic devices/media.

4.5 Third-party vendors, licensors, contractors, or suppliers shall:

- Implement process for the cleansing of data from electronic devices/media when the data retention requirements have expired, the data is no longer needed, or the data is scheduled for disposal as determined by the Commonwealth.
- Decommissioned electronic media must be degaussed, wiped, or destroyed in accordance with this ITP and by following best practices outlined in [NIST Special Publication 800-88r1](#).

5. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: <http://www.oa.pa.gov/Policies/Pages/Glossary.aspx>
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: <http://www.oa.pa.gov/Policies/Pages/default.aspx>
- [Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy](#)
- [Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program](#)
- [ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data](#)
- [ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data](#)
- [ITP-SEC029, Physical Security Policy for IT Resources](#)
- [OPD-SEC000B, Security Requirements for Third Party Vendors](#)
- [OPD-SEC015A, Chain of Custody Tracking Form](#)
- DGS Bureau of Supplies and Surplus Operations – [Process Guidelines for Surplus of IT Equipment](#)

- [DGS State Surplus Property Program](#)
- DoD 5220.22-M – [National Industrial Security Program Operating Manual](#)
- NIST SP 800-88 Revision 1 – [Guidelines for Media Sanitization](#)

6. Authority

[Executive Order 2016-06, Enterprise Information Technology Governance](#)

7. Publication Version Control

It is the [Authorized User](#)'s responsibility to ensure they have the latest version of this publication, which appears on <https://itcentral.pa.gov> for Commonwealth personnel and on the Office of Administration public portal: <http://www.oa.pa.gov/Policies/Pages/default.aspx>. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

8. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to [ITP-BUS004 IT Policy Waiver Review Process](#) for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original		Base Document	N/A
Revision	05/01/2013	Includes all mobile devices, rescinds ITP-SYM009.	N/A
Revision	03/26/2014	Updated Section II. <u>Proper Return of State-Leased Computers</u> with updated State Contract numbers and eMarketplace links.	N/A
Revision	08/20/2015	Added Chain of Custody form (OPD-SEC015A) Removed state contract references Added language requiring agencies to remove all electronic media from electronic devices before DGS acceptance of delivery Added additional definitions Added records management language and references Added methods of destruction in Failed Electronic Media (Section V) Added Responsibilities table (Section 5) Added reference to DGS Guidelines for Surplus document	N/A
Revision	09/09/2016	Corrected ITP number for "Physical Security..." from SEC019 to SEC029 in Section 4I Revised Section 6 for clarity Added Exemption Section 7 Updated Enterprise Information Technology Governance EO reference number in Section 8	N/A
Revision	10/04/2018	Removed Bureau of Supplies & Surplus Operations from specific responsibilities Moved Definitions to Policy Glossary	N/A

Version	Date	Purpose of Revision	Redline Link
		Updated language throughout adding Delivery Centers and removing Agencies where appropriate to reflect Shared Services organization Minor revisions to OPD-SEC015A	
Revision	08/09/2021	<ul style="list-style-type: none"> Added third party vendors to Scope and Responsibilities Sections Removed references to Delivery Centers, Updated links and policy references. Updated Exemption Section 	N/A
Revision	06/21/22	<ul style="list-style-type: none"> ITP Refresh Responsibilities chart was incorporated into Responsibilities section. 	N/A
Revision	07/26/2023	<p>Annual review.</p> <p>General updates throughout to clarify and add consistency to policy language without changing overall policy language intent.</p> <p>Agency requirements under Responsibilities section updated.</p> <p>References section updated.</p> <p>Added references to ITP-INF015 when discussing data classification</p> <p>Scope updated consistent with connection to commonwealth network.</p>	Revised IT Policy Redline <07/26/2023>