Data Classification Policy

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
March 31, 2026

Supersedes:
ITP-SEC015, ITP-SEC025, ITP-INF015, ITP-SEC019

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

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

3. Scope

This policy 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 policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

This Information Technology Policy (ITP) provides guidelines for the exercise of agency discretion in creating policies and procedures on the proper electronic use and disclosure of Personally Identifiable Information (PII).

The Office of Administration/Office for Information Technology (OA/IT) is committed to protecting the privacy of PII of its employees, contractors, constituents, and other individuals associated with the Commonwealth. All agencies shall take appropriate measures, implement necessary technology, and establish operating procedures to ensure data privacy is maintained. All applications collecting PII must comply with applicable laws and be vetted through the CA2 process (detailed in the *eCommerce Policy.*

4.1 Classification

Agencies shall identify the Classification of electronic records and protect information from improper disclosure based on the Classification of the records.

4.1.1 "C" CLASSIFICATION RECORDS or CLOSED RECORDS

The use of a "C" designation indicates that all or part of the record requires special treatment and/or heightened protections, including, but not limited to, as appropriate, non-disclosure to the public, non-disclosure to any person without a need to know, non-disclosure outside of certain workgroups, non-disclosure without certain prerequisites, etc.

Although a "C" designation usually equates to a "non-public record" designation under the Right-to-Know Law (65 P.S. Section 67.101, et seq.), the two designations are not the same. A record's treatment under the Right-to-Know Law must be determined in consultation with an agency's legal counsel and Right-to-Know Law staff at the time of the Right-to-Know Law request.

Failure to classify records as "C" does not give rise to any presumption, implication, or indication that records are open or accessible to the public.

Only the originating agency may remove the "C" designation. A "C" designation, and the more granular "class" within that designation, is a determination made by an agency head or designee. If another data designation or class is deemed necessary, justification shall be provided to OA for why a data element or group of data elements does not fit into the classes below.

Closed or "C" records shall be placed into one of the following Classifications:

4.1.2 Sensitive Security Information

This type of information may fall under another class, but it is placed in this one because of the significant consequences of potential disclosure, and the high degree of protection it requires. It is information maintained by an agency in connection with homeland security, national defense, military, law enforcement or other public safety activity, the disclosure of which would be reasonably likely to jeopardize public safety or preparedness. Homeland Security information includes, but is not limited to:

- Records designed to prevent, detect, respond to, and recover from acts of terrorism, major disasters and other emergencies, whether natural or manmade.
- Emergency preparedness and response, including volunteer medical, police, emergency management and fire personnel; intelligence activities; critical infrastructure protection.
- Border security.
- Ground, aviation and maritime transportation security.
- Biodefense.
- Detection of nuclear and radiological materials.
- Research on next-generation security technologies.
- Other information, which if disclosed creates a reasonable likelihood of endangering the life or safety of a natural person or threatening public safety or the physical security of a building, resource, infrastructure facility or information storage system, including:

- Documents or data relating to computer hardware, source files, software and system networks that could jeopardize computer security by exposing a vulnerability in preventing, protecting against, mitigating or responding to a terrorist act.
- Lists of critical infrastructure, key resources and significant special events, which are deemed critical due to their nature, and which result from risk analysis, threat assessments, consequences assessments, vulnerability assessments, anti-terrorism protective measures and plans, counter-terrorism measures and plans, security and response needs assessments.
- Building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration, or security of critical systems, including public utility critical systems, such as information technology, communication, electrical, structural, fire suppression, ventilation, water, wastewater, sewage, and gas systems.

4.1.3 Protected Information

This is information that is subject to some degree of protection under any Pennsylvania or federal statute, law, order, or regulation. The degree of protection necessary will vary based on the law or order in question, and the potential consequences of disclosure. This information includes, but is not limited to:

- Data elements as defined in the *Breach of Personal Information Notification Act, Act of November 3, 2022, P.L. 2139, No. 151, 73 P.S. §§ 2301-2330.*
- Information received from a federal or Commonwealth entity bound by specific regulations, including, but not limited to the following sources:
  - Social Security Administration (SSA).
  - Internal Revenue Service (IRS).
  - Centers for Medicare and Medicaid Services (CMS).
  - Criminal Justice Agencies in accordance with the Criminal History Record Information Act (CHRIA).
  - Family Education Rights and Privacy Act (FERPA).
  - Payment Card Industry (PCI) data security standards.
  - Health Insurance Portability and Accountability Act (HIPAA) or other data privacy or security law in the health care industry (including internal entities).
- Third Party Data: Information associated with and specific to the Commonwealth's regulated entities, vendors, suppliers, business partners, contractors, and other third-party entities, including the trade secrets of third parties. The degree of protection necessary will vary based on the law or order in question, and the potential consequences of disclosure.
- Geographic Data: Information associated with addresses, locational information, or elements from a Geographic Information System (GIS).
- Contract Data: Information associated with contract, award, and bidding activities related to procurement of supplies or services, at appropriate stages of procurement.

4.1.4 Privileged Information

This is information that is protected by a recognized privilege or doctrine, such as attorney-client privilege, the attorney work product doctrine, executive privilege, or deliberative process privilege.

4.1.5 Prerequisite-Required Information

This includes data that is not exempt or precluded from public disclosure under any Pennsylvania law or order (including the Right-to-Know Law), but that requires certain protections to ensure that the prerequisites to disclosure are met. The degree of protection necessary will vary based on the record in question, and the potential consequences of disclosure. For example, this includes records that may be disclosed only after a form is signed, etc.

4.2 Sensitivity Levels

The use of Sensitivity Levels provides further designation to indicate that all or part of the record requires special treatment and/or heightened protections, including, but not limited to, as appropriate, non-disclosure to the public, non-disclosure to any person without a need to know, non-disclosure outside of certain workgroups, non-disclosure without certain prerequisites, etc.

- Confidential - Data elements that are privileged under the Right-to-Know Act. Privileged or Closed Record; Sensitive Security Information.
- Restricted - Data elements that are not privileged under the Right-to-Know Act but are highly sensitive and should not be released as they may cause harm to an individual. Closed Record; Protected Information.
- Internal - Data elements that are not privileged under the Right-to-Know Act, but release would not require notification or cause individuals drastic harm. Closed Record; Privileged or Closed Record; Prerequisite-Required Information.
- Public - Data elements that are made readily available to the public through websites or other modes of publication.

4.3 Data Categorization and Classification

Agencies shall categorize and classify all data as follows:

- Data Categorization shall adhere to the NIST SP 800-60 Rev 1 Guide for Mapping Types of Information and Information Systems to Security Categories Volumes 1 and 2.
- Data classified as Public Records shall adhere to *Management Directive 205.36, Right-to-Know Law Compliance* and *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program.*
- "C" designated data shall be placed in one of the following classes: Sensitive Security, Protected, Privileged, Prerequisite-Required.
- No "C" designated electronic records can leave an approved storage solution without prior electronic approval from the Agency ISO or equivalent. Additionally, all

requests for information relating to “C” designated electronic records must be made in writing to the Agency ISO.

- Encryption standards outlined in the Encryption Policy shall be followed for any actions that specify encrypting data under the “C” Classification.
- Encryption protection mechanisms detailed below in the Data Classification Tables shall be followed.
- Systems that store, process, transmit, or otherwise handle the following categories of data: Sensitive Security, Protected, or Privileged must be protected with a Web Application Firewall (WAF) or Database Firewall (DBFW) as follows:

    - WAFs must be utilized to protect Internet accessible web sites and services.
    - DBFW must be utilized to protect Database related systems.
    - Agencies designing modernized and new database-related systems shall include DBFW configurations to meet DBFW data owner requirements and future requirements to ensure the highest level of required security controls.
    - Agencies shall evaluate the impact of third-party WAF and DBFW agents on their computing resources prior to the deployment of the WAF and DBFW agents.

- Systems that store, process, transmit, or otherwise handle prerequisite- Required or Public Records may be protected with a WAF or DBFW as follows:

    - WAFs may be utilized to protect Internet accessible web sites and services.
    - DBFW may be utilized to protect database related systems.
    - Agencies designing modernized and new database-related systems shall include DBFW configurations to meet DBFW data owner requirements and future requirements to ensure the highest level of required security controls.
    - Agencies shall evaluate the impact of third-party WAF and DBFW agents on their computing resources prior to the deployment of the WAF and DBFW agents.

Agencies shall apply appropriate protections for data as outlined herein.

4.4 Data Classification Tables

The following data Classification tables pertain to electronic records and details the requirements for the various levels of protection determined by the various forms of data and transmission methods pertaining to:

- Sensitive Security Information
- Protected Information
- Privileged Information
- Prerequisite-Required Information
- Public Records

SENSITIVE SECURITY INFORMATION

Action	**Requirement**
Storage on Fixed Media	Encrypted

Action	Requirement
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.
Faxing	Transmitted over an encrypted link to a password-protected mailbox or, if sent to a public or multi-user fax machine, received (printed) using Attended Receipt
Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to the *Encryption Policy*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per this policy, subject to any applicable records retention requirements.
Release to Third Parties	Owner approval and Non-Disclosure Agreement prior to release. Must be provided to third-party via an approved action that provides encryption.
Electronic Media Labeling Required	External and Internal Labels
Internal and External email	Addressed to Specific Person but Label only on Inside. Email must be encrypted.
Packaging	Security Envelope
Granting Access Rights	Data Owner Only

Action	Requirement
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall or Database Firewall	Required (for Web Applications/Services or Database systems)

PROTECTED INFORMATION

Action	Requirement
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.
Faxing	Transmitted over an encrypted link to a password- protected mailbox or, if sent to a public or multi- user fax machine, received (printed) using Attended Receipt
Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to the *Encryption Policy*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per this policy, subject to any applicable records retention- requirements
Release to Third Parties	Owner approval and Non-Disclosure Agreement prior to release. Must be provided to third-party via an approved action that provides encryption.
Electronic Media Labeling Required	External and Internal Labels
Internal and External email	Addressed to Specific Person but Label only on Inside. Email must be encrypted.
Granting Access Rights	Data Owner Only
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall or Database Firewall	Required (for Web Applications/Services or Database systems)

PRIVILEGED INFORMATION

Action	Requirement
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.
Faxing	Transmitted over an encrypted link to a password-protected mailbox or, if sent to a public or multi-user fax machine, received (printed) using Attended Receipt
Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to the *Encryption Policy*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per this policy, subject to any applicable records retention requirements
Release to Third Parties	Owner approval and Non-Disclosure Agreement prior to release. Must be provided to third-party via an approved action that provides encryption.
Electronic Media Labeling Required	External and Internal Labels
Internal and External email	Addressed to Specific Person but Label only on Inside. Email must be encrypted.
Granting Access Rights	Data Owner Only
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall or Database Firewall	Required (for Web Applications/Services or Database systems)

PREREQUISITE-REQUIRED INFORMATION

Action	Requirement
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.

Action	Requirement
Faxing	Transmitted over an encrypted link to a password-protected mailbox or, if sent to a public or multi-user fax machine, received (printed) using Attended Receipt
Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to the *Encryption Policy*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per requirements contained in this policy, subject to any applicable records retention requirements
Release to Third Parties	Non-Disclosure Agreement prior to release. Must be provided to third-party via an approved action that provides encryption.
Electronic Media Labeling Required	No Label Required
Internal and External email	Addressed to Specific Person but Label only on Inside. Email must be encrypted.
Granting Access Rights	Data Owner, Agency Legal
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall or Database Firewall	Recommended (for Web Applications/Services or Database systems)

PUBLIC RECORDS

Action	Requirement
Storage on Fixed Media	No restrictions
Storage on Exchangeable Media	No restrictions
Creation of Printed Media	No restrictions
Faxing	No restrictions
Sending by Public Network	No restrictions
Sending Over Agency Network	No restrictions
Disposal	No restrictions
Release to Third Parties	No restrictions
Electronic Media Labeling Required	No restrictions
Internal and External email	No restrictions
Granting Access Rights	Preapproval by Agency Legal and Business Owner required for unrestricted access
Tracking distribution and lifecycle of electronic data	Logging of initial recipients
Web Application Firewall or Database Firewall	Recommended

4.5 Data Inventory

Office of Administration, Office for Information Technology (OA/IT) shall utilize catalog technology to automate inventory collection activities on behalf of agencies for inclusion in an enterprise-level view of data structures and elements managed by OA/IT in conjunction with Agency Data Stewards.

The inventory shall be housed in a central repository, with data assets/sources mapped to adopted enterprise data standards. This asset/source mapping shall support gap analysis and identification of areas requiring new enterprise data standards. This repository will be for internal use, shared with Agency Data Steward(s) and shall providean appropriate inventory to any Commonwealth data-holding contractor for all the servers and/or application solutions in the contractor environment or under contractor control.

In situations where OA/IT has not completed inventory collection of an agency data asset/source, the agency shall produce a data inventory for inclusion in the enterprise-level inventory of data structures and elements managed by OA/IT. Refer to the *Data Inventory Template*.

The inventory provides a list of Commonwealth applications and identifies data classes and sensitivity levels for the data present on each server (and desktops, if applicable) and/or in any application solution. An inventory allows the Commonwealth and/or the contractor to identify protection mechanisms for each server and/or application solution.

Completing the inventory will aid the Commonwealth and contractors in the following:

- Identifying servers and/or application solutions with data that have stringent regulatory requirements (such as commingling requirements of Federal Tax Information (FTI)).
- Increasing the speed of incident response procedures for potential breach notifications in accordance with the law.
- Providing cost saving through selective, strict protection of the highest sensitivity levels of data and not applying strict protections on lesser sensitivity levels.
- Aiding in the identification of servers requiring special privileged user access.
- Identifying the use of production data in non-production environments and allowing for remediation of those scenarios.

Agencies using the Data Inventory Template shall document an inventory of all data assets/sources as well as identify the categories and classes of data and their respective sensitivity levels for each data asset/source, at least annually.

Agencies using the OA/IT data catalog technology shall allow OA/IT to securely connect the data catalog to data assets/sources to document data inventory of the data assets/sources as well as identify the categories and classes of data and their respective sensitivity levels for each data asset/source. Connection of the data catalog technology to an agency data asset/source will be non-persistent and only used during the time an inventory scan is actually executed by the data catalog technology.

Agencies and/or OA/IT shall perform, at a minimum, an annual update of the data inventory using either the OPD-INF015A template or the OA/IT data catalog technology. Agencies shall also perform updates of data inventory at the following security events including, but not limited to:

- Upon the commencement of the use/storage of the data.
- Upon the initiation of the agency migration into contractor facilities or into facilities under contractor control.
- New data elements introduced to the server or application solution.
- Repurposing of the server or application solution.
- Major upgrades to the IT system, application, or databases.
- Changes in regulations or policies regarding data elements present.
- Any significant change that affects or introduces "C" classified data.

4.6 Proper Use and Disclosure of Personally Identifiable Information (PII)

This Information Technology Policy (ITP) provides guidelines for the exercise of agency discretion in creating policies and procedures on the proper electronic use and disclosure of Personally Identifiable Information (PII).

It is important for an agency to recognize that non-PII can become PII whenever additional information is made available that, when combined with other available information, could be used to identify an individual.

Examples of PII include, but are not limited to, any combination of the following personally identifiable attributes:

- Name
- Date and place of birth
- Mother's maiden name
- Biometric records
- Social Security Number
- Driver's license number or a state identification card number, in lieu of a driver's license
- Passport Number
- Financial account number, credit or debit card number, in combination with any required security code, access code or password
- Medical information
- Health insurance information, policy or subscriber identification number in combination with access code or other medical information
- Username or email address, in combination with a password or security question and answer

Agencies may have additional attributes beyond those stated above they are required to protect under certain policies, laws, or regulations (i.e., Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), or Internal Revenue Service (IRS)) that are specific to their agency or type of data handled.

The Office of Administration/Office for Information Technology (OA/IT) is committed to protecting the privacy of PII of its employees, contractors, constituents, and other individuals associated with the Commonwealth. All agencies shall take appropriate measures, implement necessary technology, and establish operating procedures to ensure data privacy is maintained. All applications collecting PII must comply with applicable laws and be vetted through the CA2 process (detailed in the *eCommerce Policy*).

4.6.1 Identifying PII

Agencies are responsible for identifying and classifying all PII generated, collected, stored, used, and disclosed by the agency or by a third-party on the agency's behalf. This data includes Sensitive Security Information, Protected Information, Privileged Information and Prerequisite-required information. Refer to the *Data Classification Policy* for data classification guidance.

4.6.2 Collecting PII

Agencies shall limit the generation, collection, storage, use, and disclosure of PII to that which is necessary for business purposes only and shall further limit generation, collection, storage, use, and disclosure of PII to the ***minimum*** extent necessary for the accomplishment of those business purposes.

Systems which are vendor or agency hosted shall use PII as data elements only and not as keys to databases. PII may be used for identification purposes or as identifiers only to address a business necessity, and only if allowed by applicable law, regulations or mandates.

4.6.3 Displaying PII

Systems which are vendor or agency hosted shall not display PII visually, whether on computer monitors, or on printed forms, or other system output, unless required by any law or other requirement applicable to an agency, or business necessity.

4.6.4 PII in Test Environments

PII data shall not be used in staging, development, or test environments (non-production environments). Simulated PII data shall be utilized in these environments.

4.6.5 Unique Identifiers

Systems developed by an agency, third-party, contracted provider, or business partner that require a unique identifier shall not use PII as that identifier. All systems, which must assign an identifying number for an individual, must assign a unique identification number that is not the same as, or cannot be traced back to users PII. Security must be applied, and care must be taken to ensure that access to the electronic system and use of these unique identification numbers are restricted in accordance with any law or other requirement applicable to an agency.

4.6.6 Transferring PII

PII moved from one computer to another shall be transferred using encryption

controls defined in the *Data Classification Policy* and *Encryption Policy* to protect data integrity and confidentiality. Agency legal review may be required, and is recommended, to ensure appropriate limits and processes are applied to any PII data transfer between Commonwealth agencies, business partners, or external entities.

4.6.7 Maintaining PII

All agencies maintaining files utilizing PII for any purpose shall ensure that access or use of such information is properly controlled, encrypted, and restricted to prevent unauthorized use or disclosure and that the retention period is minimized based upon business requirements.

4.6.8 Legacy Systems

Owners of legacy information systems that use PII as keys or indexes in their databases and which are not specifically required to do so by any law, regulation, reporting requirement or other mandate shall have an action plan and timelinefor remediation.

4.6.9 Disclosure of PII

Security Incidents involving PII must be reported via the requirements outlined in *IT Security Incident Reporting Policy* regardless of other law or requirements that may be applicable to security incidents or Data Breaches. Security incidents, for reporting under *IT Security Incident Reporting Policy*, include loss or compromise of data in electronic or paper form. Good faith acquisition of personal information by an authorized user for the purposes of Commonwealth business is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of Commonwealth business and is not subject to further unauthorized disclosure. Agencies or business partners shall follow all laws applicable to the security incident and agency requirements.

4.7 Data Cleansing

Agency personnel shall ensure that Commonwealth electronic media data is:

- Assessed by agency records manager's office.
- Securely erased.
- 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 policy.

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 3.6.2 below.

For records management guidance, refer to the *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*.

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

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

- **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.

- **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 the *Physical Security Policy*.

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.

4.7.2 Surplus, Recycle, Package/Palletize

Agencies shall follow the DGS State Surplus Property Program procedures when recycling or surplusing Commonwealth IT resources.

4.7.3 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:

- 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.
- 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.

4.7.4 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 this policy 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 herein 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.

4.7.5 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*.

4.7.6 Chain of Custody

Agencies must submit *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.

For all properly sanitized electronic media that DGS accepts as surplus and ultimately disposes of, a date/time-stamped *Chain of Custody Tracking Form* will be returned to the agency signatory.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the enterprise IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document