COMMONWEALTH OF VIRGINIA

Information Technology Resource Management Standard

Removal of Commonwealth Data from Electronic Media Standard

Virginia Information Technologies Agency

ITRM Publication Version Control

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to VITA's Enterprise Architecture (EA) Division. EA will issue a Change Notice Alert and post on the VITA Website, provide an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties EA considers interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	N/A	Base Document
Revision 2.1.0	10/28/2003	SEC2003-02-1 Rev 0 (10/28/2003)
Revision 2.1.1	03/08/2004	Supersedes SEC2003-02-1 Rev 0
Revision 3	3/15/2008	Supersedes SEC2003-02-1 Rev 1. This revision reflects legislative changes that expanded the CIO's information security responsibilities to include Judicial, Legislative and Independent Agencies branches of government, and Institutions of Higher Education. In addition, appendix B (Non-Disclosure Agreement) and appendix C (Data Removal Quality Assurance Form) along with several minor changes were made to reflect current industry practices and to amplify requirement statements. Also this change reflects the new numbering structure for all PSGs. Changes to this standard are in "BLUE" text with a "legal black line" in the left margin next to the text location.
Revision 4	12/21/2015	Superseded SEC 514-03 Rev 0. This revision adds requirements for disposing of solid state media devices, Flash-memory devices, and multi-function devices. This revision also addresses future technologies and the need for an appointed individual to be responsible for the electronic data removal process. Changes to this standard are noted by a "legal black line" in the left margin next to the text location. Changes are also marked with italics as described below.
Revision 5	*4/30/2019*	*Removed obsolete references in the preface.* *Removed older technology references in the following sections: Background; B. Quality Assurance Testing of Data Removal; C.1.b. Steps; B. Non-Volatile Memory Devices Data Removal Method; E. Mobile Devices; Appendix B: Certification Tags* *Added additional and new information to the following sections: A.1. Acceptable Methods; A.2.Overwriting; A.5. Encryption; C.1. Acceptable Method; C.3. Encryption; E.2 Acceptable Methods for Open Handset Alliance (OHA) Android Device; Appendix B: Certification Tags*
Revision 5.01	*5/20/2021*	*This was an administrative change to update the format of the document and clarify the current standards. The following sections were updated: Approach; C. Certification and Auditing; Appendix A Methods for Removing Commonwealth Data: A.2, C, C.1, E., F., H.*
Revision 5.02	*4/28/2023*	*Administrative rewrite for clarification*

Identifying Changes in This Document

- See the latest entry in the table above
- Vertical lines in the left margin indicate that the paragraph has changes or additions.
- Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

EXA-R-01 **Example with No Change –** The text is the same. The text is the same. The text is the same.

EXA-R-02 **Example with Revision –** The text is the same. *A wording change, update or clarification is made in this text.*

EXA-R-03 ***Example of New Text –*** *This language is new.*

~~**EXA-R-03 Technology Standard Example of Deleted Standard** – This standard was rescinded on mm/dd/yyyy.~~

Review Process

The Director of CSRM Governance and the IS Council provided the initial review of this publication.

Online Review

All Commonwealth agencies, stakeholders, and the public were encouraged to provide their comments through the Online Review and Comment Application (ORCA). All comments were carefully evaluated and individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation
COV ITRM Standard SEC514-05.01
Removal of Commonwealth Data from Electronic Media Standard

Effective Date
May 21, 2021

Compliance Date
May 21, 2021

Supersedes
COV ITRM Standard SEC514-05.1

Scheduled Review
One (1) year from effective date

Authority
Code of Virginia, §2.2-2009
(Additional Powers of the CIO relating to security)
"The CIO shall provide technical guidance to the Department of General Services in the development of policies, standards, and guidelines for the recycling and disposal of computers and other technology assets. Such policies, standards, and guidelines shall include the expunging, in a manner as determined by the CIO, of all confidential data and personal identifying information of citizens of the Commonwealth prior to such sale, disposal, or other transfer of computers or other technology assets".

Scope
In general, this *Standard* is applicable to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education (collectively referred to as "Agency" or "Organization"). This *Standard* is offered only as guidance to local government entities.

Purpose
To define the minimum requirements for each Agency's information security management program

General Responsibilities

Chief Information Officer of the Commonwealth (CIO) Develops and approves statewide technical and data policies, standards and guidelines for information technology and related systems Directs the formulation and promulgation of policies, guidelines, standards, and specifications for the purchase, formulation, and maintenance of information technology for state agencies.

Chief Information Security Officer
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's information technology systems and data.

Virginia Information Technologies Agency (VITA)
At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts, reviewing procurement requests, agency IT projects, budget requests and strategic plans, and when developing and managing IT related services.

Executive Branch Agencies
Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems. Comply with the requirements established by COV policies and standards. Apply for exceptions to requirements when necessary.

Judicial and Legislative Branches
In accordance with the Code of Virginia §2.2-2009: the: *"CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs."*

International Standards International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 27000 series.

Definitions
Definitions are found in the single comprehensive glossary that supports Commonwealth Information Technology Resource Management (ITRM) documents (COV ITRM Glossary).

Related ITRM Policy
Current version of the COV ITRM Policy: SEC519 IT Information Security Policy

Table of Contents

Background 1
Approach 1
Statement of ITRM Requirements for the Removal of Commonwealth Data from Electronic Media 1
A. General Data Removal Steps 1
A.1 General Steps 1
B. Quality Assurance Testing of Data Removal 2
C. Certification and Auditing 2
C.1 Steps 2
E. Data Recovery 3
Resources for the Removal of Commonwealth Data from Electronic Media 4
Appendix A – Methods For Removal of Commonwealth Data 5
a. Magnetic Media Hard Drive Data Removal Methods 5
a.1 Acceptable Methods 5
a.2 Overwriting 5
a.3 Degaussing 6
a.4 Physical Destruction 6
a.5 Encryption 7
b. Non-Volatile Memory Devices Data Removal Method 7
c. Solid State Memory Devices 7
c.1 Acceptable Methods 8
c.2 Physical Destruction 8
c.3 Encryption 9
d. Multi-Function Devices 9
e. Mobile Devices 9
e.1 Acceptable Methods for Apple iOS 10
e.2 Acceptable Methods for Open Handset Alliance (OHA) Android Devices: 10
e.3 Acceptable Method for Other Devices (not iOS or Android): 11
f. Embedded Device Data Removal Methods 12
g. Other Electronic Media Data Removal Methods 12
h. Cloud Media Destruction Methods 12
Appendix B: Certification Tags 13
Appendix C: Non-Disclosure Agreement 15
Appendix D: Data Removal Quality Assurance Form 18
Appendix E: Disposal Process Flow Chart 19

Background

The surplus, transfer (including reassignment within the agency), trade-in, disposal, or replacement of electronic media can create information security risks for the agency. This standard applies to all electronic media that has memory such as the hard drives of personal computers, servers, mainframes, mobile devices, routers, firewalls, switches, tapes, diskettes, CDs, DVDs, mobile devices, printers, Multi-Function Devices (MFD), and Universal Serial Bus (USB) data storage devices.

The risks are related to potential violation of software license agreements, unauthorized disclosure of information such as personally identifiable information, trade secrets, copyrights, and other intellectual property that might be stored on the electronic media. All electronic media containing Commonwealth data, whether stored on Commonwealth assets or that of a service provider, shall have all of that Commonwealth data securely removed from the electronic media as specified by this standard before the electronic media is surplused, transferred, traded-in, otherwise disposed of, or replaced.

Approach

This Standard was developed in coordination with the Department of General Services to promote the appropriate recycling and disposal of commonwealth computers and other IT assets. Failure to effectively remove the Commonwealth data could result in a violation of laws and regulations including but not limited to the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Family Educational Rights and Privacy Act (FERPA), IRS 1075, etc.

This standard also applies to all electronic media owned or leased by the agency or utilized by a service provider. All electronic storage media shall have all Commonwealth data properly removed prior to surplus, transfer, trade-in, disposal, or replacement. Data removal procedures shall be properly documented in accordance with the processes outlined below in Appendix A and in accordance with the software manufacturers' guidelines to prevent unauthorized release of information that may be stored on electronic media. If an electronic storage technology is not specifically addressed in this standard, the agency is required to contact the Chief Information Security Officer for the Commonwealth of Virginia to determine the appropriate procedure for the removal of data from the storage device as well as explicit authorization to proceed.

Statement of ITRM Requirements for the Removal of Commonwealth Data from Electronic Media

A. General Data Removal Steps

The following steps shall be followed by all agencies and their service providers as well as their remote offices when electronic media is surplused, transferred, traded-in, disposed of, or replaced. The following standards also apply to contractor-supplied electronic media. Please see Appendix A for specific removal methodologies.

A.1 General Steps

a) Before electronic media is surplused, transferred (includes reassignment within the agency), traded-in, disposed of, or replaced, all data must be completely erased or otherwise made unreadable in accordance with this standard; however, only after the data has been reviewed and processed for retention in accordance with the agency's records retention policy.

b) All program and data files on any electronic media must be completely erased or otherwise made unreadable in accordance with this standard unless there is specific intent to transfer the particular software or data to the purchaser/recipient.

c) Electronic media shall be securely erased at the earliest time after being taken out of use but not later than 60 days.

d) Whenever licensed software is resident on any electronic media being surplused, transferred, traded-in, disposed of, or replaced, the terms of the license agreement shall be followed.

e) The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal.

f) After the removal of Commonwealth data from the electronic media is complete, the process shall be certified, as specified below, and a record maintained as specified by the agency's records retention schedule.

g) The certification process must be completed by an agency authorized official. As such, the agency head or designee must appoint an individual to be responsible for the electronic data removal process.

B. Quality Assurance Testing of Data Removal

The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal. The quality assurance tester shall test for effective data removal for electronic media once the data has been removed or otherwise made unreadable.

If more than one device has had the data removed, a sample of each device type can be tested as opposed to testing every device. Individual samples should be taken for each type of electronic media (i.e., hard drives of personal computers, mobile devices, routers, firewalls, switches, tapes, diskettes, CDs, DVDs, printers and Universal Serial Bus (USB) data storage devices, *network appliances, embedded devices and portable flash storage*). The sample size for each device type should be commensurate with the sensitivity and risk of the type of data stored but must be at least 10% of the total number of devices for each type of electronic media.

The testing must be documented including date, tester(s), total number of devices in the lot, number tested, method of testing and the result (see: Appendix D). Testing must be performed within one week of the data removal. Test methods may include physical observation if the data removal method was physical destruction or attempting to boot up and read data automated or manual verification if the method was overwriting. If testing of a sample reveals a failure in data removal the agency's ISO must be notified and all devices in that lot must be tested.

C. Certification and Auditing

The data remover must document and certify that the data has been effectively removed.

C.1 Steps

a) Prior to the physical disposition of the electronic media (surplus, transfer to include reassignment within the agency, trade-in, disposal, or replacement), the following information regarding the data removal process shall be documented:

1. The type of equipment/media from which Commonwealth data is being removed.

2. The date of the data removal.

3. The method(s) used to expunge the data from the storage media.

4. The name of the person removing the Commonwealth data.

5. The name and documented approval of the responsible party, i.e. person's supervisor, *AITR, etc*. .

b) A Data Removal Quality Assurance Form and a Certification Tag shall be completed and approved by the person responsible for the removal of Commonwealth data. The completed documentation shall be maintained in a secure location and available for audit. The completed Certification Tag shall be affixed to the electronic media storing the data. For devices such as those with hard drive(s), a certification tag shall be affixed to each device. For mobile media such as CDs, tapes, etc., one certification may be completed for each physically aggregated lot by affixing the certification tag to the box or shrink-wrapped pallet. Lots must be aggregated when there is more than one person per function per lot (i.e., more than one data remover, or more than one quality assurance tester, etc.). See examples in Appendix D for the Data Removal Quality Assurance Form and Appendix B for the Certification Tag.

D. Maintenance and Warranty

It is necessary to protect data on data storage devices that malfunction and require maintenance or replacement under warranty. Each agency or its service provider shall make considerations in new or renewed contracts that address the protection of COV data on data storage devices for warranty or maintenance purposes. Following are standards when maintenance or warranty is necessary:

a) If the data storage device_malfunctions and data can be removed in accordance with the requirements in this standard, the device may be returned to the supplier for replacement under warranty or maintenance.

b) Data storage devices that are inoperable and do not allow data to be removed in accordance with the requirements in this standard, shall be physically destroyed using a method outlined in Appendix A, A.1 Acceptable Methods, Physical Destruction.

E. Data Recovery

In the event data stored on a damaged, failed, corrupted or inaccessible primary storage media cannot be accessed normally and must be salvaged, data recovery methods must be employed. If recovery of data contained on an electronic storage media is required, the agency must provide adequate controls commensurate with the sensitivity of the data contained on the storage media as follows:

a) If a third party is used to recover the data, the agency must ensure that the third party adheres to the requirements for data protection as outlined in the COV ITRM IT Security Policy and Standard.

b) The agency shall require a non-disclosure agreement (see: Appendix C) and/or confidentiality agreement in order to strictly enforce the privacy of the data.

c) If the media must be removed from the agency premises and sent offsite for recovery, the agency must ensure and the vendor must agree to provide a secure facility and safeguarding capabilities such as background checks, etc., to address handling and processing requirements of sensitive information and that the vendor agrees to notify the agency immediately if an unauthorized party is believed to have gained access to

the Commonwealth data on the media.

Resources for the Removal of Commonwealth Data from Electronic Media

VITA will maintain on its website a list of resources that according to the manufacturers' claims (which the agencies are cautioned to verify), appear to meet this Standard for the removal of data from electronic media. The list of recommended software may be viewed at the VITA website.

Appendix A – Methods For Removal of Commonwealth Data

a. Magnetic Media Hard Drive Data Removal Methods

The following section outlines the acceptable methods to remove data from hard drives. Removal of Commonwealth data shall be performed on hard drives to ensure that information is removed from the hard drive in a manner that the data cannot be recovered. Before the removal process begins, the computer shall be disconnected from any production network to prevent accidental damage to the network operating system or other files on the network. For media going to surplus all identifying tags such as asset inventory tags or licensing information must be completed as outlined in Appendix B.

a.1 Acceptable Methods

There are four acceptable methods to be used for the hard drives:

- Overwriting – Overwriting is an approved method for removal. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process shall be correctly understood and carefully implemented.

- Degaussing – Degaussing is a process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable.

- Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired or when Commonwealth data cannot be removed. Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data.

- Encryption – The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users. Encryption with a temporary key (i.e. a key that cannot be recovered once the encryption process is complete) is an approved method for removal.

The method used for removal of Commonwealth data, depends upon the operability of the hard drive.

- Operable hard drives that will be reused shall be overwritten prior to disposition. If the operable hard drive is to be removed from service completely and has no value for surplus, it shall be physically destroyed or degaussed.

- If the hard drive is inoperable or has reached the end of its useful life, it shall be physically destroyed or degaussed.

Clearing data (deleting files) removes information from electronic media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is ***NOT*** an acceptable method of removing Commonwealth data from agency or service provider hard disk storage media.

a.2 Overwriting

Overwriting is an approved method for the removal of Commonwealth data from *magnetic media* hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. The overwriting process including the software/hardware products and applications used for the overwriting process shall include the following steps:

a) The data shall be properly overwritten with zeros or pseudo random pattern with a minimum of one pass. – (The software*/hardware* shall have the capability to overwrite as required above, including all sectors, blocks, tracks, and any unused disk space on the entire disk medium.

b) The software/hardware shall have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any intelligible data.

c) The software/hardware or supporting software shall have a method to verify that all data has been removed. Verification must be performed to verify that each drive overwritten is, in fact, clean of any intelligible or prior data. This verification can be either as a separate process or included as part of the software/hardware used for overwriting.

d) Sectors not overwritten shall be identified and if they cannot be removed, overwriting is not acceptable and another method must be employed.

a.3 Degaussing

Degaussing is a process whereby the magnetic media is erased. Magnetic media hard drives seldom can be used after degaussing. The degaussing method will only be used for hard drives when the drive is inoperable and will not be used for further service.

Please note that extreme care should be used when using degaussing equipment since this equipment can cause damage to nearby telephones, monitors, and other non-shielded electronic equipment. Also, the use of degaussing equipment does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts must be audited periodically to detect equipment or procedure failures. The following steps shall be followed when hard drives are degaussed:

a) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

b) Shielding materials (cabinets, mounting brackets), which may interfere with the degaussing equipment magnetic field, shall be removed from the magnetic media hard drive before degaussing.

c) Magnetic media hard disk platters shall be degaussed in accordance with the manufacturer's specifications.

a.4 Physical Destruction

Magnetic media hard drives shall be destroyed when they are defective or cannot be repaired or Commonwealth data cannot be removed for reuse.

a) Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data. This can be attained by removing the magnetic media hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The magnetic

media hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

b) Multiple holes drilled into the magnetic media hard disk platters is an optional method of destruction that will preclude use of the hard drive and provide reasonable protection of data written on the drive.

a.5 Encryption

Encryption with a temporary key (i.e. a key that cannot be recovered once the encryption process is complete) is an approved method for removal. Encryption of data means replacing previously stored plain text data on the magnetic media hard disk platters with the cypher text resulting from the encryption process. All data on the magnetic media hard disk platters must be encrypted using volume or full disk encryption. Encryption of individual files is not recommended. This method effectively renders the data unrecoverable so long as the key is **NOT** recoverable once the encryption process is complete. The use of encryption shall be correctly understood and carefully implemented. The encryption process including the software products and applications used for the encryption process shall include the following steps:

a) The data shall be properly encrypted with a random key of at least 256-bits in length. The key must not be stored on the device to be encrypted and must not be retained once the encryption process has completed.

b) The encryption software must conform to the Federal Information Processing Standard (FIPS) Publication 140-2 Standard (excluding Electronic Code Book mechanism for the encryption process) for the generation of cypher text and must not contain any known software vulnerabilities.

c) The software or supporting software shall have a method to verify that all data has been encrypted. Verification must be performed to verify that each drive encrypted is, in fact, devoid of any plain text data. This verification can be either as a separate process or included as part of the software used for encryption.

b. Non-Volatile Memory Devices Data Removal Method

Electronic devices that hold data or configurations in non-volatile memory shall have all Commonwealth data removed by the method recommended by the manufacturer for devices. This is to include all computer equipment that has memory such as personal computers, mobile devices, network appliances, routers, firewalls and switches.

c. Solid State Memory Devices

Traditional hard drives use magnetic media storage platters to record data so overwriting memory locations to remove data is a well-known and simple action. Solid State Device (SSD) technology uses a form of flash memory for data storage.

Traditional spinning hard disk wiping tools cannot guarantee the wiping of data on Solid State Drives (SSD). Traditional wiping tools write data to the disk to overwrite data on the drive. Due to differences in storage technology writing data to a NAND flash-based SSD does not result in an empty drive. The drive must still be erased before new data is written which shortens the service life of the SSD. The built-in sanitize or secure erase function should be invoked per the asset or device manufacturers instruction to consider the data on the drive erased or wiped. Should the sanitize or secure erase function be unable to be performed and verified the drive should be physically destroyed.

SSD's today utilize one of two different technologies interface with the computer; SATA (Serial Advanced Technology Attachment) and NVMe (Non-Volatile Memory Express). Just about every SSD in production today has a sanitize function, often referred to as 'secure erase' or 'secure wipe', built into the firmware of the drive. The sanitize commands are invokable via system BIOS, manufacturer application, or 3rd party application. The specific sanitize commands are different between the SATA and NVMe technologies but the result is the same; secure erasure of all user data from an SSD and restoration of the drive to a fresh-out-of-box (FOB) performance state

For most current HP and Dell laptop models this can be done via the BIOS. The wipe features performed via the BIOS may also work for traditional HDD's as well.

https://www.dell.com/support/kbdoc/en-us/000146892/dell-data-wipe

https://support.hp.com/us-en/document/c06204100

c.1 Acceptable Methods

There are three acceptable methods to be used for the SSDs:

- Physical Destruction – SSDs should be physically destroyed when they are defective or cannot be economically repaired or when Commonwealth data cannot be removed. Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data.

- Encryption of data with temporary key – Encryption with a temporary key (i.e. a key that cannot be recovered once the encryption process is complete) is an approved method for removal. Encryption of data means replacing previously stored plain text data on the SSD with the cypher text resulting from the encryption process. All data on the SSD must be encrypted using volume or full disk encryption. Encryption of individual files is not recommended. This method effectively renders the data unrecoverable so long as the key is not recoverable once the encryption process is complete. The use of encryption shall be correctly understood and carefully implemented.

- ATA / NVMe Secure Erase - The SSD firmware has an embedded sanitize command set that will overwrite all data on the SSD. This command can be managed by software that runs within a bootable environment.

The method used for removal of Commonwealth data, depends upon the operability of the SSD:

- Operable SSDs that will be reused shall *have the secure erase functions successfully applied or* be encrypted with a temporary key (i.e. a key that cannot be recovered once the encryption process is complete) prior to disposition. If the operable SSD is to be removed from service completely and has no value for surplus, it shall be physically destroyed.

- If the SSD is inoperable or has reached the end of its useful life, it shall be physically destroyed.

Clearing data (deleting files) removes information from electronic media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is NOT an acceptable method of removing Commonwealth data from agency or service provider SSDs.

c.2 Physical Destruction

SSDs shall be destroyed when they are defective or Commonwealth data cannot be removed for reuse.

a) Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data. This can be attained by removing the SSD Flash memory chips from the protective enclosure. The SSD FLASH memory chips must then be subjected to physical force (pounding with a hammer or processed in a shredder) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the SSD FLASH memory chips so it cannot be reinserted into a functioning computer.

b) Multiple holes drilled into the SSD enclosure containing the SSD FLASH memory chips is an optional method of destruction that will preclude use of the SSD and provide reasonable protection of data written on the drive.

c.3 Encryption

Encryption with a temporary key (i.e. a key that cannot be recovered once the encryption process is complete) is an approved method for removal. Encryption of data means replacing previously stored plain text data on the SSD with the cypher text resulting from the encryption process. All data on the SSD must be encrypted using volume or full disk encryption. Encryption of individual files is not recommended. This method effectively renders the data unrecoverable so long as the key is **NOT** recoverable once the encryption process is complete. The use of encryption shall be correctly understood and carefully implemented. The encryption process including the software products and applications used for the encryption process shall include the following steps:

a) The data shall be properly encrypted with a random key of at least 256 -bits in length. The key must not be stored on the device to be encrypted and must not be retained once the encryption process has completed.

b) The encryption software must conform to the Federal Information Processing Standard (FIPS) Publication 140-2 Standard (excluding Electronic Code Book mechanism for the encryption process) for the generation of cypher text and must not contain any known software vulnerabilities.

c) The software or supporting software shall have a method to verify that all data has been encrypted. Verification must be performed to verify that each drive encrypted is, in fact, devoid of any plain text data. This verification can be either as a separate process or included as part of the software used for encryption.

d. Multi-Function Devices

A Multi-function device (MFD) performs a number of input and output document functions including print, scan, copy, email and fax. MFDs store many types of sensitive data on an internal storage device including configuration settings for the operation of the device, configuration settings for the network administrative interface, and previously processed data. This storage device could be a traditional magnetic hard drive, a SSD, a Flash-based chip array, or a hybrid combination of devices. The information stored on the internal storage device could create a risk to an organization if exposed. Before disposing of a MFD, care should be taken to ensure that organizational information has been completely removed. The removal process for data contained within a multi-function device should follow the acceptable removal methods for the type of physical storage device as defined within this standard. Before the removal process begins, the MFD shall be disconnected from any production network to prevent accidental damage to the network operating system or other files on the network. For media going to surplus all identifying tags such as asset inventory tags or licensing information must be completed as outlined in Appendix B.

e. Mobile Devices

Mobile Devices are defined as devices that are highly portable, utilize Flash-based storage technology, and are not traditionally serviceable by the end-user. Examples of mobile devices include cell phones,

smartphones, tablets, and smart watches Mobile devices can contain both internal and external Flash-based storage media. Failure to properly sanitize all storage media could create a risk to an organization if exposed. Before disposing of a mobile device, care should be taken to ensure that organizational information has been completely removed. The removal process for data contained within a mobile device that is to be disposed or provided to another entity/organization should follow the acceptable removal methods for the type of physical storage device as defined within this standard.

The following section provides additional information on the acceptable methods to remove data from mobile devices. Removal of Commonwealth data shall be performed on mobile devices to ensure that information is removed from the mobile device in a manner that the data cannot be recovered. For media going to surplus all identifying tags such as asset inventory tags or licensing information must be completed as outlined in Appendix B. The following instructions were accurate at the time of publishing this standard. Please refer to the manufacturers' current recommendations to purge data appropriately.

e.1 Acceptable Methods for Apple iOS

The acceptable method of information removal for an Apple iOS device that will be repurposed within an agency is:

Clear/ Purge:
The data on the device should be purged without physically destroying the Flash-memory chips. To perform the data purge:

- Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu).

Once the Clear/Purge operation is complete, manually inspect the areas of the device such as the browser history, files, photos, and contacts to verify that no organizational information has been retained on the device. Refer to the manufacturer's support website and published documentation for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and OS versions*. Additionally, the device should be removed from the Apple ID account it was connect to.*

The acceptable method of information removal for an Apple iOS device that will be surplused or provided to another agency is:

Destroy:
The data on the device should be removed by physically destroying the Flash-memory chips. The optimal methods to physically destroy the Flash-memory chips are to shred, disintegrate, pulverize, or incinerate. If the incinerate option is chosen the actions must be performed in a licensed incinerator.

e.2 Acceptable Methods for Open Handset Alliance (OHA) Android Devices:

The acceptable method of information removal for an OHA Android device that will be repurposed within an agency is:

Clear/ Purge:
The factory data reset purges the data without physically destroying the Flash-memory chips. To perform the factory data reset follow these steps (these steps may differ slightly depending on your android phone):

1. Disable the Factory Reset Protection (FRP) in accordance with your mobile device's manufacturer's instructions. For example:
    a. On a Samsung Galaxy go to Settings > Lock screen and security > Screen lock type and choose None.

   b. ~~On a Huawei phone, go to Settings > Security & privacy > Screen lock & passwords > Disable lock screen password.~~
   c. On a Google Pixel phone, go to Settings > Security & location > Screen lock and choose None.
2. Remove the Google account. For example:
   a. On a Samsung Galaxy, go to Settings > Cloud & accounts > Accounts and tap on Google, then tap Remove account.
   b. On a Google Pixel, go to Settings > Accounts > Google and tap Remove account. If you have more than one Google account registered with your phone, then make sure you remove all of them.
3. Remove any manufacturer accounts. For example, if you have a Samsung Galaxy phone, then you should remove the Samsung account. To do this, go to Settings > Lock screen and security > Find My Mobile. Then enter the password if prompt, tap on the Samsung account at the top, and select More > Remove account.

4. Perform the Factory Data Reset in accordance with the manufacturer instructions. For example:
   On a Samsung Galaxy, go to Settings > General Management > Reset > Factory data reset and then tap Reset device.
   ~~On a Huawei phone, go to Settings > System > Reset > Factory data reset and then tap Reset Phone.~~
   On a Google Pixel, it's Settings > System > Advanced > Reset options > Erase all data (factory reset) and then tap Reset phone.

5. Manually inspect the areas of the device such as the browser history, files, photos, and contacts to verify that no organizational information has been retained on the device. Refer to the manufacturer's support website and published documentation for additional information on the proper sanitization procedure and for details about implementation differences between device versions and OS versions. Please note that device vendors or service providers may modify android configuration settings and operational capabilities. Therefore, no assumptions should be made about the level of assurance provided by performing a factory data reset.

The acceptable method of information removal for an OHA Android device that will be surplused or provided to another agency is:

Destroy:
The data on the device should be removed by physically destroying the Flash-memory chips. The optimal methods to physically destroy the Flash-memory chips are to shred, disintegrate, pulverize, or incinerate. If the incinerate option is chosen the actions must be performed in a licensed incinerator.

e.3 Acceptable Method for Other Devices (not iOS or Android):

The acceptable method of information removal for a device that will be repurposed within an agency is:

Clear/ Purge:
The data on the device should be purged without physically destroying the Flash-memory chips. To perform the data purge:

1. Select the full sanitize option in accordance with manufacturer instructions (typically in either the 'Options > Security Options > General Settings > [menu button] > Wipe Handheld' OR in 'Options > Security Options > Security Wipe' menu), making sure to select all subcategories of data types for sanitization.

2. Manually inspect the areas of the device such as the browser history, files, photos, and contacts to verify that no organizational information has been retained on the device. Refer to the manufacturer's support website and published documentation for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and OS versions.

The acceptable method of information removal for other devices (not iOS or Android) that will be surplused or provided to another agency is:

Destroy:
The data on the device should be removed by physically destroying the Flash-memory chips. The optimal methods to physically destroy the Flash-memory chips are to shred, disintegrate, pulverize, or incinerate. If the incinerate option is chosen the actions must be performed in a licensed incinerator.

f. Embedded Device Data Removal Methods

Embedded devices are defined as devices that are built to perform a single function of a very limited array of related functions. The device's operating system, configuration, and applications are usually static in nature and require specialized tools or techniques to modify the operation of the device. The device will employ a combination of erasable/programmable memory chips as well as Flash-based storage technology, and are not traditionally serviceable by the end-user. Examples of embedded devices include Point-of-Sale (POS) systems, touch-screen voting systems, kiosk computers, surveillance system digital video records, laboratory, internet of things (IOT) devices, and heating/ventilation/air condition control systems, etc,. Failure to properly sanitize all storage media could create a risk to an organization if exposed. Before disposing of an embedded device, care should be taken to ensure that organizational information has been completely removed. The removal process for data contained within an embedded device that is to be disposed or provided to another entity/organization should follow the acceptable removal methods for the type of physical storage device as defined within this standard. Before the removal process begins, the embedded device shall be disconnected from any production network to prevent accidental damage to the network operating system or other files on the network. For media going to surplus all identifying tags such as asset inventory tags or licensing information must be completed as outlined in Appendix B.

g. Other Electronic Media Data Removal Methods

If there is any risk of disclosure of sensitive data on media other than hard drives or devices that hold data or configurations in non-volatile memory, that media should be overwritten, degaussed or destroyed. Disintegration, incineration, pulverization, shredding or melting is acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.

Diskettes, CDs, DVDs, Tape backups may be degaussed or destroyed.

If overwriting or degaussing is selected, the steps for the selected method as stated in this standard shall be followed.

Burning, shredding or pulverizing of non-classified CD-ROMs by end- users is not recommended. CD-ROM discs do not require extensive destruction. Discs that are outdated or no longer needed may be rendered unreadable by cutting in half or deep scratching the data side (the shiny side without the label) with a nail, screwdriver, or similar tool. Two deep radial scratches extending from the small inner hole to the outer edge are sufficient to prevent unauthorized access to the data. These discs may be placed in the general waste stream for disposal.

h. Cloud Media Destruction Methods

Contractual agreements for cloud services must include requirement to remove and sanitize media in accordance with the requirements of COV ITRM Removal of Commonwealth Data Electronic Media Standards (SEC514).

Appendix B: Certification Tags

Certification of the Removal of Commonwealth Data from Electronic Media

This Standard requires that "The completed Certification Tag shall be affixed to the electronic media storing the data. For devices such as those with hard drive(s) or firewalls, a certification tag shall be affixed to each device. For mobile media such as CDs tapes, etc. one certification must be completed for each physically aggregated lot by affixing the Certification Tag to the box or shrink wrapped pallet." To reduce costs and standardize tags, each agency or its service provider shall adhere to the following method for tagging equipment certified to be in compliance with this Standard. If encryption was used as the method to remove data the tag should indicate that the data was "WIPED".

Printing Certification Tags

Copy the Certification Tags on the following page into a standard 8.5 by 11 inch portrait orientated word document. The tags are designed to print out on standard 2 by 4 inch shipping labels (i.e., Avery Template 5163). Preferably the tags will be printed in red letters for ease of recognition; therefore if possible, each agency or its service provider will print the tags from a color printer. In addition, the certification tags are also included on the Tools and Templates section on the VITA ITRM Policies, Standards, and Guidelines website.

To avoid tag printing errors, click your computer's Tools/Letters and Mailings/Envelopes and Labels tab and set the Labels option to "Avery standard, 5163 shipping" then practice using plain paper, holding the paper in front of a label sheet and up to the light, in order to check positioning. Most laser products are designed to work in laser printers directly from the automatic feed tray. Manual, copier and ink jet labels will not feed through consistently and may damage laser printers. To ensure proper operation, read the manufacturer's instructions that come with the shipping label before printing.

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**

SURPLUS/ASSET TAG NO: _____

_____
Removed by (PRINT NAME) **DATE**

_____
SUPERVISOR SIGNATURE **DATE**

_____
PRINT SUPERVISOR NAME

In addition, the certification tags are also included on the Tools and Templates section on the VITA ITRM Policies, Standards, and Guidelines website.

Appendix C: Non-Disclosure Agreement

CONFIDENTIALITY OF AGENCY INFORMATION:

1. Contractor shall take all precautions and measures necessary to ensure the integrity, nondisclosure, confidentiality and protection of all data and information obtained from <AGENCY NAME> or derived there from, including but not limited to all original reporting forms and data in any other form, and agrees to comply with all Federal and state guidelines including but not limited to the COV ITRM Standard SEC501and the Data Protection Guideline SEC507concerning the protection of sensitive data.

2. Prior to the commencement of any work for <AGENCY NAME>, the contractor shall declare in writing that he or she understands that all data and information obtained from <AGENCY NAME> or derived there from is sensitive and will be held in the strictest confidence by Contractor, its officers, directors, agents, and employees and that Contractor, its officers, directors, agents, and employees shall be governed by and comply with Federal and State laws prohibiting the disclosure of information obtained or compiled during the course of their work for <AGENCY NAME>.

3. All information obtained and work performed under this <AGENCY NAME> contract/order is considered sensitive, requires use of sensitive and personal data and information and falls under one or more categories of information that is subject to protection from disclosure and misuse, including but not limited to: personal information and highly restricted personal information in connection with motor vehicle records under the Federal Drivers Privacy Protection Act, (18 USC 2721 et seq.) law enforcement sensitive data and information, the Privacy Act, personal, vehicle and driver information as defined under and governed by Va. Code §46.2-208 et seq. and personal information as defined under and governed by the Virginia Government Data Collection and Dissemination Practices Act (VA Code §2.2-3800 et seq.).

4. All source materials/data/information and resultant work products compiled or created and any information or portion of information derived there from are the property of <AGENCY NAME> and must not be used by the contractor for any purpose other than the purpose outlined by this agreement.

5. The contractor, its officers, directors, agents and employees shall hold all information obtained under a <AGENCY NAME> contract/order in the strictest confidence. All information obtained shall be used only for the purpose of performing this contract/order and shall not be divulged nor made known in any manner to any person except as necessary to perform this contract/order. Neither Contractor, nor its officers, directors, agents, or employees shall divulge, sell, or distribute any information obtained from <AGENCY NAME> or derived there from at any point in time, even after termination or expiration of a contract/order.

6. Except as specifically authorized by the contract/order, Contractor, its officers, directors, agents, and employees are prohibited from reproducing <AGENCY NAME> source media, written products, or any portion thereof.

7. The contractor shall notify in writing, each of its officers, directors, agents, and employees having access to <AGENCY NAME> information that such information may be used only for the purpose and to the extent authorized in this contract.

8. The Contractor shall provide a security plan outlining the steps and methods taken to secure and protect the information provided by <AGENCY NAME> to address the following points:

- Security of Files and/or Copies of Records (for Hardcopy).
- Security of on-line Computer Terminals (On-Line Users Only).
- Designation of Authorized Users/Assignment of Access Codes.
- For automated interfaces/electronic extraction and storage of data, if applicable:
- Security of Records, Files, and Systems, use of encryption for storage.

- Names and addresses of data extraction method and software creators/vendors,
- Network Diagrams and descriptions of Data Extraction methods and software,
- Descriptions of system support processes including backup methods and frequencies.
- Proposed Audit/Management Controls Over Access and Dissemination of Requested Information.

9. Contractor agrees to comply with all federal and state statues, rules and regulations and understands that disclosure of any information, by any means, for a purpose or to an extent unauthorized herein, shall be grounds for immediate termination of this agreement may subject the offender to criminal sanctions.

10. Contractor shall indemnify, defend, and hold harmless the Commonwealth, <AGENCY NAME>, its officers, directors, employees and agents from and against all losses, liabilities, damages and all related costs and expenses (including reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgments, interest and penalties), incurred in connection with any action or proceeding arising directly or indirectly from unauthorized use or disclosure by Contractor, its agents, directors, officers or employees, of any data or information obtained from <AGENCY NAME> pursuant to this agreement, or derived therefrom. Contractor shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. Contractor shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification required may be delayed if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.

- Notice may be provided by one of the following methods:

(1) written notice to the most recent available address the person or business has in its records;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following:

i. e-mail notice when the person or business has an e-mail address for the subject persons;

ii. conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

iii. notification by major statewide media, including newspaper, radio and television.

- If a person discovers circumstances requiring notification of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

- Notification must include:

(1) a general description of what occurred and when:

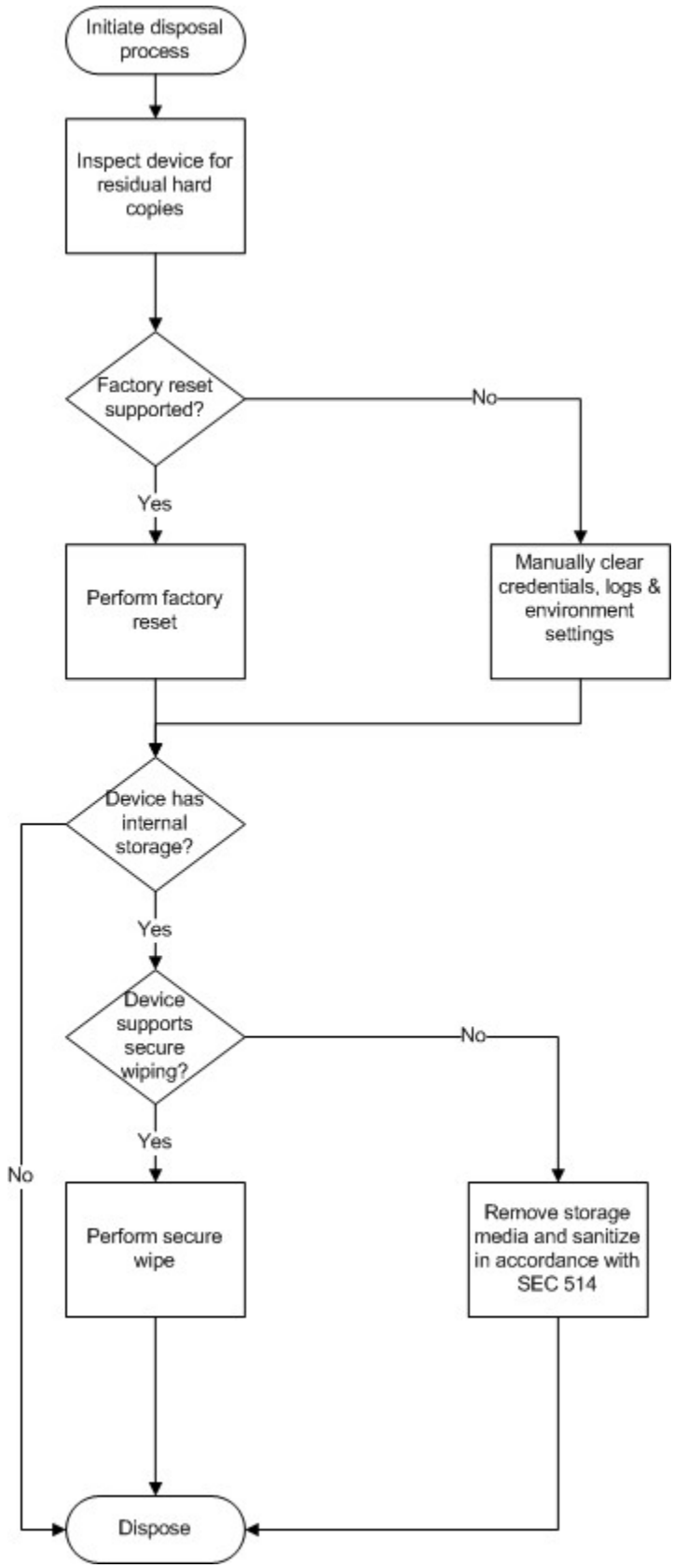
(2) the type of PII that was involved

(3) what actions have been taken to protect the individuals personal information from further unauthorized disclosure.

(4) what if anything, the contractor will do to assist affected individuals, including contact information for more information and assistance; and

(5) what actions the contractor recommends that the individual take.

Appendix D: Data Removal Quality Assurance Form

Date:	
Tester(s):	
Total Number of Devices in the Lot:	
Number of Devices Tested:	
Method of Testing:	
Findings:	

Appendix E: Disposal Process Flow Chart