

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management

INFORMATION TECHNOLOGY DATA PROTECTION GUIDELINE

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the user's responsibility to ensure that he or she has the latest version of the ITRM publication. Questions should be directed to the Director for Policy, Practice and Architecture (PPA) at VITA's IT Investment and Enterprise Solutions (ITIES) Directorate. ITIES will issue a Change Notice Alert when the publication is revised. The Alert will be posted on the VITA Web site. An email announcement of the Alert will be sent to the Agency Information Technology Resources (AITRs) at all state agencies and institutions, as well as other parties PPA considers interested in the publication's revision.

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

Version	Date	Purpose of Revision
Original	04/18/2007	Base Document
Revision 1	07/02/2007	To correct grammatical error, change title description for PPA director, and to add COV to guideline title. None of these changes altered the substance and meaning of the guideline.

Review Process

Technology Strategy and Solutions Directorate Review

N. Jerry Simonoff, VITA Director of Information Technology Investment and Enterprise Solutions (ITIES), and Chuck Tyger, Director for Policy, Practices, and Architecture Division, provided the initial review of the report.

Agency Online Review

The report was posted on VITA's Online Review and Comment Application (ORCA) for 30 days. All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were carefully evaluated and the individual commenters were notified of the action taken.

PAGE INTENTIONALY BLANK

Publication Designation

ITRM Guideline SEC507-00

Subject

Information Technology Data Protection

Effective Date

April 18, 2007

Scheduled Review

One (1) year from effective date

Authority*Code of Virginia* § 2.2-603(F)
(Authority of Agency Directors)*Code of Virginia*, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; “VITA;” Appointment of Chief Information Officer (CIO))**Scope**

This *Guideline* is offered as guidance to all Executive Branch State agencies and institutions of higher education (collectively referred to as “agency”) that manage, develop, purchase, and use information technology (IT) resources in the Commonwealth.

Purpose

To guide agencies in the implementation of the information technology contingency planning requirements defined by ITRM Standard SEC501-01.

General Responsibilities

(Italics indicate quote from the Code of Virginia)

Chief Information Officer

In accordance with *Code of Virginia* § 2.2-2009, the CIO is assigned the following duties: *“the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures, and standards shall address the scope of*

security audits and which public bodies are authorized to conduct security audits.”

Chief Information Security Officer

The 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 IT systems and data.

IT Investment and Enterprise Solutions Directorate

In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the IT Investment and Enterprise Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions.”*

All State Agencies

In accordance with § 2.2-603, § 2.2-2005, and §2.2-2009 of the *Code of Virginia*, all Executive Branch State agencies are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the Chief Information Officer of the Commonwealth.

Definitions

Agency All Executive Branch State agencies and institutions of higher education that manage, develop, purchase, and use IT resources in the Commonwealth of Virginia (COV).

Agency Control - If an agency is the Data Owner of the data contained in a Government database, that agency controls the Government database.

BIA - Business impact analysis – The process of determining the potential consequences of a disruption or degradation of business functions.

COOP – Continuity of Operations Plan – A set of documented procedures developed to provide for the

continuance of essential business functions during an emergency.

Data - Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge

Database - a collection of data organized into interrelated tables and specifications of data objects.

Data Communications - Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COV data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of this information. As used in this Guideline, Data Communications is included in the definition of government database herein.

Data Owner - An agency manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data

Government Database: For the purposes of this document, the term “government database” includes both databases that contain COV data and data communications that transport COV data. This definition applies irrespective of whether the COV information is in a physical database structure maintained by COV or a third-party provider. However, this definition does not include databases within Agencies that have been determined by the Agencies themselves to be non-governmental. See also *Database* and *Data Communications*.

Information Security Officer (ISO) - The individual who is responsible for the development, implementation, oversight, and maintenance of the agency’s IT security program.

IT System - An interconnected set of IT resources and data under the same direct management control.

Sensitive Data - Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of agency programs, or the privacy to which individuals are entitled.

Sensitive IT Systems - COV IT systems that store, process, or transmit sensitive data.

System Owner - An agency Manager responsible for the operation and maintenance of an agency IT system.

Threat - Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Related ITRM Policy and Standards

ITRM Policy, SEC500-02, Information Technology Security Policy (Effective 07/01/2006)
ITRM Standard SEC501-01: Information Technology Security Standard (Effective 07/01/2006)
ITRM Standard SEC2003-02-1: Data Removal from State Electronic Equipment Standard (Effective 03/08/2004)

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	INFORMATION TECHNOLOGY SECURITY	1
1.2	DATA PROTECTION	1
1.2.1	<i>Sensitive Data</i>	1
1.2.2	<i>Risks to Data</i>	1
1.2.3	<i>Special Precautions for Sensitive Data Storage</i>	2
1.2.4	<i>Special Precautions for Sensitive Data in Transmission</i>	3
1.3	DOCUMENTATION OF AGENCY PRACTICES	3
2	KEY DATA PROTECTION ROLES AND RESPONSIBILITIES	4
2.1	DATA OWNER	4
2.2	DATA CUSTODIAN	4
3	DATA STORAGE MEDIA PROTECTION	5
3.1	SENSITIVE DATA ON MOBILE DATA STORAGE MEDIA.....	5
3.1.1	<i>Definition of Mobile Data Storage Media</i>	5
3.1.2	<i>Agency Head Approval</i>	5
3.1.3	<i>Logical and Physical Security of Mobile Data Media</i>	5
3.2	AUTHORIZING PHYSICAL ACCESS TO DATA STORAGE MEDIA	7
3.2.1	<i>Authorization and Media Tracking</i>	7
3.3	DISPOSAL AND REUSE OF DATA STORAGE MEDIA.....	8
3.3.1	<i>Disposal of Data Storage Media</i>	8
3.3.2	<i>Re-Use of Data Storage Media</i>	9
4	ENCRYPTION.....	12
4.1	TYPES OF ENCRYPTION	13
4.1.1	<i>Data-At-Rest versus Data-In-Motion</i>	13
4.1.2	<i>Where to Encrypt</i>	14
4.1.3	<i>Private vs. Public Key Encryption</i>	16
4.2	DOCUMENTATION OF AGENCY ENCRYPTION PRACTICES	18
4.3	KEY MANAGEMENT AND PROTECTION	18
4.3.1	<i>Key Escrow</i>	20
4.4	USER TRAINING	20
5	APPENDICES.....	21
	APPENDIX A – DATA PROTECTION AND ACCESS REQUIREMENTS	22
	APPENDIX B – COMMUNICATING DATA PROTECTION REQUIREMENTS	23

APPENDIX C – DATA PROTECTION STATUS REPORT26
APPENDIX D – AUTHORIZATION TO STORE DATA ON A MOBILE DATA STORAGE MEDIUM29
APPENDIX E – CUSTODY/TERMINATION OF CUSTODY OF SENSITIVE DATA STORAGE MEDIA31

1 Introduction

1.1 Information Technology Security

In order to provide overall Information Technology (IT) security that is cost-effective and risk based, data protection must be a part of an agency's comprehensive risk management program. This Guideline presents a methodology for data protection suitable for supporting the requirements of the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Technology Security Policy (ITRM Policy SEC500-02), the COV ITRM Information Technology Security Standard (ITRM Standard SEC501-01), and the COV ITRM Information Technology Security Audit Standard (ITRM Standard SEC502-00). These documents are hereinafter referred to as the "Policy," "Standard," and "Audit Standard," respectively. Agencies are not required to use this guideline, and may use methodologies from other sources or develop their own methodologies, provided that the methodologies implement the requirements of the Policy and the Standard.

1.2 Data Protection

1.2.1 Sensitive Data

Sensitive data is data which, if compromised with respect to confidentiality, integrity, or availability, could adversely affect COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data is classified as sensitive if compromise of that data results in a material and significant adverse affect of COV's interest, the inability of the affected agency to conduct its business, and breach of privacy expectations. Data sensitivity classification is determined by the agency, and is the responsibility of the Data Owner, as defined in the *COV ITRM Risk Management Guideline* (ITRM Guideline SEC506-00).

1.2.2 Risks to Data

As shown in Figure 1, risks to data occur when threats combine with vulnerabilities to enable a compromise of confidentiality, integrity, or availability of data. For example, theft of sensitive data stored on an agency laptop is a threat. If agency employees are allowed to take laptops

home, data stored on the laptops is vulnerable to theft. One resulting risk is agency data residing on laptops taken home may be compromised if the laptop is stolen.

Figure 1 - Threat Formation



1.2.3 Special Precautions for Sensitive Data Storage

All stored data should be protected commensurate with sensitivity and risk. When sensitive data is stored on an electronic, magnetic, or optical data storage medium, the medium requires protection commensurate with this sensitivity and risk, as illustrated in Figure 2, and described in the remainder of this Guideline. Section 6 of the Standard requires, in particular, that sensitive data not be stored on a mobile data storage medium unless there is documented agency business necessity and description of mitigating controls approved in writing by the Agency Head (see also Section 3.1.2 of this Guideline).

Figure 2 - Data Protection Requirements



1.2.4 Special Precautions for Sensitive Data in Transmission

The Standard defines data protection requirements only for stored data. Agencies are strongly encouraged, however, to provide protection for data in transmission, commensurate with sensitivity and risk. A common means of protecting sensitive data in transmission is through encryption; data encryption technologies are discussed in Section 4 of this Guideline.

1.3 Documentation of Agency Practices

Section 6 of the Standard requires agencies to document data protection practices. The elements of such practices should describe, at a minimum:

- Roles and Responsibilities
- Relationship to agency privacy policies
- What must be protected
- Data storage protection practices
- Data encryption practices

The remainder of this document provides guidance for meeting these requirements.

2 Key Data Protection Roles and Responsibilities

While all users and managers of agency data have responsibilities for its protection, there are key roles that should be described in the agency's data protection practices.

2.1 Data Owner

The Data Owner is the agency manager responsible for the policy and practice decisions regarding the data to be protected. A Data Owner must:

- Evaluate and classify sensitivity of the data. This classification should occur as part of IT system and data sensitivity classification.¹
- Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
- Define requirements for access to the data.
- Communicate data protection requirements to the System Owner.

A template and example for documenting data sensitivity, and data protection and access requirements is contained in Appendix A; a template and example for communication data protection requirements to the System owner is contained in Appendix B.

2.2 Data Custodian

A Data Custodian is any individual or organization in possession of data for Data Owners. Data Custodians must:

- Protect the data in their possession from unauthorized access, alteration, destruction, or usage.
- Establish, monitoring, and operating IT systems in a manner consistent with COV IT and agency security policies and standards.
- Provide Data Owners with data protection status reports, as required by the Data Owner.

A template and example for a data protection status report is contained in Appendix C.

¹ IT system and data sensitivity classification is discussed in detail in the COV ITRM Risk Management Guideline (ITRM Guideline SEC507-00).

3 Data Storage Media Protection

The agency must document practices that it requires for data storage media protection. These practices should be in accordance with the agency's and COV IT policies and standards.

3.1 Sensitive Data on Mobile Data Storage Media

3.1.1 Definition of Mobile Data Storage Media

Mobile data storage media include any data storage medium which may be easily transported by an individual without any special equipment. Mobile data storage media includes, but is not limited to:

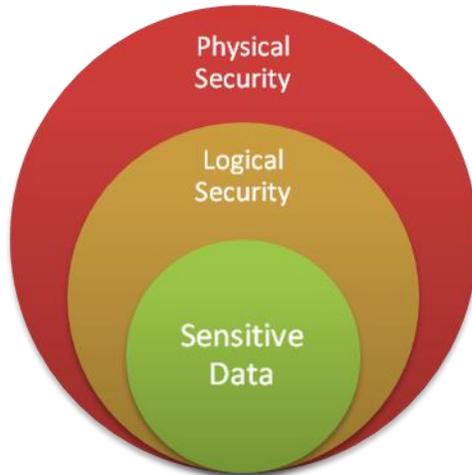
- Portable External Hard Drives
- Laptops, tablet PCs, palmtop, or other mobile computers that contain an internal hard drive.
- Personal digital assistants and smartphones (e.g. Blackberry, Palm, Treo, and Windows Mobile devices)
- Compact and Digital Video Disks (CDs/DVDs)
- Floppy Disks
- Flash Drives (memory stick, USB drive, MMC, SD, and others)

3.1.2 Agency Head Approval

Sensitive data may not be stored on mobile data storage media without a documented agency business necessity and description of mitigating controls approved in writing by the Agency Head. All data storage media containing sensitive data must be both physically and logically secured. The approval must document the business reasons for accepting the risks to the data and a description of mitigating controls in place. Appendix A contains an example and template for Authorization to Store Sensitive Data on a Mobile Medium.

3.1.3 Logical and Physical Security of Mobile Data Media

Sensitive data requires multiple types of protection so that the confidentiality, integrity, or availability of data cannot be degraded by compromise of a single protection mechanism. For this reason, access to sensitive data stored on mobile data media must be both logically and physically secured. Figure 3 depicts this multi-layer protection.

Figure 3 - Logical and Physical Protection of Sensitive Data**a) Logical Security**

Logical security includes IT protection mechanisms to limit users' access to information and to restrict their access levels based on the rule of least privilege². Logical access controls are built into operating systems, and may be part of the logic of applications programs or database management systems. They may also be implemented by add-on security packages, such as Radius and Kerberos. Such packages are available for a variety of systems, including PCs and mainframes. Additionally, logical access controls may be present in specialized components, such as remote access servers, that regulate communications between computers and networks.

² The rule of least privilege states that access to data should be provided only to those who require it and to the extent they require it. For example, if a user has the need to view data but not change it, that user should be given read only access to the data, not read-write access. The rule of least privilege is often referred to as the “need to know.”

An example of logical security of data is the assignment of a power-on password to access a laptop computer. Implemented logical access controls should be geared to the risks to and sensitivity of the data.

b) Physical Security

Physical security includes physical protection mechanisms which restrict physical access to the data storage medium itself. An example of physical security of data is placing the medium in a locked office or file cabinet. The requirements for physical security of mobile storage media should be geared to the risks to and sensitivity of the data. Effective practices for physical security of mobile storage media include:

- Requiring use of locking security cables on mobile computers;
- Locking all offices where sensitive data is stored;
- Restricting the use of USB and Firewire based storage hard drives and flash drives; and
- Checking mobile storage media (for example, laptop PCs, CDs, DVDs, USB drives) in and out of agency facilities and documenting where the media is heading.

3.2 Authorizing Physical Access to Data Storage Media

Only authorized personnel are allowed to pick-up, receive, transfer, or deliver any data storage media containing sensitive data. In order to enforce this requirement, the agency should determine who is authorized, and how their access will be controlled.

3.2.1 Authorization and Media Tracking

To control physical access to data storage media, agencies should establish procedures to track custody. When service providers (delivery services, storage service providers, disaster recovery providers, etc.) have physical access to data storage media, the agency should work with the service provider to develop sets of procedures that:

- Validate authorizations; and
- Track custody.

Appendix D contains an example and template for Custody/Termination of Custody of Sensitive Data Storage Media.

3.3 Disposal and Reuse of Data Storage Media

If a data storage medium has become surplus, or it has reached the end of its service life and needs to be disposed of, the agency must follow, at a minimum, ITRM Standard SEC2003-02.1, *Removal of Commonwealth Data from State Electronic Equipment Standard*. A template for labeling data storage media for disposal may be found in SEC2003-02.1, Appendix A.

Magnetic and optical media cannot be cleansed of sensitive data simply by erasing or formatting the medium. Due to the physical properties of the medium and the disk technology, remnants of sensitive data may remain after erasure or formatting. To ensure complete removal of the sensitive data, overwriting, degaussing (in the case of magnetic media), or physical destruction of the medium is required. In cases of extremely sensitive information, a combination of two or more methods may be desirable. See Table 1 at the end of Section 3.3 for a comparison of the three methods.

3.3.1 Disposal of Data Storage Media

Agencies must dispose of data storage media by means of destruction when required by the Removal of Commonwealth Data from State Electronic Equipment Standard (SEC2003-02-1). The two approved methods for disposal for data storage media are degaussing and physical destruction.

Degaussing uses an extremely powerful magnet to destroy a magnetic disk by completely randomizing its magnetic field properties³. Degausses' must be used with care, because the fields they generate can impair or destroy other electronic equipment. In most cases, degaussing technical requirements may be obtained from the manufacturer of the hard disk.

Physical destruction entails crushing, shredding, incinerating, perforating, or otherwise rendering the medium physically unable to be used. It is important to note physical destruction does not

³ In general, a disk is unusable after degaussing. It is important to note, however, that degaussing may not completely destroy all sensitive data on the magnetic medium, and that advanced forensic tools exist that may enable recovery of sensitive data from a magnetic disk that has been degaussed.

alter the magnetic properties of the data storage medium and that physical destruction must be conducted in such a way as prevent recovery of sensitive data.

3.3.2 Re-Use of Data Storage Media

If the medium is to be re-used (either because it is to be repurposed or surplus), one of the most proven ways to eliminate data from magnetic or optical media is overwriting the data.

Overwriting simply means to write patterns of non-sensitive data (usually, simply binary ones and zeros) over the existing data. The method and complexity of the overwriting required may vary depending on the sensitivity of the original data, Typically, this variation takes the form of multiple iterations (or passes) of overwriting, and variations in the patterns of ones and zeros used.

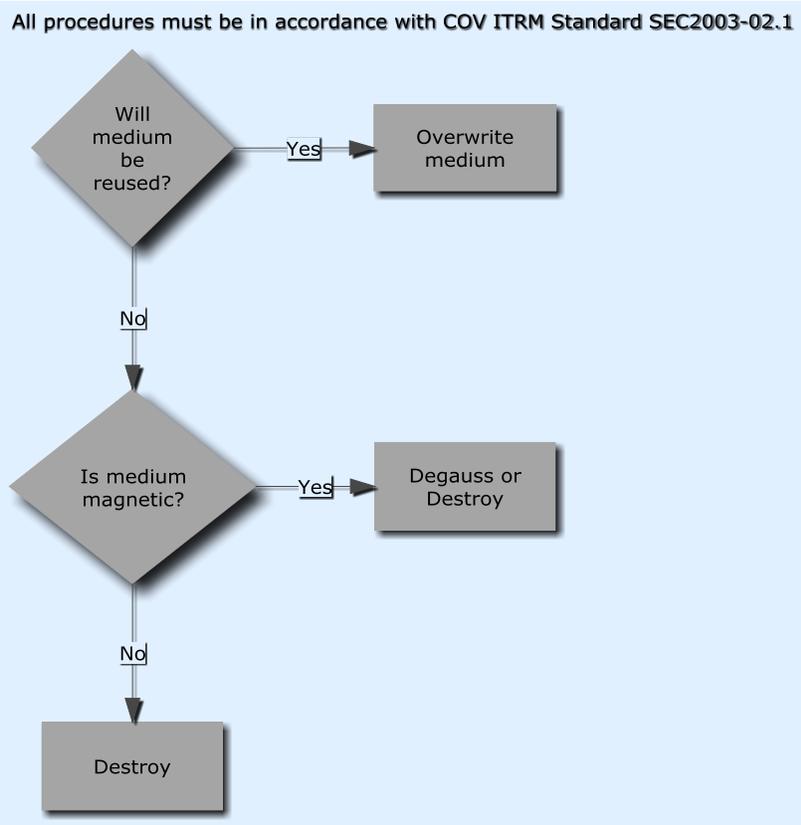
Many operating systems have built-in overwriting mechanisms, and there are several commercial off-the-shelf tools available. A list of recommended tools may be found at

<http://www.vita.virginia.gov/library/default.aspx?id=5046>.

Figure 4 illustrates the process of overwriting data. The ones and zeroes depict data that has been overwritten, while the other characters depict data that has not yet been overwritten. Table 1, which follows, summarizes data storage medium disposal methods; Figure 5 illustrates the data storage medium disposal process.

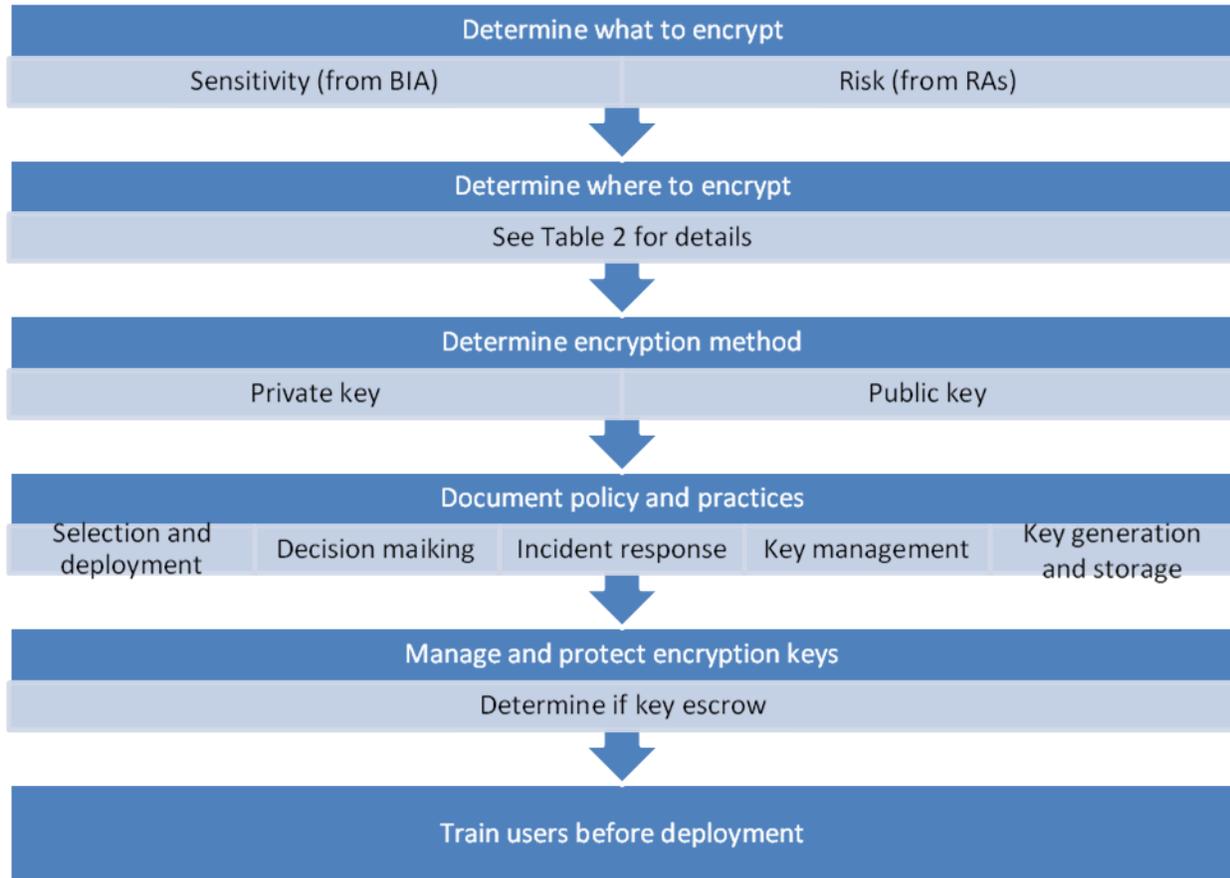
<p>Physical Destruction</p>	<ul style="list-style-type: none"> • Optical, flash, magnetic media 	<ul style="list-style-type: none"> • Media will not be reused; and • Speed of data destruction is important 	<ul style="list-style-type: none"> • Physical force (mangling) • Incineration • Disk surface perforation
------------------------------------	--	---	---

Figure 5 - Data Medium Disposal Process



4 Encryption

Encryption is the conversion of data into a form that is unreadable by an unauthorized user or process. Encrypted data must be decrypted (converted back to original form) prior to use. For most common encryption methods, a key is required for encryption and decryption. The major difference (from the users' standpoint) between encryption methods is the type and management of the keys. Agencies should consider encryption as a means of protecting data, commensurate with sensitivity and risk. Especially useful for higher risk situations such as removable media including laptops. Figure 6 illustrates the process of selecting and managing data encryption technologies.

Figure 6 - Data Encryption Technologies Selection and Management Process

4.1 Types of Encryption

4.1.1 Data-At-Rest versus Data-In-Motion

There are two types of data that may require encryption. “Data-in-motion” is data that is in transit between two points, and may also be referred to as data in transmission. Data-in-motion comprises traffic moving over LANs, WANs, the Internet, etc. Another form of data-in motion is transport of data via mobile media (e.g. flash drives, portable hard drives, laptops, etc.)

“Data-at-rest” is data at the end-points of the transmission. That is data stored in applications, files, databases, etc. Encryption of data-in-motion does not protect data-at-rest.

4.1.2 Where to Encrypt

Once the decision to encrypt data has been made, the Data Owner and System Owner should decide whether to implement encryption of data-in-motion, data-at-rest, or both. Before selecting data-in-motion, data-at-rest, or both, consideration should be given to:

- The sensitivity of the data and the risks to which it is subject;
- The amount of data requiring encryption;
- The frequency of changes to the data;
- The cost to implement a specific solution; and
- The burden the encryption may place on IT system users.

Table 2 outlines IT platforms where data may be encrypted and the benefits and drawbacks of each.

Table 2 - Encryption Location Comparison

Location	Cost	Benefits	Drawbacks
Application	<ul style="list-style-type: none"> • Relatively inexpensive 	<ul style="list-style-type: none"> • May protect both “data-in-motion” & “data-at-rest”, depending on application • Transparent to end users • Does not interfere with lower level protocols 	<ul style="list-style-type: none"> • Must be implemented for each application • May requires customization of application • May require additional configuration of application • Creates additional application overhead
Host (Mainframe or	<ul style="list-style-type: none"> • Moderately 	<ul style="list-style-type: none"> • Protects all “data-at-rest” residing on the 	<ul style="list-style-type: none"> • Does not protect

Location	Cost	Benefits	Drawbacks
Server)	expensive	server & its storage <ul style="list-style-type: none"> • Transparent to end users • Does not interfere with lower level protocols 	“data-in-motion” <ul style="list-style-type: none"> • Must be implemented for each host • Requires administration • Creates additional host overhead
Network encryption (Encryption of all network traffic through hardware or software)	<ul style="list-style-type: none"> • Moderately expensive 	<ul style="list-style-type: none"> • Protects all data transiting the network • Transparent to the end users • Fewer encryption devices require less key management 	<ul style="list-style-type: none"> • May interfere with network & storage management protocols • Does not protect “data-at-rest” • Requires dedicated encryption devices, which require management
Storage encryption (Encryption of all data on a storage device such as SAN or laptop hard disk through hardware or software)	<ul style="list-style-type: none"> • Moderately expensive 	<ul style="list-style-type: none"> • Protects all data residing on the storage device 	<ul style="list-style-type: none"> • Does not protect “data-in-motion” • Since all stored data is encrypted, non-sensitive data incurs burden of encryption • May not be transparent to end-user; may require user training • Encryption devices or

Location	Cost	Benefits	Drawbacks
			software require more management
File encryption	<ul style="list-style-type: none"> Moderately inexpensive to moderately expensive, depending on solution 	<ul style="list-style-type: none"> Protects files selected for encryption, avoiding burden of encrypting non-sensitive data 	<ul style="list-style-type: none"> Does not protect “data-in-motion” Encryption devices or software require more management May not be transparent to end-user; may require user training

4.1.3 Private vs. Public Key Encryption

Private key encryption is also known as shared key or symmetric encryption. In private key encryption, the encryption and decryption keys are the same. With private key encryption, the biggest challenge is sharing the keys themselves in a secure manner. This challenge is less of an issue with data-at-rest, because the key can be managed close to the storage medium, as, for example, when a hard disk needs encryption, encrypt all the data to be stored. Figure 7 outlines the operation of private key encryption.

Figure 7 - Shared Private Key Encryption (Good fit for data-at-rest that will remain with one custodian.)





Private key encryption, however, presents greater challenges when applied to data-in-motion. If two custodians of sensitive data wish to transmit data back and forth, the challenge becomes how to share the knowledge of the key without compromising the confidentiality of the key.

For example, if an agency headquarters in Richmond wishes to share data encrypted with its regional location in Big Stone Gap via its Wide Area Network, using private key encryption, the agency must find a means other than network to share the key, because the confidentiality of the key would be compromised if shared across the network. Sharing private keys via non-network means also provides challenges, as the confidentiality, integrity, and availability of the keys must be protected in transit, for example, by sending them via Registered U.S. Mail.

Public key or asymmetric encryption addresses these difficulties by encrypting the data with a public key that is defined by the receiver. The data is transmitted to the receiver, who then decrypts the data with the receiver's private key, which is known only to the receiver. This encryption method works very well for data-in-motion, since no private key-sharing is required. Figure 8 outlines the operation of public key encryption.

Figure 8 - Public Key Encryption (Good fit for data-in-motion and custodian-to-custodian sharing of data.)





The challenge in administering public key encryption is managing the public keys. In a large agency, this task involves a significant commitment of resources. To address these challenges, encryption vendors have created public key infrastructure management systems.

4.2 Documentation of Agency Encryption Practices

Agencies must document their encryption practices. The documentation must establish:

- Agency practices for selecting and deploying encryption technologies
- Practices to determine when, what, and how to encrypt.
- How to respond to an incident when keys are compromised.
- How the agency will securely manage, administer, and distribute keys
- Requirements for the generation and secure storage of keys.

4.3 Key Management and Protection

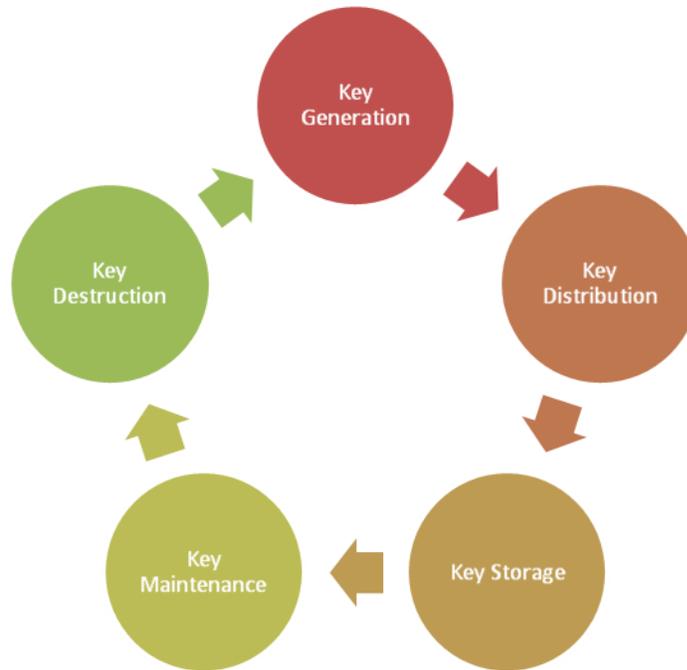
There are inherent risks if proper key management procedures are not followed because of the complexity of distributing keys to all users in a synchronized fashion. The loss, theft, or compromise of encryption keys could seriously affect the integrity, confidentiality, and availability of agency data. Without proper handling of keys during their life cycle, keys could be disclosed, modified, or substituted by unauthorized personnel who could then intercept, modify, or destroy the sensitive data. This risk can be significantly mitigated through adequate key controls and proper education on encryption key management.

To protect keys or keying materials during their life cycle, guidelines providing detailed instructions or planned security measures must be available and followed. Since most encryption algorithms are published and well known, the security of data being transmitted is dependent upon the protection of the key. The destruction or loss of the key is equivalent to the loss or destruction of the data itself. If disgruntled employees or unauthorized users know that

encryption keys are not changed regularly, more opportunities exist for encrypted communications to be monitored and broken over time.

Key management is the overall process of generating and distributing cryptographic keys to authorized recipients in a protected manner. Figure 9 illustrates the key management life cycle.

Figure 9 - Key Management

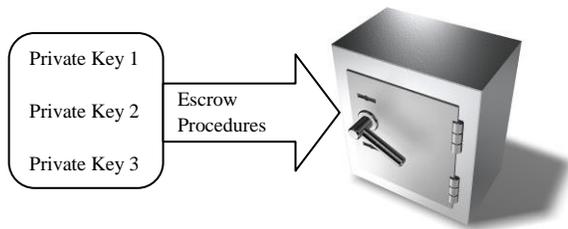


Encryption keys must be protected as sensitive data. Prior to deployment of encryption technologies, procedures to manage the keys must be developed and implemented. Key management systems and accompanying business processes can be obtained from most encryption vendors. Detailed guidance on key management can be found in NIST Special Publication 800-57, Recommendations for Key Management (http://csrc.nist.gov/CryptoToolkit/kms/SP800-57Part1_6-30-06.pdf).

4.3.1 Key Escrow

Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow by a third party, so that someone else can obtain them to decrypt messages. The keys are securely protected by the third party who is prohibited from accessing the keys unless requested by the Data Owner. Implementing a key escrow agreement addresses the recovery of the keys in case of loss. Figure 10 illustrates the operation of key escrow.

Figure 10 - Key Escrow



4.4 User Training

Prior to deployment of an encryption system, users and administrators must be trained in the agency's encryption policies and the use of the chosen encryption technologies. Most encryption vendors provide training for system administrators. Agencies should include user training on encryption technologies as part of initial and annual IT Security Awareness and Training.

5 Appendices

These Appendices provide examples and templates that agencies may use to document their use of many of the methodologies described in this Guideline. Each template consists of:

- 1) An example of the document, completed with fictional information; and
- 2) A blank version of the template for use by COV agencies.

The examples use different fonts for instructions and example information, as follows:

- Times New Roman text is used for the template itself.
- **Shaded Arial Bold text** is example text.
- *Times New Roman Italic text* is provided as instructions for completing the template.

Appendix A – Data Protection and Access Requirements

Example

Type of Data	Sensitive With Respect To			Required Special Protections	Access Requirements
	Confidentiality	Integrity	Availability		
Employee Records	X			Encrypted Cannot leave the agency headquarters	Agency Head authorization
Permit Applications	X	X		Encrypted for transmission	Two persons required to make changes Agency Head authorization
COOP Documents	X		X	Encrypted for storage Hard-copy backup	All agency employees
Customer Feedback				None	None

Type of Data	Sensitive With Respect To			Required Special Protections	Access Requirements
	Confidentiality	Integrity	Availability		

Appendix B – Communicating Data Protection Requirements**Example****Communication of Data Protection Requirements**Date: **March 15, 2007**Subject: **Protection of COOP Documentation Data**Data Owner: **Steve Brown, COOP Coordinator**System Owner: **Ann Lee, COOP Documentation System**

Please ensure the subject data is protected according to the requirements in the following table.

Note: Paste the table from Appendix A into the memorandum from the Data Owner to the System Owner.

Type of Data	Sensitive With Respect To			Required Special Protections	Access Requirements
	Confidentiality	Integrity	Availability		
Employee Records	X			Encrypted Cannot leave the agency headquarters	Agency Head authorization
Permit Applications	X	X		Encrypted for transmission	Two persons required to make changes Agency Head authorization
COOP Documents	X		X	Encrypted for storage Hard-copy backup	All agency employees

Customer Feedback				None	None
------------------------------	--	--	--	-------------	-------------

Communication of Data Protection Requirements

Date:

Subject:

Data Owner:

System Owner:

Please ensure the subject data is protected according to the requirements in the following table.

Note: Paste the table from Appendix A into the memorandum from the Data Owner to the System Owner.

Type of Data	Sensitive With Respect To			Required Special Protections	Access Requirements
	Confidentiality	Integrity	Availability		

Appendix C – Data Protection Status Report**Example****Data Protection Status Report**Date: **April 19, 2007**Subject: **Protection of COOP Documentation Data**Data Owner: **Steve Brown, COOP Coordinator**Data Custodian: **Sam Brown, Director, Acme IT Data Services**

This memorandum certifies that Acme IT Data Services has provided the required protection, documented below, to the subject data.

Note: Paste the table from Appendix A into the memorandum from the Data Custodian to the Data Owner.

Type of Data	Sensitive With Respect To			Required Special Protections	Access Requirements
	Confidentiality	Integrity	Availability		
Employee Records	X			Encrypted Cannot leave the agency headquarters	Agency Head authorization
Permit Applications	X	X		Encrypted for transmission	Two persons required to make changes Agency Head authorization
COOP Documents	X		X	Encrypted for storage Hard-copy backup	All agency employees

Customer Feedback				None	None
------------------------------	--	--	--	-------------	-------------

Data Protection Status Report

Date:

Subject:

Data Owner:

Data Custodian:

This memorandum certifies that *Name of Data Custodian* has provided the required protection, documented below, to the subject data.

Note: Paste the table from Appendix A into the memorandum from the Data Custodian to the Data Owner.

Type of Data	Sensitive With Respect To			Required Special Protections	Access Requirements
	Confidentiality	Integrity	Availability		

Appendix D – Authorization to Store Data on a Mobile Data Storage Medium

May 30, 2007

I hereby, authorize the storage of **Budget Formulation System (BFS) Agency Budget Plans** on **USB “flash” drives by Analysts in the BFA Budget Analysis Section**. I recognize the data is sensitive, and accept the risks of storage on the named medium. The business reasons driving this requirement are the needs to:

- a) **Allow Budget Analysts to work remotely to implement COV telework initiatives;**
- b) **Provide for physical transport of data to other agencies for use in budget review sessions;**
and
- c) **Provide access to the data from BFA computers not connected to the BFA network**

The mitigating controls in place are agency polices that require:

- a) **All USB “flash” drives to be protected with strong passwords; and**
- b) **Full disk encryption of USB “flash” drives used to store sensitive data; and**
- c) **BFA employees to keep USB “flash” drives that contain sensitive data under their physical control at all times.**

This authorization expires one year from the date above.



Date

I hereby, authorize the storage of Data to be stored on Data storage medium by Individuals authorized to store data . I recognize the data is sensitive, and accept the risks of storage on the named medium. The business reasons driving this requirement are the needs to:

- a) First reason
 - b) Second reason
 - c) Third reason
- Add additional reasons, as required*

Mitigating controls in place are:

- a) First mitigating control
 - b) Second mitigating control
 - c) Third mitigating control
- Add additional mitigating controls, as applicable*

This authorization expires one year from the date above.

 Agency Head Name

 Agency Head Title

 Agency Name

Appendix E – Custody/Termination of Custody of Sensitive Data Storage Media

Example

May 30, 2007

I hereby, authorize **Partner Services, Inc. (PSI)** to maintain custody of **Budget Formulation System (BFS) backup data** on **magnetic tape cartridges**. I recognize the data is sensitive, and accept the risks of authorizing this custody.

This authorization expires **one year** one year from the date above, or upon execution of the termination portion of this agreement.

[Redacted signature]

Authorization of custody is hereby terminated.

[Redacted signature]

November 15, 2007

Date

I hereby, authorize Data Custodian to maintain custody of Data for which custody is authorized on Specific data storage media . I recognize the data is sensitive, and accept the risks of authorizing this custody.

This authorization expires Period for which custody is authorized one year from the date above, or upon execution of the termination portion of this agreement.

 Data Owner Name
 Data Owner Title
 Agency Name

Authorization of custody is hereby terminated.

 Data Owner Name
 Data Owner Title
 Agency Name

 Termination Date