IT System and Data Classification Policy

EFFECTIVE DATE: 07/01/2014

PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure the Virginia Information Technologies Agency (VITA) develops, disseminates, and updates the IT System and Data Classification Policy. This policy and procedure establishes the minimum requirements for the IT System and Data Classification Policy.

This policy is intended to meet the requirements outlined in SEC501, Section 4 IT System and Data Sensitivity Classification.

SCOPE

All VITA employees (classified, hourly, or business partners) as well as all sensitive VITA systems

ACRONYMS

CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
HIPAA:	Health Insurance Portability and Accountability Act
IRS:	Internal Revenue Service
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
PCI:	Payment Card Industry
SEC501:	Information Security Standard 501
VITA:	Virginia Information Technologies Agency

DEFINITIONS

See COV ITRM Glossary

BACKGROUND

The IT System and Data Classification Policy at VITA is intended to facilitate the effective implementation of the processes necessary meet the IT System and Data Sensitivity Classification requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that VITA meet these requirements for all sensitive IT systems.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1) Responsible (R) – Person working on activity

2) Accountable (A) – Person with decision authority and one who delegates the work

3) Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity

4) Informed (I) – Person who needs to know of decision or action

Roles	Agency Head	Information Security Officer	Data Owner	System Administrator	System Owner
Tasks					
IDENTIFY THE TYPES OF DATA HANDLED BY EACH SYSTEM	I	C	A	R	I
DETERMINE WHETHER THE TYPE OF DATA IS SUBJECT TO REGULATORY REQUIREMENTS		C	A/R		I
CLASSIFY SENSITIVITY OF DATA	I	C	A/R		I
OBTAIN APPROVAL OF CLASSIFICATION	R	C	A		
VERIFY ALL SYSTEMS ARE CLASSIFIED		A	R	R	R
COMMUNICATE CLASSIFICATIONS	I	R	A	I	I
PROHIBIT POSTING OF SENSITIVE DATA ON PUBLICLY ACCESSIBLE MEDIUM	I	A	R	R	
REQUIRE ENCRYPTION		A	R	R	R
DOCUMENT EACH SENSITIVE IT SYSTEM		I	I	R	A
ASSIGN A SYSTEM OWNER, DATA OWNER, AND SYSTEM ADMINISTRATOR TO EACH SENSITIVE SYSTEM	A	R	I	I	I
UPDATE NETWORK DIAGRAMS		A		R	

STATEMENT OF POLICY

In accordance with SEC501, VITA shall identify any sensitive data that is data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on VITA and/or Commonwealth of Virginia (COV) interests, the conduct of VITA programs, or the privacy to which individuals are entitled. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. VITA must classify each IT system by sensitivity according to the most sensitive data that the IT system handles, stores, processes, transmits, etc.

A. IT SYSTEM AND DATA CLASSIFICATION

1. VITA's Information Security Officer (ISO) will:

   a. Use the results of VITA's Business Impact Analysis as a primary input to classifying the sensitivity of VITA's IT systems and data.

   b. Identify or require that the Data Owner Identify the type(s) of data handled by each VITA IT system.

   c. Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.

   Example: Some VITA IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973, § 508, Federal National Security Standards, etc.

   d. Determine or require that the Data Owner determine the potential damages to the agency of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system and classify the sensitivity of the data accordingly.

      i. Confidentiality, which addresses sensitivity to unauthorized disclosure;

      ii. Integrity, which addresses sensitivity to unauthorized modification; and

      iii. Availability, which addresses sensitivity to outages.

   Example: Data Owners should construct a table similar to the following table that classifies sensitivity requirements of all types of data. The following Sensitivity Analysis Results table is only an illustration.

System ID: ABC123	**Sensitivity Criteria**		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal Records	High	High	High

   e. Classify the IT system as sensitive if any type of data transmitted, stored or processed by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity or availability.

   Note: The ISO and/or Data Owner should consider classifying IT systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability, based on the materiality of a compromise of the IT system or the data it handles.

f. Review IT system and data classifications with the ISO or designee, and obtain Agency Head or designee approval of these classifications.

g. Verify and validate that all agency IT systems and data have been classified for sensitivity.

h. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.

i. Require that the agency prohibit posting any data classified as sensitive with respect to confidentiality on a public web site, ftp server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating logical and physical controls, and any residual risk.

j. Require encryption during transmission of data that is sensitive relative to confidentiality or integrity.

k. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process.

l. Document each sensitive IT system owned by VITA, including its ownership and boundaries, and update the documentation as changes occur.

m. As part of the documentation of each sensitive IT system owned by VITA, develop Interconnection Security Agreements with the other IT system with which the sensitive IT system interconnects or shares data, including, but not limited to:

    i. The types of shared data;

    ii. The direction(s) of data flow;

    iii. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator;

    iv. IT security requirements for each interconnected IT system and for each type of data shared;

    v. Other systems with which the IT systems interconnect or share data;

    vi. A requirement that System Owners of the IT systems that share data inform one another prior to establishing any additional interconnections or data sharing;

    vii. Specifications regarding if and how the shared data will be stored on each IT system;

    viii. Specifications that System Owners of the IT systems that share data acknowledge and agree to abide with any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data;

    ix. Each Data Owner’s authority to approve access to the shared data;

    x. Each System Owner’s responsibility to enforce the agreement; and

    xi. Approval of the agreement by each System Owner.

n. Assign a System Owner, Data Owner(s), and System Administrator(s) for each sensitive IT system.

   Note: A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

o. Maintain or cause its business partner to update network diagrams.

ASSOCIATED PROCEDURE VITA Information Security Program Policy

AUTHORITY REFERENCE *Code of Virginia, §2.2-2005 et seq.*
(Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency; "VITA")

OTHER REFERENCE ITRM Information Security Policy (SEC519)

ITRM Information Security Standard (SEC501)

Version History		
Version	Date	Change Summary
1	09/28/2007	Original document. Establishes requirements for the classification of IT systems and data according to their sensitivity with respect to Confidentiality, Integrity and Availability.
2	01/22/2009	Updated "Sensitivity" definition. Under Statement of Procedure clarified Item 9, added Item 10 and re-numbered subsequent items.
3	11/12/12	Administrative changes including relocating the definitions to COV ITRM Glossary
4	07/01/2014	Name changed and updated to conform to Information Security Standard SEC501 revision 8. Role matrix added