### IT System and Data Classification Policy TEMPLATE

### 

**EFFECTIVE DATE: 07/01/2014**

**IT System and Data Classification Policy Template**

# 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 that “YOUR AGENCY NAME” 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 “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all sensitive “YOUR AGENCY NAME” 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

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT System and Data Classification Policy at “YOUR AGENCY NAME” 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 “YOUR AGENCY NAME” 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, “YOUR AGENCY NAME” 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 “YOUR AGENCY NAME” and/or Commonwealth of Virginia (COV) interests, the conduct of “YOUR AGENCY NAME” 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. “YOUR AGENCY NAME” must classify each IT system by sensitivity according to the most sensitive data that the IT system handles, stores, processes, transmits, etc.

1. IT SYSTEM AND DATA CLASSIFICATION
   1. “YOUR AGENCY NAME”’s Information Security Officer (ISO) will:
      1. Use the results of “YOUR AGENCY NAME”’s Business Impact Analysis as a primary input to classifying the sensitivity of “YOUR AGENCY NAME”’s IT systems and data.
      2. Identify or require that the Data Owner Identify the type(s) of data handled by each “YOUR AGENCY NAME” IT system.
      3. Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.

**Example:** Some “YOUR AGENCY NAME” 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.

* + 1. 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.
       1. Confidentiality, which addresses sensitivity to unauthorized disclosure;
       2. Integrity, which addresses sensitivity to unauthorized modification; and
       3. 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 |

* + 1. 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.

* + 1. Review IT system and data classifications with the ISO or designee, and obtain Agency Head or designee approval of these classifications.
    2. Verify and validate that all agency IT systems and data have been classified for sensitivity.
    3. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.
    4. 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.
    5. Require encryption during transmission of data that is sensitive relative to confidentiality or integrity.
    6. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process.
    7. Document each sensitive IT system owned by “YOUR AGENCY NAME”, including its ownership and boundaries, and update the documentation as changes occur.
    8. As part of the documentation of each sensitive IT system owned by “YOUR AGENCY NAME”, develop Interconnection Security Agreements with the other IT system with which the sensitive IT system interconnects or shares data, including, but not limited to:
       1. The types of shared data;
       2. The direction(s) of data flow;
       3. 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;
       4. IT security requirements for each interconnected IT system and for each type of data shared;
       5. Other systems with which the IT systems interconnect or share data;
       6. A requirement that System Owners of the IT systems that share data inform one another prior to establishing any additional interconnections or data sharing;
       7. Specifications regarding if and how the shared data will be stored on each IT system;
       8. 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;
       9. Each Data Owner’s authority to approve access to the shared data;
       10. Each System Owner’s responsibility to enforce the agreement; and
       11. Approval of the agreement by each System Owner.
    9. 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.

* + 1. Maintain or cause its business partner to update network diagrams.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| 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 |
| 5 | 11/22/2021 | Formatting changes |