# COMMONWEALTH OF VIRGINIA


Information Technology Resource Management

Data Classification Standard

**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 the VITA Policy, Practice and Architecture (PPA) Division. PPA will issue a Change Notice Alert, post it on the VITA Web site, and provide an e-mail announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers to be interested in the change.

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

| Version | Date | Purpose of Revision |
|---|---|---|
| Original | 6/20/2025 | Base Document |

**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. Deleted language shall be noted by ~~striking it through.~~

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

**EXA-R-01 Example with No Change –** 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.*

# PREFACE

**Publication Designation**

COV ITRM Standard SEC540-01

**Effective Date**

June 20, 2025

**Compliance Date**

June 20, 2025

**Scheduled Review**

One (1) year from effective date

**Authority**

Virginia Code reference needed here.

***Scope***

*This standard is applicable to all executive branch agencies, independent agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology databases or data communications in the Commonwealth.*

***Purpose***

*This standard identifies, defines, and provides guidance on Data Classification for state agencies.*

***Chief Information Officer of the Commonwealth (CIO)***

*Develops and recommends to the Secretary of Technology statewide technical and data policies, standards and guidelines for information technology and related systems.*

***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.*

***Information Technology Advisory Council (ITAC)***

*Advises the CIO and Secretary of Technology on the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.*

***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.*

***Related ITRM Policies, Standards, and Guidelines***

*Commonwealth of Virginia Information Technology Security Policy (ITRM Policy SEC519)*

*Commonwealth of Virginia Information Technology Security Policy (ITRM Policy SEC530)*

***General Responsibilities***

*(Italics indicate quote from the Code of Virginia requirements)*

# TABLE OF CONTENTS

# 1. Introduction

## 1.1. Intent

The intent of the Data Classification Standard is to establish a baseline for classifying data for agencies across the Commonwealth of Virginia (COV). In accordance with the Code of Virginia, Section 2.2-603.F each Agency Head is responsible for securing the electronic data that is held by the agency and shall comply with the requirements of Code of Virginia, Section 2.2-2009. Agencies that have access to, or handle information that is subject to Federal laws or regulations should ensure compliance with those respective requirements. For example, agencies could be subject to laws and regulations including, but not limited to the following:

Health Insurance Portability and Accountability Act of 1996 (HIPAA);

Internal Revenue Service (IRS) Publication 1075.

Privacy Act of 1974;

Payment Card Industry (PCI) Standard;

Rehabilitation Act of 1973;

508 General Services Administration (GSA) Government-wide IT Accessibility Program;

Criminal Justice Information Services (CJIS);

Social Security Administration (SSA);

Federal Education Rights and Privacy Act of 1974 (FERPA); and

National Institute of Standards and Technology (NIST).

## 1.2 Purpose

The purpose of this Data Classification Standard is to establish a framework for identifying information based on the characteristics of the data. Identifying the type of data ensures that information is handled in a manner that maintains the target risk posture of the organization and complies with legal, regulatory, and business requirements. Using this framework will help users identify what data, documents and other information needs to be restricted.

Data classification and sensitivity classification are two separate steps. Data classification will identify the data type in use and sensitivity is defined based on the impact to confidentiality, integrity, and availability. Keeping the classification items separate provides the ability to identify datasets that when combined may become sensitive.

### 1.3 Scope

This standard applies to all employees, contractors, consultants, and third-party partners who create, manage, store, transmit, or access organizational data. It includes data in all formats (digital, paper, etc.). COV sensitive information is 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. COV agencies are expected to maintain and enforce compliance with requirements for the handling of all data processed through documented agreements with third-party providers and oversight of the services provided.

## 2. Data Classification Criteria

2.1 Data should be classified based on the following criteria:

**Confidentiality Requirements:** Consider the impact of unauthorized access to the data (e.g., loss of competitive advantage, legal penalties).

**Legal/Regulatory Requirements:** Identify whether the data is subject to specific legal or regulatory frameworks (e.g., FTI, HIPAA, PCI-DSS).

**Business Impact:** Evaluate the effect on the organization if the data is lost, compromised, or publicly disclosed (e.g., reputational harm, financial loss).

**Access Needs:** Determine the employees and third parties who need access to the data.

## 3. Data Classification Labels

3.1 Data classification shall be used to identify the authorized use and release of information. Commonwealth data shall be classified using the minimum data classification and additional labels as required to identify regulatory compliance requirements, protected data, sensitivity, or special considerations for labeling and handling data.

**Table 1. Minimum Data Classification Labels**

| Data Classification | Definition | Characteristics | | |
|---|---|---|---|---|
| | | Risk/Impact | Access Control | Information Handling |
| **Public** | Freely available to the general public and can be accessed, shared, and used without restrictions. | Does not pose a risk to individuals or organizations if accessed or disclosed.<br><br>Cannot lead to negative consequences on its own or when combined. | Controls preventing access, processing or obtaining the data are not present. Available through unrestricted channels such as government websites, public databases, or open data portals. | Can be freely shared with the general public and without violating laws or regulations related to data privacy or security |
| **Internal Use Only** | Internal use only data is meant for use within the organization and its approved affiliates. | Unauthorized access would result in reputational damage or internal inefficiencies. | Requires users to authenticate before access.<br><br>Requires monitoring for misuse or unauthorized disclosure. | Data sharing authorization must be documented prior to providing the data to an identified party.<br><br>Data sharing authorization must be documented prior to providing the data to an identified party |
| **Personal** | Information generated or stored by personnel that is not directly related to the Commonwealth's operations. | Disclosure of data included with this classification should not impact the risk posture of the Commonwealth in any way. | Organizations retain the right to access and disclose personal data even if it does not pertain to the business of | Personal data should not be shared with anyone in the organization using Commonwealth systems or data storage. |

| | | | | |
|---|---|---|---|---|
| | NOTE: This data will be accessible and disclosable by the Commonwealth | Any data that does impact the risk posture of the Commonwealth cannot be classified as Personal. | the Commonwealth | |
| **Confidential** | Confidential data is information that should only be accessible to authorized individuals. | Unauthorized access or exposure could lead to significant consequences for the organization, its employees, citizens, or customers.<br><br>Unauthorized disclosure could have moderate to severe adverse effects on the organization.<br><br>Exposure could result in financial penalties, damage to reputation, violation of regulatory terms, violation of the law or potentially result in legal action. | Organization must maintain documentation for roles or users which will have access to data.<br><br>All changes to classification of this data type must be documented and logged. | Access to this data must follow data handling and storage policies.<br><br>Data sharing authorization must be documented prior to providing the data to an identified party<br><br>Technology and mediums used to share data must be authorized prior to providing the data to an identified party.<br><br>Organizations must document authorized locations to store this data. |

**Table 2. Regulatory and Protected Data Labels**

| Protected Data | Definition | References |
|---|---|---|
| **Personally Identifiable Information (PII)** | PII shall include but not be limited to: (i) name; (ii) date of birth; (iii) social security number; (iv) driver's license number; (v) bank account numbers; (vi) credit or debit card numbers; (vii) personal identification numbers (PIN); (viii) electronic identification codes; (ix) automated or electronic | *§ 18.2-186.3 Sub section C* |

| | | |
|---|---|---|
| | signatures; (x) biometric data; (xi) fingerprints; (xii) passwords; or (xiii) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain money, credit, loans, goods, or services. | |
| **Personal Medical Information (PMI)** | Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth: 1.) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or 2.) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. | § 32.1-127.1:05 |
| **Protected Health Information (PHI)** | Individually identifiable health information transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component (HIPAA applies to Covered Components, which are health care providers, health plans, and clearinghouses that engage in certain types of transactions electronically).<br><br>PHI is considered individually identifiable if it contains one or more of the following identifiers:<br><br>Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or<br><br>An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. | https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#what<br><br>The Privacy Rule is located at 45 CFR Part 160, links to an external website and Subparts A and E of Part 164, links to an external website.<br><br>https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html |
| **Family Educational Right** | FERPA is a federal law that affords parents the right to have access to their children's | The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA |

| | | |
|---|---|---|
| **and Privacy Information (FERPA)** | education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). | regulations are found at 34 CFR Part 99.PCI |
| **Federal Tax Information (FTI)** | FTI is defined as any return, return information or taxpayer return information that is entrusted to the commonwealth by the Internal Revenue Services. Federal law provides that all returns and return information are confidential. No current or former employee of the IRS, state or federal agency may access or disclose returns or return information unless specifically authorized under provisions of the Code. A return means any tax or information return, estimated tax declaration or refund claim (including amendments, supplements, supporting schedules, attachments or lists) required by or permitted under the Code and filed with the IRS by, on behalf of, or with respect to any person. | https://www.govinfo.gov/app/details/USCODE-2011-title26/USCODE-2011-title26-subtitleF-chap61-subchapB-sec6103<br><br>https://www.irs.gov/privacy-disclosure/protecting-federal-tax-information-fti-in-integrated-eligibility-systems-ies |
| **Social Security Administration Information (SSA)** | Data subject to the social security administration data exchange agreement. | https://www.ssa.gov/dataexchange/privacyinfo.html<br><br>The foundation for the requirements are the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, the Privacy Act of 1974 and SSA's own policies, procedures and directives. |
| **Payment Card Information (PCI)** | Information printed or stored on a physical card. PCI covers all cardholder data, including Primary account number (PAN), Cardholder's name, Card expiration date, and Security code. | https://www.pcisecuritystandards.org/standards/ |
| **Critical Infrastructure (CI)** | Any information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video that is either vital to the functioning of critical infrastructure of the commonwealth or the United States or so vital that the incapacity or destruction of such systems would have a debilitating impact on commonwealth or national security, economic security, or public health and safety. | |

| | | |
|---|---|---|
| **Law Enforcement Data (LE)** | Information that is essential to the law enforcement mission. This could be any criminal investigative data that may jeopardize an ongoing investigation or prosecution; jeopardize the safety of an individual; or cause a suspect to flee or evade detection. | https://www.fbi.gov/services/cjis |
| **Control System / Supervisory Control and Data Acquisition Data** | Data in systems and networks that monitor, manage, and control automation, production and distribution in industrial environments or equipment used to support physical environments. | https://www.ferc.gov/legal |
| **Intellectual Property** | Data such as inventions, artistic works, designs, symbols, names, and images used in commerce, which are protected by law allowing the owner exclusive rights to the data. | |
| **Legal Privileged Data** | Data that is subject to attorney-client privilege is considered confidential. This includes any written advice of legal counsel to state, regional or local public bodies or the officers or employees of such public bodies, and any other records protected by the attorney-client privilege. In addition, any data that may be considered part of any attorney work product is also confidential. This includes legal memoranda and other work product compiled specifically for use in litigation or for use in an active administrative investigation. | |

## 4. Sensitivity Labels

4.1 Once data is classified with the classification label the data should be evaluated for sensitivity. Data should be classified as sensitive relative to confidentiality, integrity and/or availability. All data identified as sensitive should also apply the appropriate Sensitive Data Label (Table 3).

**Table 3. Sensitivity Labels**

| Sensitivity Area | Definition |
|---|---|
| **Sensitive-Confidential** | Any data that must be protected from access by one or more authorized parties |
| **Sensitive – Integrity** | Any data that must be protected from unauthorized modification |

| | |
|---|---|
| **Sensitive – Availability** | Any data that has a target recovery time objective of 8 hours or less or a recovery point objective of 4 hours or less |

## 5. Special Considerations

5.1 Special conditions may warrant additional data labeling and handling requirements to protect data from unauthorized disclosure, reliability, and availability.

**Table 4. Special Consideration Data**

| **Data Classification** | **Definition** | **Characteristics** | | |
|---|---|---|---|---|
| | | Risk/Impact | Access Control | Information Handling |
| Artificial Intelligence Training Data | AI Training Data refers to any structured or unstructured data identified as permitted for training, validating, or testing artificial intelligence models. This data may include, but is not limited to, text, images, video, sensor data, or any other data type used to develop and refine learning algorithms. | Unintentional data leakage or exposure of data generated from the trained model.<br><br>Creation of bias or inaccuracy from the model due to data that is not suitable for training or learning. | Each AI model or interface to data used for AI must maintain a separate access account per model or AI application. | Prior to usage the agency must document a policy supporting the data is eligible for usage in AI systems and training.<br><br>Data owner must document the approval of usage of the data in the AI system, including understanding once the data is used, they may not be able to remove it from the trained system. |

## 6. Review and Updates

6.1 Data classification should be periodically reviewed and updated based on changes in legal, regulatory, or business needs. Security audits must include verification of compliance for sensitive systems hosting data that has been classified.