Data Classification Policy and Standard

Purpose

This policy establishes a framework for classifying Commonwealth data based on its sensitivity, criticality, and applicable legal or regulatory requirements. The purpose is to ensure data is protected against unauthorized access, disclosure, modification, or destruction, thereby maintaining the Commonwealth's target risk posture, ensuring operational continuity, and complying with all obligations. This framework guides the implementation of appropriate security controls throughout the data lifecycle.

Scope

This policy and standard apply to all Commonwealth Executive Branch agencies, employees, contractors, consultants, and third-party partners who create, access, manage, store, process, transmit, or dispose of Commonwealth data, regardless of format (e.g., digital, paper, verbal) or location (e.g., on-premises, cloud, third-party).

Definitions

Term	Definition
Data Owner	The person or entity responsible for the overall data governance and classification of a dataset, typically a senior leader within the organization.
Data Steward	An individual responsible for managing a dataset and ensuring its quality and metadata accuracy. Data Stewards are typically subject matter experts, middle managers, technical staff, or people in specialized roles like records managers.
Data User	Any individual who interacts with data for analysis, reporting, or operational purposes.
Data Custodian	Typically, IT personnel or business unit staff managing IT systems, Data Custodians are responsible for implementing and managing the security controls specified by this standard and directed by Data Owners/Stewards
ISO	Responsible for overseeing the implementation and enforcement of this policy.
Personally Identifiable Information (PII)	Personal information means the first name or first initial and last name in combination with and linked to any one or more of the

Term	Definition
	following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1) Social security number; 2) Driver's license number or state identification card number issued in lieu of a driver's license number; or 3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;
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 claim history, including any appeals records.
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). PHI is considered individually identifiable if it contains one or more of the following identifiers: • 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 • 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 claim history, including any appeals records.
Family Educational Right and Privacy Information (FERPA)	FERPA is a federal law that affords parents the right to have access to their children's 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"). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99.PCI

Term	Definition
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.
Social Security Administration Information (SSA)	Data subject to the social security administration data exchange agreement.
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.
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.
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.
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.

Roles and Responsibilities

Role	Responsibility
Data Owner	• Assigning an appropriate classification level to data assets, often in consultation with Data Stewards. • Formally appointing Data Stewards for key data domains or assets. • Approving authorized users and access requirements. • Setting the policy for data handling, sharing, and disposal consistent with its classification. • Reviewing classifications periodically (at least annually) or when significant changes occur. • Making final decisions regarding data classification and usage conflicts.
Data Steward	• Understanding the specific data elements, metadata, quality, and business context within their assigned domain. • Recommending appropriate data classification levels to the Data Owner based on data content and usage. • Assisting in defining and documenting data definitions, business rules, and quality standards for their domain. • Collaborating with Data Custodians to ensure security controls align with policy for their specific data assets. • Reviewing access requests for their data domain and providing recommendations to the Data Owner. • Ensuring data handling practices within their domain comply with this policy and other relevant standards.
Data User	• Adhering to this policy and associated handling requirements for all data they access. • Using data only for authorized purposes. • Reporting any suspected policy violations or data security incidents immediately. • Completing mandatory data security and classification training.
Data Custodian	• Implementing technical controls (e.g., access controls, encryption, logging) aligned with the data classification. • Managing data backup and recovery processes according to defined RTO/RPO based on criticality. • Executing data disposal procedures upon authorization. • Monitoring systems for compliance and security events.
ISO	• Providing guidance on data classification and protection. • Ensuring classification aligns with legal, regulatory, and contractual requirements. • Overseeing data security training programs. • Facilitating periodic reviews and updates of this policy.

Role	Responsibility
	• Overseeing security audits which must include verification of compliance for systems hosting classified data.

Policy

- All Commonwealth data must be classified according to the levels defined in this standard.
- Classification levels must be documented in the agency's data inventory.
- Appropriate security controls, corresponding to the assigned classification level, must be implemented and maintained throughout the data lifecycle.
- Data must be classified based on an assessment of the impact of unauthorized disclosure (Confidentiality), unauthorized modification or destruction (Integrity), and disruption of access or use (Availability).

Standard

Data Classification Levels

Data is classified into one of four levels based on an assessment of risk and impact related to its confidentiality, integrity, and availability. The potential impact (Low, Moderate, High) should be assessed for each C-I-A component to determine the overall classification.

> **NOTE:** Regulatory data types (e.g. PHI, FERPA, FTI) must be classified at minimum as Tier 2 (Confidential) and in most cases as Tier 3 (Highly Confidential).

> ***Tip:*** Check out ODGA's Data Classification Tool to help you pick the right classification based on the data you have - Data Classification Tool - Power BI

Level	Description	Examples	Handling
Public/Tier 0 Confidentiality-Low Integrity – Low Availability-Low	Information explicitly approved for public distribution or that must be released under public records laws. Disclosure carries no adverse impact on the Commonwealth, its partners, or individuals.	Public websites, press releases, published reports, job announcements, brochures, publicly released datasets.	*Access:* No restrictions. *Storage:* Store in designated public access locations. *Transmission:* No specific restrictions, but protect against unauthorized modification. *Labeling:* Recommended but not mandatory (e.g., "Public"). *Disposal:* No specific requirements.
Internal/Tier 1 Confidentiality-Low/Moderate Integrity – Moderate	Information intended for internal Commonwealth business use among employees, contractors,	Routine internal memos, non-sensitive operational data, draft documents not yet approved for	*Access:* Requires authentication; access granted based on legitimate business need ("Least Privilege").

Level	Description	Examples	Handling
Availability-Moderate	and authorized partners. Unauthorized disclosure could cause minor operational inefficiencies, reputational harm, or procedural disadvantage but is not expected to violate laws or cause significant harm.	release, internal project documentation, internal procedures, meeting minutes not containing sensitive information.	*Storage:* Store on COV-managed systems with appropriate access controls. Avoid storage on personal devices or unauthorized cloud services. *Transmission:* Use secure methods (e.g., encrypted email, secure file transfer) when transmitting outside the secure COV network. *Labeling:* Must be labeled (e.g., "Internal Use Only"). Digital labeling via metadata tags preferred where feasible. *Disposal:* Dispose of via approved methods (e.g., shredding, secure electronic wipe/destruction).
Confidential/Sensitive/Tier 2 Confidentiality-Moderate/High Integrity – Moderate/High Availability- Moderate/High	Sensitive information protected by law, regulation, contract, or policy, or which, if disclosed or modified without authorization, could cause significant harm to individuals, Commonwealth operations, reputation, or finances. Access is strictly limited to authorized individuals with a documented need-to-know.	• Personally Identifiable Information (PII) not otherwise classified as Restricted. • Protected Health Information (PHI) / Personal Medical Information (PMI). • Student Education Records (FERPA). • Non-public financial data. • Intellectual Property (IP). • Attorney-Client Privileged communications / Legal Work Product. • Pre-decisional policy drafts, sensitive procurement data. • Security vulnerability information. • Law Enforcement data not classified as Restricted. • Governor's Working Papers	*Access:* Requires strong authentication (MFA recommended); access granted based on explicit authorization and strict need-to-know, reviewed periodically. Access logs must be maintained. *Storage:* Store only in approved, secure locations with robust physical and logical access controls. Encryption at rest is mandatory. *Transmission:* Must be encrypted during transmission (both internal and external). Use approved secure transfer mechanisms only. *Sharing:* External sharing requires documented Data Owner approval. *Labeling:* Must be clearly labeled including any regulatory tags (e.g., "Confidential," "Confidential - PII"). Digital labeling via metadata tags is required where feasible. Physical documents require cover sheets and secure handling. *Disposal:* Must be disposed of using approved secure destruction methods (e.g., shredding, degaussing, physical destruction) with verification.

Level	Description	Examples	Handling
Restricted/Highly Confidential/Tier 3 Confidentiality- High Integrity –High Availability- High	Highly sensitive information subject to stringent legal/regulatory protection, where unauthorized disclosure, modification, or loss could result in severe or catastrophic harm, including significant financial loss, legal penalties, risk to public safety or critical infrastructure, or damage to Commonwealth interests. Access is exceptionally limited.	• Federal Tax Information (FTI). • Criminal Justice Information Services (CJIS) data. • Social Security Administration (SSA) data covered by specific agreements. • Payment Card Industry Data Security Standard (PCI-DSS) data. • Critical Infrastructure Information (CI). • Certain Law Enforcement (LE) data jeopardizing investigations or safety. • Control System / SCADA data if compromise could cause severe impact. • Authentication secrets (e.g., private keys, system-level passwords).	*Access:* Requires strongest authentication methods (e.g., MFA); access granted only to specifically named individuals with rigorous vetting and documented justification, audited frequently. Principle of Least Privilege strictly enforced. *Storage:* Store only in highly secured, certified environments with maximum physical and logical controls. Encryption at rest is mandatory, potentially with enhanced key management. Data minimization principles must be applied. *Transmission:* Must be encrypted during transmission with Virtu, or FIPS-compliant technology. Secure, dedicated channels preferred. Prohibit transmission via insecure methods (e.g., standard email). *Sharing:* Extremely limited. Requires explicit Data Owner and potentially legal/ISO approval, strict data sharing agreements, and verification of recipient controls. *Labeling:* Must be clearly labeled including any regulatory tags (e.g., "Restricted," "Restricted - FTI"). Prominent digital and physical labeling required. *Disposal:* Must follow specific regulatory or contractual requirements for secure destruction, often requiring witnessing and certificates of destruction.

Special Considerations

- **Tier 4 Data:** The Commonwealth Data Trust refers to Tier 4 data as “sensitive or proprietary data where the unauthorized disclosure could potentially cause major damage or injury, including death, to entities or individuals identified in the information, or otherwise significantly impair the ability of the Data Trust Member to perform its statutory functions. Tier 4 Data includes any dataset designated by a federal agency at the level “Confidential” or higher under the federal government’s system for marking classified information. No Tier 4

Data shall be knowingly incorporated into the Commonwealth Data Trust" (e.g. lists of gang members, confidential informants, homeland security data).

- **Data Labeling:** Data Owners must ensure data is labeled according to its classification. Where technically feasible, automated metadata tagging should be employed. Physical media containing Confidential or Restricted data must be physically labeled. Emails transmitting Confidential or Restricted data must include the classification in the subject line (e.g., "[CONFIDENTIAL]").
- **Data Aggregation:** When data from multiple sources or classification levels is combined, the resulting dataset must be classified at the highest level of any individual data element within it, unless the aggregation demonstrably removes sensitivity (e.g., anonymized statistical summaries, requiring Data Owner approval for reclassification).
- **Personal Use and Data:** Commonwealth IT resources are provided for official business. Incidental personal use must not interfere with work duties, consume significant resources, or violate any laws or policies. Users have no expectation of privacy for any data, including personal data, stored or transmitted on Commonwealth systems. Refer to VITA'S acceptable Use Policy for more information.
- **Artificial Intelligence (AI) Training Data:** Data intended for use in training AI models must be classified according to this standard based on its inherent sensitivity.
    - Using Confidential (Level 3) or Restricted (Level 4) data requires explicit, documented Data Owner approval, which must assess risks of bias, data leakage from the model, and security vulnerabilities. The approval must document understanding that data removal from a trained model may be impossible.
    - Prior to usage the agency must document a policy supporting the data is eligible for usage in AI systems and training
    - Access controls for AI models and data interfaces must be strictly managed. Public data (Level 1) is generally preferred unless higher-level data is essential and appropriately protected/anonymized.

Compliance and Monitoring

- Compliance with this policy is mandatory.
- Violations may result in disciplinary action, up to and including termination for employees, and contract termination or legal action for contractors and third parties.
- Exceptions to handling requirements must be documented and approved by the CISO.
- Agencies must implement processes to monitor compliance including automated scanning.
- Security audits must include verification of compliance for sensitive systems hosting data that has been classified.
- Suspected violations or data security incidents must be reported immediately by following the agency's incident response policy and procedure.

Training and Support

- All employees must complete basic data classification training annually.
- Data owners and stewards must complete advanced classification training.
- IT staff must complete technical security training related to protecting classified data.
- Training completion must be documented.

Policy Review

Data classification should be reviewed annually and updated based on changes in legal, regulatory, or business needs.

Related Policies

Policies, Standards and Procedures
SEC530_Information_Security_Standard.pdf
Information Resource Acceptable Use Policy - October 2024
SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and
SP 800-60 Rev. 2, Guide for Mapping Types of Information and Systems to Security
NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable
FIPS 199, Standards for Security Categorization of Federal Information and Information

Version History

Version Number	Revision Date	Description of Change	Author
V1	4/25/2025	Initial Draft	Chris Burroughs