Office of Security Management

DATA CLASSIFICATION POLICY

Version Number: 1.1

Date Issued: 10/01/2024

Date Last Revised: 2/21/2025

Table of Contents

Revision Control History

Version	Author(s)	Date	Description
1.0	Gregory S. Rogers	October 11, 2024	Initial Version
1.0	Gregory S. Rogers	December 12, 2024	Final Version
1.1	Jason Silva	February 21, 2025	Minor Revision

Approval

Jason Silva 2/21/2025

Jason Silva — Date
Acting State Chief Information Security Officer

1. Purpose

This policy establishes standards of information classification, providing a framework outlining security levels that promotes effective management and oversight of data to protect against unauthorized access and use. The State's policy is to be transparent in enabling the public to access public information while at the same time protecting individuals' rights to data privacy and the State's interest in maintaining the confidentiality of highly sensitive or confidential information.

This policy forms the basis from which Maryland Executive Branch agencies create procedures to protect the confidentiality, integrity and availability (CIA) of data by considering data content, data context, regulatory requirements, and risk level to stakeholders (public, individuals, agencies). Risk of harm to individuals who authorize the use of their "personal information" for a specific purpose is a key factor when determining data classification. Risk of harm to the agency and the State, be it financial, reputational, or social welfare, is considered as well. Data classification informs the level of security to be applied to a system to protect against unauthorized access to the data. Data classification should inform the data user on how to protect that data.

Agencies are responsible for adhering to this Data Classification Policy and the application of appropriate handling requirements to ensure data is used and protected in accordance with its data classification.

2. Scope

This policy applies to all data, whether in electronic or non-electronic formats, collected, created or processed by All Executive Agencies. This policy applies to all State Executive Branch Agency data owners, employees, contractors, processors, and data users granted authorized access to State data and information systems. Information security personnel use data classification levels to provide the appropriate system security level.

This policy is subject to applicable law. In the event of a conflict between the provisions of this policy and applicable law, including, without limitation, Md.

Code Ann., Gen. Provisions Article, Title 4 (Public Information Act), the provisions of applicable law shall control.

3. Authority

Md. State Finance and Procurement Code Ann, 3.5-2A-04(b)(1)

Md. State Finance and Procurement Code Ann, 3.5-303

4. Policy

Data classification aids in the proper management and security of data in use, in transit, and at rest. This Data Classification Policy establishes a baseline against which to assess the responsibilities for CIA (Appendix B Table 1), and legal requirements to ensure the appropriate designation for data accessibility and protection. Data creators/generators and owners are responsible for appropriate classification of their data, while data users are responsible for following data protection guidelines for each data classification.

While data may be provided security levels above the data's classification, data should not have security levels below its classification. Assigning higher data protection levels than necessary may impact data protection resource requirements and lessen transparency and needed access.

This Policy categorizes data into four (4) levels of classifications, as follows:

- Public
- Protected/Internal Use Only
- Confidential
- Restricted

Level 1 - Public

Public data is data that a State entity has collected or created and is permitted, required or able to make available to the public consistent with applicable laws, rules and regulations.

Correctly classifying data as Public is the most effective way to deliver government transparency and accountability and maximize access to authoritative, reliable and current data.

Level 2 - Protected/Internal Use Only

Data within this classification is accessible to Agency personnel or contractors who require access, and require protection from unauthorized use, disclosure, modification, or destruction. For example, draft versions of statistical or factual information that are used for internal analysis by a governmental entity do not constitute “open data” under the Open Data Act and should be classified as “Protected/Internal Use Only.” Storage of Protected/Internal Only information should be protected via physical and logical access controls to ensure authorized staff can easily access the data and maintain a level of control such that unauthorized individuals cannot easily access the data.

Level 3 - Confidential

The sensitive nature of some data requires that it be treated as confidential. Confidential information is information that is protected from either release or disclosure by law. Confidential information includes but is not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), credit card and financial information, student records, information about children, and other privileged or sensitive information. Confidential information must be kept confidential and requires individual consent, de-identification or anonymization, a public health mandate, or other requirement of law prior to being released. Confidential data should be accessible to authorized users only, remain encrypted at rest and in transit, and used for only those purposes for which it was collected or for which an individual consented.

Level 4 - Restricted

Restricted is data that, if disclosed, accessed, altered or destroyed without authorization, could cause significant damage to the Agency, e.g., financial loss, damage to the Agency’s or the State’s reputation, or the individual(s) whose information is compromised, and may lead to criminal charges or other legal consequences.

Statutes, regulations, other legal obligations or mandates protect much of this information. Federal and/or state laws or regulations mandate specific, restrictive, administrative, technical and physical controls be in place throughout the restricted information's lifecycle. Disclosure of restricted data is limited to only those individuals who meet and maintain the legal criteria to be authorized to access the restricted data for only those purposes allowable by regulation, law or policy.

Examples of restricted data include Federal Tax Information (FTI), Criminal Justice Information maintained by law enforcement and Non-Criminal Justice Information maintained by Non-Criminal Justice Agencies with legal authority to utilize CJIS data. Restricted information should be accessible to only authorized users who meet the regulatory requirements to access the information, remain encrypted at rest and in transit, and used for only those purposes for which an individual consented or a governing authority allows.

Where there is no clear system to assign the proper classification to a particular dataset, the impact as described in Table 1 below can lend to assigning the appropriate level of protection.

Table 1: Data Classification Quick Reference Table

Data Class	Description	Examples
Level 1 Public	Information that can be or currently is released to the public. It does not need protection from unauthorized disclosure.	The original or copy of any documentary material in any form, including written materials, books, photographs, photocopies, films, microfilms, records, tapes, computerized records, maps, and drawings created or received by the agency in connection with the transaction of public business. Data collected and permitted, required, or able to be made available to the public in a machine-readable format. Includes recordings of public meetings, public websites, press releases, job

		announcements, public reports, and procurement related information.
Level 2 Protected/ Internal-Only	Information that may not be specifically protected from disclosure by law, is generally for official use only and is not released to the public unless specifically requested and permissible. Does not include confidential information. Protected/Internal data could be potentially harmful were unauthorized people to access it**.**	Draft versions of statistical or factual information reserved for internal analysis, draft reports and memos, internal project documents, learning management data, budget documentation, minutes or recordings of departmental or inter-departmental meetings, unreleased press releases, unpublished marketing materials, and competitive analysis.
Level 3 Confidential	Data subject to protection by law or regulation and access to which requires specific authorization. Includes personal information and sensitive data. The data is subject to protection from disclosure.	Personnel records, sensitive, but unclassified data, financial records, student records, health records, non-critical infrastructure information, non-critical network information, and customer transaction account data. Includes data such as Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Information (PCI), Family Educational Rights and Privacy Act (FERPA), Substance Use Disorder (SUD), children's information, and Privileged or Sensitive.
Level 4 Restricted	Information that is specifically protected from disclosure by law. Unauthorized disclosure of data could cause irreparable damage to the Agency and/or the State and may lead to criminal charges and/or other legal consequences . If released could endanger the public health, safety, or welfare, hinder the operation of government, impose an undue financial, operational, or administrative burden on a State entity, and disclose proprietary or confidential information.	Criminal justice information (CJI or CJIS), Non-criminal Justice Information NCJI), federal tax information (FTI), law enforcement sensitive data, legally privileged data, critical infrastructure information, critical network information, information about security vulnerabilities and risk, cybersecurity assessments and findings, cybersecurity audits, and physical security access logs.

5. Policy Roles and Responsibilities

Each individual with authorized access to protected/internal only, confidential, and/or restricted information is accountable to protect the data from unauthorized use and disclosure. Data governance and privacy mechanisms delineate the appropriate disclosure, processing, and analysis of data.

Data Owner: An individual or entity that is responsible for a particular data asset or for a group of data assets at the Agency and has approval authority for decisions about the data asset(s). A data owner is an individual or entity responsible to appropriately classify data.

Data Steward: A data steward is an individual or entity who is responsible for safeguarding data based on the labeled classification.

Data User: A data user is an individual or entity who is responsible for complying with the data use requirements associated with the labeled classification. The user is accountable to protect the data by ensuring only those who require and have been authorized to access the data as part of their job function have access to the data, use reasonable security controls, and, with the exception of open/public data, ensure only that data which is necessary to fulfill a valid request is provided. Data users need to understand that various data elements alone may not constitute personal information; but the combination of disparate data elements may create “personally identifiable information” such that the combined data is subject to a higher data classification level.

6. References and Maintenance

The State Chief Information Security Officer maintains and reviews this policy annually and on an ad hoc basis in response to changes in security and privacy related laws and regulations. The following regulations, recommendations, and standards impact the data classification policy:

42 CFR Part 2 - Confidentiality of Substance Use Disorder Patient Records

Health Information Protection and Portability Act (HIPAA) Privacy Rule: 45 CFR Part 160 and Subparts A and E of Part 164.

Internal Revenue Service Publication 1075 - Tax Information Security Guidelines (2021)

US Department of Justice: Criminal Justice Information System (CJIS) Security Policy, v.5.9.4

Maryland General Provisions - Title 4 - Public Information Act (PIA)

Md. State Finance and Procurement Code Ann, 3.5-2A-04(b)(1)

Maryland State Government, Title 10, Subtitle 13 Protection of Information in Government Agencies (MD PIGA)

Maryland State Government, Title 10, Subtitle 15 Open Data

NIST 800-53 v5, AC-11

APPENDIX A. Definitions & Acronyms

All defined terms below should be capitalized within the document and defined below.

Acronym/Phrase	Definition
Authorized User/Personnel - CJI	Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI. Source: CJIS Security Policy, v.5.9.4
Business Associate	A person who: (i) On behalf of a "covered entity" or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information, including claims processing or administration, data analysis, processing, administration, or utilization. Business associate does not include: A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
Covered Entity	A health plan, health care clearinghouses, and any health care provider who transmits health information in electronic form.
Criminal History Record Information (CHRI)	Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system. Source: CJIS Security Policy, v.5.9.4
Criminal Justice Information (CJI)	Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their

	mission; including, but not limited to data used to make hiring decisions. The following types of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII. Source: CJIS Security Policy, v.5.9.4
Federal Tax Information (FTI)	FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source such as the Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS) or Centers for Medicare and Medicaid Services (CMS) or another entity acting on behalf of the IRS pursuant to an IRC § 6103(p)(2)(B) Agreement. FTI includes any information created by the recipient (Agency) that is derived from federal return or return information that is received from the IRS or obtained through a secondary source. In addition to "personal information" as defined below, FTI also includes taxpayer mailing address, taxpayer identification number, telephone numbers, date and place of birth, and mother's maiden name, or a combination of any personal information. (Source: Publication 1075, 2021)
Individually identifiable health Information	Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Noncriminal Justice Agency (NCJA)	A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances. Source: CJIS Security Policy, v.5.9.4
Open Data	Data that, consistent with any applicable laws, rules, regulations, ordinances, resolutions, policies of other restrictions including requirements or rights associated with the data, a State entity has collected, and is permitted, required, or able to make available to the public.
Personally Identifiable Information	Means any information that, taken alone or in combination with other information, enables the identification of an individual, including:

	(i) a full name; (ii) a Social Security number; (iii) a driver's license number, state identification card number, or other individual identification number; (iv) a passport number; (v) biometric information including an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity; (vi) geolocation data; (vii) Internet or other electronic network activity information, including browsing history, search history, and information regarding an individual's interaction with an Internet website, application, or advertisement; and (viii) a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account. (2) "Personally identifiable information" does not include data rendered anonymous through the use of techniques, including obfuscation, delegation and redaction, and encryption, so that the individual is no longer identifiable. (Source: MD State Govt 10-13A-01)
Process	Means any operation or set of operations that is performed on personally identifiable information or on a set of personally identifiable information, whether or not by automated means, including collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. (Source: MD State Govt 10-13A-01)
Processor	Means an entity that processes personally identifiable information.

	Means individually identifiable health information that is transmitted and maintained by electronic or any other form of medium. The eighteen identifiers include names; all geographical subdivisions smaller than a State all elements of dates (except year) for dates directly related to an individual; phone numbers; fax numbers; electronic mail addresses; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); internet protocol (IP) address numbers; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code (except unique codes assigned by the investigator to code the data). PHI excludes individually identifiable health information that is not related to healthcare treatment, payment or operations, such as student records under Family Educational Rights and Privacy Act or employment records held by a covered entity in its role as employer. Source: Privacy Rule,45 CFR Part 160 and Subparts A and E of Part 164. .
Person In Interest (aka Data Subject)	Person in interest means a person, the person's designee, the parent or legal representative of a person with a legal disability, or governmental unit that is the subject of a public record. Source: MD PIGA
Public Record	A Public Record is defined as the original or copy of any documentary material in any form, including written materials, books, photographs, photocopies, films, microfilms, records, tapes, computerized records, maps, and drawings created or received by the department in connection with the transaction of public business. Source: (MD General Provisions, Title 4, Public Information Act)
Sensitive information	A subset of "Personal information" that includes data revealing racial or ethnic origin, religious beliefs, consumer health data, sex life, sexual orientation, status as transgender or nonbinary, national origin, or citizenship or immigration status, genetic data or biometric data, substance abuse, personal

	data of an individual that the data owner/controller knows or has reason to know is a child (under 18 years of age), or precise geolocation.
Substance Use Disorder Patient Records	42 CFR Part 2 imposes restrictions upon the use and disclosure of substance use disorder (SUD) patient records which are maintained in connection with the performance of any Part 2 program. The regulation provides for limited exceptions for the disclosure of these records.

APPENDIX B Table 1. Data Security Objectives

Security Objective	FISMA Definition [44 U.S.C., Sec. 3542)	FIPS 199 Definition
Confidentiality	"Preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of **confidentiality** is the unauthorized disclosure of information.
Integrity	Avoid "improper information modification or destruction, and include ensuring information nonrepudiation and authenticity…"	A loss of **integrity** is the unauthorized modification or destruction of information.
Availability	"Ensure timely and reliable access to and use of information…"	A loss of **availability** is the disruption of access to or use of information or an information system.

Table 2: Data Security Impacts

Security Objective	Low Impact	Moderate Impact	High Impact
Confidentiality	Unauthorized access of data could be expected to have a **limited** adverse effect on the Agencies' operations, assets, or employees.	Unauthorized access of data could be expected to have a **serious** adverse effect on the Agencies' operations, assets, or employees.	Unauthorized access of data could be expected to have a **severe or catastrophic** adverse effect on the Agencies' operations, assets, or employees.
Integrity	Unauthorized modification or destruction of data could be expected to have a **limited** adverse effect on the Agencies' operations, assets, or employees.	Unauthorized modification or destruction of data could be expected to have a **serious** adverse effect on the Agencies' operations, assets, or employees.	Unauthorized modification or destruction of data could be expected to have a **severe or catastrophic** adverse effect on the Agencies' operations, assets, or employees.
Availability	Disruption of access to or use of information could be expected to have a **limited** adverse effect on the Agencies' operations, assets, or employees.	Disruption of access to or use of information could be expected to have a **serious** adverse effect on the Agencies' operations, assets, or employees.	Disruption of access to or use of information could be expected to have a **severe or catastrophic** adverse effect on the Agencies' operations, assets, or employees.