Division of Enterprise Technology Strategy and Services

Data, Analytics, and AI Center of Excellence

Data Classification Guideline 400.1G

Scott Gausland, Chief Data and Analytics Officer (CDAO)

Brian Tardiff, Chief Digital Officer (CDO)

2026

This guideline is distributed by the Division of Enterprise Technology Strategy and Services (ETSS) to inform our supported Agency and employee communities of best practices for classification of data under their control using the classification tools provided by ETSS. This advisory is not policy, rather it is intended to provide direction for agencies and employees on how to implement best practices in classifying data in a manner that complies with state and federal guidelines for data protection and privacy and will also enhance data sharing, analytics, and AI opportunities when practiced.

Information and data protection is the responsibility of all employees that have access. This is true for structured and unstructured data, stored within, or external to State of R.I. information systems. Traditional controls applied for information protection have included (among others) cover sheets, watermarks, footnotes, encryption, secure file transfers, and file and folder permissions and restrictions (least privilege). The nature of how data is leveraged in modern business operations and shared within and across technology platforms and users requires continuous enhancement to how we protect that data from unintentional access, leakage, and breaches.

As a foundation for all methods to protect data, we need a standardized understanding of how to classify data sensitivity. This understanding provides for scalable controls and methodologies to be applied to make the process of protecting and sharing data achievable at the user level, where the greatest risk to data resides. The classification of State data helps to ensure that adequate controls are in place to protect the confidentiality, integrity, and availability of the data. It is critical that data is adequately protected from individuals with malicious intent, that privacy rights are maintained, and that federal and state regulations and compliance requirements are followed to reduce the risk associated with unauthorized access or loss of privacy and/or confidentiality that may result in financial losses and criminal or civil penalties. State data remain attractive targets for cybercriminals, so protecting this data and maintaining public trust is critically important.

This guideline is to assist all State of Rhode Island Executive Branch Departments (including agencies, boards, and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state Network Resources, whether operated or maintained by the state or on behalf of the state. For this guideline, the term "Agency" is used to refer to any department, Agency, division, or unit of the Executive Branch of the State of Rhode Island that has state data under its control or as a component of its business operating model.

Key Definitions

Authentication: The process of determining whether the person or entity that is attempting to access a computing system really is who they claim to be. Authentication systems make a binary decision: they allow or deny access based on credentials or other proof provided by those requesting access. To have been "authenticated" means that the identity of a user has been verified before granting access to the system.

Authenticators: Data that is used to verify the identity of a user, service, or process. Examples include passwords, token codes, public key certificates, etc.

CIA: A core principle in IT and Data Systems risk management and security control decision making. A balance of these three must be achieved, with more weight applied to controls commensurate with the classification of the Data or System.

(C) Confidentiality: Protecting data from unauthorized access or disclosure to maintain the privacy of personal or proprietary data in accordance with all relevant state or federal laws and policies. For any Non-Public Classified Data, enforce access restrictions and encryption as dictated by the applied label.

(I) Integrity: Protecting data from unauthorized modification or destruction to maintain the authenticity and non-repudiation of the data. If content drives decisions or is subject to regulatory reporting, use labels that restrict editing, require change tracking, and preserve authenticity (a key consideration for unstructured data and AI use cases).

(A) Availability: Ensuring timely and reliable access to and use of data. For Public content, emphasize integrity and tamper protection; confidentiality controls are implemented at lowest level required to achieve policy compliance.

Data Container: An email, chat, file, document, table, database, report, dashboard, or transcript that contains one or more points of data, that taken as a whole, determines which data sensitivity label needs to be applied.

Data Custodian: A role responsible for the safe custody, transport, and storage of data, ensuring data is accessible and secure, and implementing business rules related to data management. Data custodians focus on the technical aspects of data management such as programming, hosting and transport infrastructure and security.

Data Steward: An individual or group responsible for overseeing and ensuring the quality, integrity, and effective use of an Agency's data assets, acting as a bridge between the technical and business teams. Data stewards focus on data quality and business rules.

Data Owner: An individual or group within an Agency that holds ultimate responsibility for a specific dataset, overseeing its accuracy, integrity, usage, and protection throughout its lifecycle, essentially having the authority to make critical decisions regarding the collection, storage, and sharing of that data.

Data Sensitivity Label: Data Sensitivity Labels are digital tags that classify and protect the State's data based on its sensitivity level. Once applied, the label travels with the Data Container wherever it goes, enforcing protection policies automatically. Data Sensitivity Labels that are available in Microsoft Purview are as follows:

Public: Default label. Data or work products contain no Non-Public Classified Data.

Private: Data requiring elevated security control, access and restrictions: Internal use only.

Sensitive:

PII: Personally Identifiable Information. This includes any information about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

FERPA: Family Educational Rights and Privacy Act protected information. Student education records that can be linked to a specific individual.

PCI DSS: Payment card and industry data. Cardholder data and sensitive authentication data are considered account data and are defined as follows: Primary Account Number (PAN), Cardholder name, Expiration Date, Service Code, Full track data (magnetic stripe or chip data), card verification code, PINs/PIN Blocks.

Working Confidential: Any information to be safeguarded, protected, and shared on a need-to-know basis. Historically marked with Confidential Working Draft RIGL §38-2-2(4)(E),(K)

Confidential:

PHI: Protected Health Information. Information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

CUI: Controlled Unclassified Information is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified.

CJIS: Criminal Justice Information Services (CJIS) is the term used to refer to all the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

SSA: SSA (Social Security Information) Information collected and provided by the Social Security Administration. This data includes details about people's wages, identifying information, employers, addresses, and more. It encompasses various types of information such as names, Social Security numbers, addresses, wages, benefits, and disabilities.

FTI: Federal Tax Information (FTI) Any return or return information received from the IRS or any secondary source which is protected by the confidentiality provisions of Internal Revenue Code section 6103.

Non-Public Classified Data: Any data that is not public (including private, sensitive, or confidential data as defined by associated federal regulations and denoted by ETSS data classification labels). Non-Public Classified Data requires additional security controls, such as access restrictions and encryption.

Microsoft Purview: A set of tools that help organizations classify, protect, and govern their data so it is handled consistently and securely across emails, documents, files, and other digital content. It provides a unified way to classify data, manage risks associated with unauthorized access and support responsible use of AI and collaboration tools. The sensitivity labeling feature built into Microsoft 365 apps (such as Outlook, Word, PowerPoint, Excel, and File Explorer) allows users to apply data sensitivity labels that protect and govern how files and emails can be accessed, used, or shared.

Potential Impact: The loss of confidentiality, integrity, or availability of data that is expected from severe, moderate, or limited adverse impacts on Agency operations, assets, or personnel. For example, the degradation of mission critical capabilities or primary Agency functions, damage to Agency assets, life-threatening injuries to personnel, or financial losses.

State Data: Data that is collected, stored, and managed by an Agency. This includes, but is not limited to, personally identifiable information such as Social Security numbers, driver's license information, and tax and financial information.

System Owners: The entity or individual responsible for the entire lifecycle of a State information system, including activities such as its procurement, development, integration, modification, operation, maintenance, and eventual disposal, ensuring it aligns with business needs, and complies with security standards; System Owners hold the highest level of accountability for a system within an Agency.

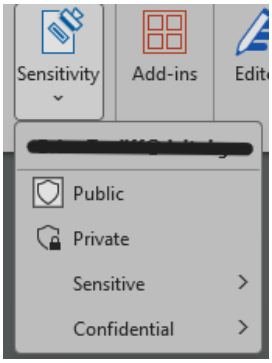
Data Classification Categories

All data under Agency control should be assigned a data sensitivity label in one of the following categories (**Public, Private, Sensitive, Confidential**) in accordance with the potential impact to Agency operations, assets, or personnel resulting from a loss of confidentiality, integrity, or availability. Potential impact assessments should focus on areas of risk most relevant to the Agency and its specific business mission, operational needs, and compliance requirements, as well as risks that may potentially impact multiple State agencies. These classifications of data pertain to how they are organized and packaged together for labeling. Agencies should standardize and document data sensitivity labeling requirements for Agency specific forms, records, and data in accordance with the provisions of this guidance.

- **Public Data** is data requiring a low level of security controls, protection, and access restrictions to maintain its integrity and availability. Because Public Data has no access restrictions and may be viewed by anyone, care must be taken prior to assigning this classification. The greatest threat to Public Data is the unauthorized or unintentional alteration or destruction of the data. Examples include press releases, de-identified data, data made available on public-facing websites, and general marketing materials.

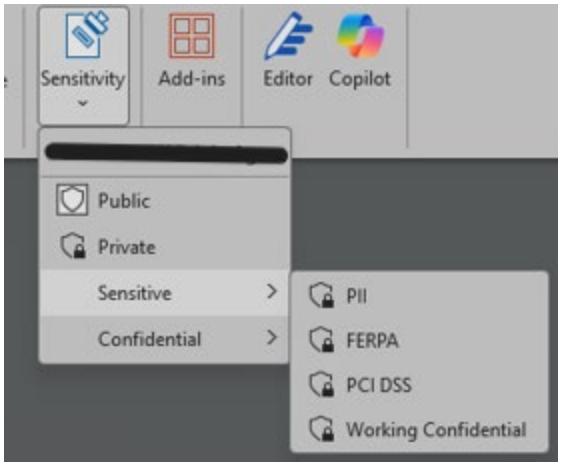
Our Microsoft 365 applications are configured to apply the "Public" data sensitivity label as the default; all content will display with the "Public" label and will remain as such until you choose a different data sensitivity label.

- **Private Data** is data requiring a reasonable level of security controls, protection, and access restrictions to maintain its integrity and availability. Access is restricted to authorized and authenticated individuals who require access to perform their duties. Private data may be thought of as internal-only data and is generally considered to have a moderate impact on the State if compromised. Examples include internal policies and procedures, internal budgets, and business strategies



Purview Sensitivity dropdown

- **Sensitive Data** is data requiring a high level of security controls, protection, and access restrictions to maintain its integrity and availability. Access is restricted to authorized and authenticated individuals who require access to perform their duties. Sensitive Data may be regulated by federal or state laws, regulations, statutes, or internal business workflow requirements, but do not have prescribed security controls that the System Owner must enforce. However, Sensitive Data do require the use of encryption when at rest and during transmission. Unauthorized access or disclosure may result in financial loss, identity theft, and is generally considered to have a high impact on the State if compromised.

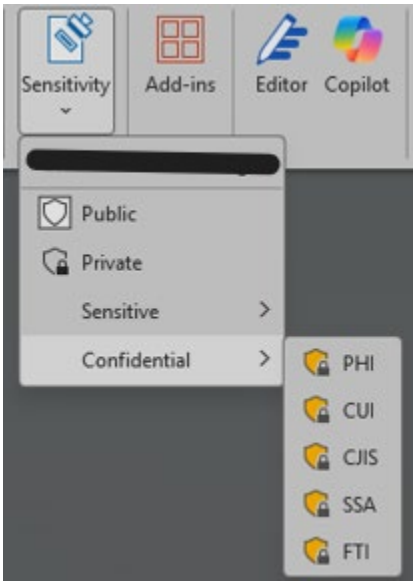


Purview Sensitivity dropdown with “Sensitive” sub-labels

Examples include attorney files and attorney-client communications (Working Confidential), authenticators (e.g. password, PIN), Social Security numbers, credit card numbers, license numbers and associated data, and driver history records, Personally Identifiable Information (PII), Payment Card Information (PCI), IT security data (e.g. configurations, logs, Business Continuity Plans, Disaster Recovery Plans), personnel records, payroll data, Federal Educational Rights and Privacy Act (FERPA) data, data regulated by Federal Information Security Management Act (FISMA) and other regulated data. *See Appendix A for more information regarding Sensitive Data types*.

- **Confidential Data** is data requiring the highest level of security controls, protection, and access restrictions to maintain confidentiality. Access is strictly controlled and restricted to select and authenticated individuals. Confidential Data will be encrypted when at rest and during transmission. Unauthorized loss or disclosure of confidential data poses a serious risk or threat to the State or the individual it references, may be a violation of federal or state law, regulation, or privacy statute, and may result in critical financial, health, or safety repercussions. Confidential Data have prescribed security controls that the System Owner must enforce.

  Examples include state law investigative records, banking, demographic or household information contained in customer/taxpayer files or applications, Protected Health Information (PHI), Health Insurance Portability and Accountability Act (HIPAA) data and Section 1411(g) of the Patient Protection and Affordable Care Act (ACA), National Directory of New Hires (HDNH) data, Controlled Unclassified Information (CUI), Criminal Justice Information Services (CJIS) data, Federal Tax Information (FTI), and Social Security Administration (SSA) data. Data covered by the Identity Theft Protection Act of 2015 (RIGL Chapter 11-49.3) is also considered Confidential Data. *See Appendix A for more information regarding confidential data types.*



Purview Sensitivity dropdown with “Confidential” sub-labels

Data Sensitivity Labeling Quick Tips for Users

- **DEFAULT LABEL:** Data / Content is approved for public release (press, website, de-identified datasets) → Public.
- Internal-only data / content without regulated elements (memos, plans, non-public strategy) → Private.
- Data / Content contains regulated personal/education/payment data (PII, FERPA, PCI) or "Confidential Working" drafts → Apply Sensitive sub-label (e.g., Sensitive//PII, //FERPA, //PCI, //Working Confidential).
- Data / Content contains PHI, CJIS, SSA, FTI, or CUI → Apply Confidential sub-label (e.g., Confidential//PHI, //CJIS, //SSA, //FTI, //CUI).
- Note: Downgrading any label requires justification; enforcement updates immediately.

Agency Data Classification Category Determination Process

The following guidance is provided to Agencies with data that does not have predefined Federal or State classification. For the Agency to determine the appropriate classification category for data or data element requires assessing the potential impact on the State should confidentiality, integrity, or availability (CIA) of the data be compromised. The determination process has four (4) steps:

Step 1. Assess the severity level that a potential impact would have on each CIA security objective, or the pre-defined, regulatory classification requirement.

Step 2. Assess the total potential impact based on all the assessed severity levels.

Step 3. Determine the classification of the data based on assessed total potential impact.

Step 4. Apply Sensitivity Label at the determined level of classification using ETSS authorized tools, document footers or watermarks.

The process can often be based on Federal and State regulations and compliance requirements that mandate specific security controls to be implemented to protect data. However, this is not always the case and, sometimes, determining the appropriate data classification category is not so obvious or easily assessed. To reduce subjectivity, this guideline has been documented to provide a method to provide structure and consistency. Although it is not possible to consider every possible impact scenario, this guideline should provide sufficient guidance for Data Owners to appropriately classify their data. Assigning data Ownership is an important part of the data classification process. Data Owners have a vested interest in maintaining the security of the data and an understanding of the value of the data to the Agency. In general, Data Owner responsibilities include:

- Ensuring all data under their control is classified.
- Determining data access rulesets based on the principles of separation of duties and least privilege.
- Define and document Agency classification standards for common work products (classification catalog).
- Defining data use, security, encryption, retention, and disposal requirements.

- Maintain currency with federal and State regulations and regulatory compliance requirements that effect data under their control.

Data Owners are typically department heads or other individuals within the Agency senior management structure. Information system administrators and other IT staff are not Agency Data Owners; with exception of ETSS specific data. The ETSS technical staff serve as Data Custodians that perform such tasks as granting access to the data (based on data owner's access requirements), maintaining databases, auditing security controls, and performing data backups. Data Owners are expected to work with information system administrators to ensure that appropriate technical security controls are implemented to protect confidentiality, integrity, and availability of data.

The "Security Objectives" and "Severity" tables below provide descriptions of some of the terms used in the data classification process and should be referenced as required.

Security Objectives		
Objective	**Description**	**Loss**
Confidentiality	Preserving authorized data access and data disclosure restrictions. Protecting individual privacy and proprietary data.	A loss of confidentiality is unauthorized access or disclosure of data.
Integrity	Protecting against improper modification or destruction of data. Ensuring non-repudiation and authenticity of data.	A loss of integrity is the unauthorized modification or destruction of data.
Availability	Ensuring the timely and reliable access to and use of data or information system.	A loss of availability is the disruption of access to or use of data or information system.

Severity	
Level	**Description**
Low	The potential impact of a loss of CIA is minor. For example, minor degradation in mission capability (ability to perform one or more primary functions is somewhat reduced), minor damage to Agency assets, minor financial loss, or minor harm to individuals.
Medium	The potential impact of a loss of CIA is moderate. For example, moderate degradation in mission capability (ability to perform one or more primary functions is moderately reduced), moderate damage to Agency assets, moderate financial loss, or moderate harm to individuals (not life-threatening injuries).
High	The potential impact of the loss of CIA is severe. For example, severe degradation in mission capability (cannot perform one or more primary functions), severe damage to Agency assets, severe financial loss, or severe harm to individuals (loss of life- or life-threatening injuries).

Process for Determining and Applying Classification

Step 1. Assess the severity level that a potential impact would have on each CIA security objective, or the pre-defined, regulatory classification requirement.

Severity Level			
Objective	**Low**	**Medium**	**High**
Confidentiality	Unauthorized access or disclosure of data has a minimal impact. Data may be accessed by and disclosed to anyone at any time (public data).	Unauthorized access or disclosure of data has a moderate impact. Data should not be accessed or disclosed to unauthorized users (private/sensitive data).	Unauthorized access or disclosure of data has a severe impact. Data must not be accessed or disclosed to any unauthorized users at any time (confidential data).
Integrity	Unauthorized modification or destruction of data has a minimal impact. Data can be extensively corrupted.	Unauthorized modification or destruction of data has a moderate impact. Data can be slightly corrupted.	Unauthorized modification or destruction of data has a severe impact. Data cannot be corrupted (any loss of integrity has big impact).
Availability	Disruption of access to or use of data has a minimal impact. Data can be unavailable for more than one (1) week.	Disruption of access to or use of data has a moderate impact. Data can be unavailable for up to one (1) week.	Disruption of access to or use of data has a severe impact. Data must always be available (any unavailability is critical).

Some losses have a greater potential impact than others. After considering the possible impact and consequences due to a loss of CIA, determine the most appropriate severity level (low, medium, high) for each security objective (CIA). The "Severity Level" table above provides a general description of security level requirements for each severity objective. For example, after careful consideration of the impact of a loss of CIA for a particular piece of data, it is determined that the most appropriate severity levels due to a loss of confidentiality are low, due to a loss of integrity is low, and due to a loss of availability is high.

Step 2. Assess the total potential impact based on all the assessed severity levels.

The overall potential impact is determined by the highest severity level across CIA. For example, if confidentiality is low, integrity is low, and availability is high, then the total potential impact will be high.

Generally, data classifications are directly related to the potential impact assessment. The higher the potential impact, the more restrictive the assigned data category should be. For example, if the total potential impact is assessed as "high", then the data should be classified as sensitive data (in this example, the data would have a "Sensitive" sub label applied for classification and not a "Confidential" sub label because the assessed confidentiality severity level, from step 1, was "low").

Step 3. Determine the classification of the data based on assessed total potential impact.

Data Categories		
Classification	**Potential Impact**	**Requirements**
Public Data	**Low**	Data requires a low level of security controls, protection, and access restrictions to maintain its integrity and availability. Data has no access restrictions and may be accessed by anyone.
Private Data	**Medium**	Data requires a reasonable (moderate) level of security controls, protection, and access restrictions to maintain its integrity and availability. Access is restricted to authorized and authenticated individuals. Maintaining confidentiality is important, but the data itself is not confidential.
Sensitive Data	**High**	Data assessed with an integrity or availability severity level of "high". Data requires the highest level of security controls, protection, and access restrictions to maintain its integrity and availability. Access is restricted to authorized and authenticated individuals. Maintaining confidentiality is important, but the data itself is not confidential.
Confidential Data	**High**	Data assessed with a confidentiality severity level of "high". Data will be encrypted to maintain its confidentiality. Data requires the highest level of security controls, protection, and access restrictions to maintain its integrity and availability. Access is restricted to authorized and authenticated individuals.

There are many variables and factors that influence the data classification process, but that cannot be accounted for in a guideline or step-by-step process. While the severity of the potential loss plays a role in determining the most appropriate category for data, the meaning of severity has different connotations depending on the type of data (e.g. operational data, program data, medical data, tax data), which may affect the assessed total potential impact. Other than confidential data, which is automatically assigned to data assessed a confidentiality severity level of "high", strictly following this step-by-step process may sometimes result in a potential impact that is not the most appropriate for the type of data being classified. For example, the result of the total potential impact assessment is "medium", which indicates that the data should be classified as "private" data, but, because of other factors, it is determined that a more appropriate classification for this piece of data is "public" data. **It is up to the Data Owner to take into consideration other factors, such as knowing where the data lives and how it will be accessed and used, to determine the most appropriate category for the data.**

One possible solution is to classify data as a group (data that has a common function or purpose) instead of categorizing individual data elements. Under this process, the group will assume the data category of the group's most restrictive data element(s). For example, a database table has, amongst many other fields, a social security number field and a name field. Because anyone can simply make up a social security number and names are readily accessible via an internet search, neither a social security number nor a name field, by itself, is considered PII. However, once the name is associated with the social security number, the two pieces of data take on the attributes of PII, which should be classified as "sensitive" data (see "Sensitive Data" section in this

guideline for more information). Under this circumstance, the data Owner would classify either the database table or entire database, as appropriate, as "sensitive" and the entire group of data will have the same security controls as the group's most restrictive data elements to ensure the confidentiality of the data.

There is no one-size-fits-all process or formula that, for all types of data under all circumstances, will result in the "correct" assignment of a category for the data. Circumstances differ, assigning severity levels to CIA security objectives can vary, and data may be more easily assessed as a group than as individual elements. ***It is up to the data Owner to determine how best to classify data under their control based on what is known about the data, how the data will be used, where the data will be used, its criticality and value to the Agency, and any other concerns that may affect the final outcome of the data classification process.***

Step 4. Apply Sensitivity Label at the determined level of classification using ETSS authorized tools, document footers or watermarks.

Data sensitivity labels are primarily applied directly in Microsoft applications, like Word, Excel, PowerPoint, and Outlook. The labeling process is similar in Word, Excel, and PowerPoint. For each of those applications, a Sensitivity button can be found on the Home tab. The button is located towards the right side of the Home tab. After clicking on "Sensitivity", a dropdown will appear that shows the parent labels of Public, Private, Sensitive, and Confidential, which expands into a more detailed set of options for the specific labels for Sensitive and Confidential when hovered over. Alternatively, sensitivity labels can be added when saving the file under the Sensitivity dropdown, or by clicking the file name at the top of the application and selecting from the Sensitivity dropdown.

To apply a data sensitivity label in Outlook, start by creating a new email draft. Click on the Message tab and use the arrow to the far right to navigate within the tab to locate the Sensitivity button. After clicking on "Sensitivity", a dropdown will appear that shows the parent labels of Public, Private, Sensitive, and Confidential, which expands into a more detailed set of options for the specific labels for Sensitive and Confidential when hovered over. Alternatively, the sensitivity label can be changed in the top right of the email draft.

Additionally, for some users with appropriate access, data sensitivity labels can also be applied through the Information Protection File Labeler in File Explorer, or in Adobe Acrobat with a Pro License. To label files without opening them, open File Explorer and navigate to the file that needs to be labeled. Right click on the file and select "Show more options". In the larger list of options, find and select "Apply sensitivity label with Microsoft Purview". This will open the application that allows for selection of the applicable data sensitivity label. If "Apply sensitivity label with Microsoft Purview" is not listed in the dropdown, the Information Protection File Labeler might not be installed on the user's device.

Data sensitivity labels can be applied to PDFs using Adobe Acrobat for users with a Pro License. Under "All tools", select "Protect a PDF". Under the new options, select "Select a Microsoft Sensitivity Label" and use the dialog box to pick the appropriate data sensitivity label.

Reminder: RI Purview configuration: Sensitive and Confidential must be applied via sublabels (e.g., Sensitive//PII, Confidential//PHI). The parent labels for Sensitive and Confidential are not selectable.

Full details on how to apply data labels, including screenshots, can be found in the knowledge-based article KB0010478 within ServiceNow and in the training video on Proofpoint.

Data Classification Matrix. The "Purview Data Classification Matrix" in *Appendix B* provides a high-level guide to assist Data Owners in assigning the appropriate data sensitivity label to their data. Data may belong to more than one classification, but only one label can be applied to a container of data such as an email, file or document. In general, the Data Container should be assigned to the data sensitivity label that aligns with the strictest confidentiality or availability requirements of the data. However, there is no one-size-fits-all process for assigning data the "correct" sensitivity label. It is the responsibility of the Data Owner to assign appropriate data sensitivity labels for all data they own based on federal or state laws or privacy statutes, how and where the data will be used, who requires access to the data, and the value and criticality of the data to the Agency.

Reclassifying Data. Lowering the sensitivity level of a file, email or document requires justification by the user, which is stored in the file, email or document's audit metadata and becomes part of its governance history. When a sensitivity label is updated, Purview automatically applies the corresponding protection settings of that label, which may adjust encryption, access permissions, and collaboration restrictions such as sharing, forwarding, printing, or external access. These enforcement behaviors are central to the State's broader data governance strategy, where data sensitivity labels, Data Loss Prevention (DLP), records management, and audit controls form the foundation of enterprise information protection.

Updated labels can also trigger new DLP policy tips or enforcement actions, especially when the content becomes more sensitive than before. In practice, even a small change in label selection can significantly alter how a file behaves, who can access it, and what obligations apply to its handling throughout its lifecycle.

Reference

NIST SP 800-60 Rev 1 – Mapping Types of Information and Information Systems to Security Categories

Appendix A:

The data listed below require the highest levels of security controls, access restrictions, and protection. This list is not all-inclusive. It is the responsibility of the data owner with assistance from the data custodian to appropriately classify all data under Agency control.

Confidential Data

Federal Tax Information (FTI)

Federal tax returns and return information (and information derived from it) in the State agency's possession or control covered by confidentiality protections of the Internal Revenue Code (IRC) and subject to IRC 6103(p)(4) safeguarding requirements, including Internal Revenue Service (IRS) oversight are considered FTI. FTI includes return or return information received directly from IRS or obtained through an authorized secondary source, such as 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 other entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from IRS or obtained through a secondary source. Safeguarding FTI is critical to protecting taxpayer confidentiality as required by IRC 6103 and may not be masked to change the character of information to circumvent IRC 6103 confidentiality requirements.

Social Security Administration (SSA) Data

Data under the control of SSA provided to the State agency under the terms of an Information Exchange Agreement with the SSA, including data provided to the State agency by a source other than SSA but for which the State agency attests to that the SSA verified it or the State agency couples the data with other SSA data to certify its accuracy. SSA data is confidential data, including:

- SSA response to request from State agency for information from SSA (e.g. date of death).
- SSA response to query from State agency for verification of Social Security number (SSN).
- Display by State agency of SSA response to query for verification of SSN and associated SSN provided by SSA.
- Display by State agency of SSA response to query for verification of SSN and associated SSN provided to State agency by source other than SSA.
- Electronic records that contain only SSA response to query for verification of SSN and associated SSN whether provided to State agency by SSA or source other than SSA

Criminal Justice Information Services (CJIS)

Criminal Justice Information is the term used to refer to all the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to:

- Biometric
- Identity History
- Biographic Data
- Property Records
- Case/Incident History Data

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified.

- Personally identifiable information (PII)
- Sensitive personally identifiable information (SPII)
- Proprietary business information (PBI)
- Unclassified controlled technical information (UCTI)
- Sensitive but unclassified (SBU)
- International agreements
- Procurement and acquisition information
- Law enforcement-sensitive information

Protected Health Information (PHI)

Data held by a covered entity regarding health status, provision of health care, or payment for health care that can be linked to an individual (i.e. any medical or health insurance data). PHI linked with one or more of the following identifiers is considered confidential data:

- Name
- Address
- All date elements related to an individual (except year)
- Telephone number
- Fax number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/License number
- Vehicle/Device identifier and serial number
- Vehicle license plate number
- Universal Resource Locator
- Internet Protocol (IP) address
- Biometric identifier, including finger and voice prints
- Full face photographic image and any comparable image
- Any other unique identifying number, characteristic or code

Sensitive Data

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is any information about an individual that is maintained by an Agency, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information:

- Social Security number (SSN)
- Driver's license number, Rhode Island state identification card number, or tribal identification number.
- Account or credit/debit card number in combination with security/access code, password, or personal identification number (PIN) that permits access to an individual's financial account.
- Medical or health insurance information.

- Email address with any required security/access code or password that permits access to an individual's personal, medical, insurance, or financial account.
- Authenticators

Family Educational Rights and Privacy Act (FERPA)

Data that is collected and stored that becomes part of a student's education record. Education records are records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to:

- Grades
- Transcripts
- Class lists
- Health records
- Student course schedules
- Student discipline files
- Student financial information (at the postsecondary level)

Payment Card Information (PCI)

Credit card data. A credit card number or primary account number in combination with one or more of the following is considered confidential data:

- Cardholder name
- Service code
- Expiration date
- CAV2, CVC2, CVV2, CID
- PIN or PIN block
- Full magnetic stripe/chip data

Working Confidential

Any information to be safeguarded, protected, and shared only on a "need-to-know" basis with an expected impact to security posture, health, or safety.

- Attorney Files, Attorney-Client Communications, State Law Investigative Records
- IT security data (Configurations, Logs, Business Continuity Plans, Disaster Recovery Plans)
- Personnel Records, Payroll Data

Private Data

Private

Data that requires an elevated level of security controls, protection, and access restrictions. Private data is considered proprietary, internal-only data and not to be shared without approval (i.e. Access to Public Records Act (APRA) or Proxy access request).

- Internal Policies
- Internal Budgets
- Business Strategies

Appendix B:

Purview Data Classification Matrix

Classification	Definition	Examples	Purview Label	Sub-levels	Handling Requirements
Public	No access restrictions; may be viewed by anyone.	Press releases, public website content, de-identified datasets.	Public	N/A	May be shared internally and externally; no encryption required.
Private	Internal-only data; proprietary content; not for external sharing without approval.	Internal memos, project plans, non-public organizational information.	Private	N/A	Internal-only. External sharing requires Agency approval. Encryption recommended if shared.
Sensitive	Regulated or protected data identifiable to individuals or governed by law, but do not have prescribed security controls that the System Owner must enforce.	PII, student records, cardholder data, Draft contracts, unreleased policy documents, strategic materials.	Sensitive	PII, FERPA, PCI, Working Confidential	Encryption required. Internal use only unless authorized by law or contract. Strict access control.
Confidential	Highest sensitivity; unauthorized disclosure can cause organizational harm and have prescribed security controls that the System Owner must enforce.	Medical data, criminal justice information, social security administration data, Federal Tax Information	Confidential	PHI, CUI, CJIS, SSA, FTI	Encryption required. External sharing is prohibited unless formally authorized.

These classifications of data pertain to how they are organized and packaged together. The object that packages the data as one unit (Data Container) must have one of the following Data Sensitivity Labels applied. The data that resides in a container may belong to multiple classifications. Choose that label that has the highest confidentiality of the data stored in the container.

Information Assurance Level (IAL) indicates control stringency

IAL-1 applies to Public/Private

IAL-2 applies to Sensitive/Confidential

Data Classification Matrix		
Classification	**Information Assurance Level (IAL) 1**	
Type	**Public**	**Private**
Sub-Type	N/A	N/A
Definition	Data that requires a low level of security controls to ensure applicable release compliance. Public data has no access restrictions and may be viewed by anyone.	Data that requires an elevated level of security controls, protection, and access restrictions. Private data is considered proprietary, internal-only data and not to be shared without approval (i.e. APRA or Proxy access request).
Data Tag/Label	Public	Private
Document Water Marking	No Label	Private
Dissemination Restrictions	None	External or APRA sharing must be approved before sharing
Supersedes /Replaces	N/A	N/A
Regulation /Authority	https://webserver.rilegislature.gov//Statutes/TITLE38/INDEX.HTM	https://webserver.rilegislature.gov//Statutes/TITLE38/INDEX.HTM

Data Classification Matrix				
Classification	**Information Assurance Level (IAL) 2**			
Type	**Sensitive**			
Sub-Type	Personally Identifiable Information (PII)	Family Educational Rights and Privacy Act (FERPA)	Payment Card Industry Data Security Standard (PCI DSS)	Working Confidential
Definition	Any information about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.	Student education records that can be linked to a specific individual.	Cardholder data and sensitive authentication data are considered account data and are defined as follows: Primary Account Number (PAN), Cardholder name, Expiration Date, Service Code, Full track data (magnetic stripe or chip data), card verification code, PINs/PIN Blocks.	Any information to be safeguarded, protected, and shared only on a "need-to-know" basis with an expected impact to security posture, health, or safety. Confidential Working Document RIGL §38-2-2(4)(E),(K)
Data Tag/Label	PII	FERPA	PCI	Working Confidential
Document Water Marking	Sensitive//PII	Sensitive//FERPA	Sensitive//PCI	Sensitive //Working Confidential
Dissemination Restrictions	Internal or External sharing must be approved prior to dissemination and not to be shared via APRA request.	Internal or External sharing must be approved prior to dissemination and not to be shared via APRA request.	Internal or External sharing must be approved prior to dissemination and not to be shared via APRA request.	Only approved for authorized internal colleagues sharing as part of required daily tasks and not approved for external or APRA sharing outside of legal requirement or approved sharing MOU.
Supersedes /Replaces	N/A	N/A	PCI DSS v4.0	N/A
Regulation /Authority	https://webserver.rilegislature.gov/BillText24/HouseText24/H7787A.htm	https://www.ecfr.gov/current/title-34/subtitle-A/part-99?toc=1	https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf	Access to Public Records RIGL 38 http://webserver.rilin.state.ri.us/Statutes/TITLE38/38-2/38-2-2.HTM

Data Classification Matrix			
Classification	**Information Assurance Level (IAL) 2**		
Type	**Confidential**		
Sub-Type	Protected Health Information (PHI)	Controlled Unclassified Information (CUI)	Criminal Justice Information Services (CJIS)
Definition	Information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.	Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified.	Criminal Justice Information is the term used to refer to all FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.
Data Tag/Label	PHI	CUI	CJIS
Document Water Marking	Confidential //PHI	Confidential//CUI	Confidential//CJIS
Dissemination Restrictions	Internal or External sharing must be approved prior to dissemination and not to be shared via APRA request.	Only approved for authorized internal colleagues sharing as part of required daily tasks and not approved for external or APRA sharing outside of legal requirement or approved sharing MOU.	Only approved for authorized internal colleagues sharing as part of required daily tasks and not approved for external or APRA sharing outside of legal requirement or approved sharing MOU.
Supersedes /Replaces	N/A	N/A	N/A
Regulation /Authority	https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C?toc=1	https://www.ftc.gov/policy-notices/controlled-unclassified-information	https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/cjis_security_policy_v5-9-5_20240709.pdf

Data Classification Matrix		
Classification	**Information Assurance Level (IAL) 2**	
Type	**Confidential**	
Sub-Type	Social Security Administration (SSA)	Federal Tax Information (FTI)
Definition	Information collected and provided by the Social Security Administration. This data includes details about people's wages, identifying information, employers, addresses, and more. It encompasses various types of information such as names, Social Security numbers, addresses, wages, benefits, and disabilities.	Any return or return information received from the IRS or any secondary source which is protected by the confidentiality provisions of Internal Revenue Code section 6103.
Data Tag/Label	SSA	FTI
Document/Water Marking	Confidential//SSA	Confidential//FTI
Dissemination Restrictions	Only approved for authorized internal colleagues sharing as part of required daily tasks and not approved for external or APRA sharing outside of legal requirement or approved sharing MOU.	Only approved for authorized internal colleagues sharing as part of required daily tasks and not approved for external or APRA sharing outside of legal requirement or approved sharing MOU.
Supersedes/Replaces	MARS-E v2	Publication 1075 (October 2014)
Regulation/Authority	https://www.cms.gov/files/document/mars-e-v2-2-vol-1final-signed08032021-1.pdf	IRS Publication 1075 https://www.irs.gov/pub/irs-utl/p1075.pdf