Data Classification Policy

1. Purpose

Explain why data classification should be done and what benefits it should bring.

The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to the organization, so sensitive corporate and customer data can be secured appropriately.

2. Scope

Define the types of data that must be classified and specify who is responsible for proper data classification, protection and handling.

This policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all of the organization's employees, as well as to third-party agents authorized to access the data.

3. Roles and Responsibilities

Describe the roles and responsibilities associated with the data classification effort. Departments should designate individuals who will be responsible for carrying out the duties associated with each of the roles.

Data owner — The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management. The data owner shall address the following:

Review and categorization — Review and categorize data and information collected by his or her department or division

Assignment of data classification labels — Assign data classification labels based on the data's potential impact level

Data compilation — Ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data

Data classification coordination — Ensure that data shared between departments is consistently classified and protected

Data classification compliance (in conjunction with data custodians) — Ensure that information with high and moderate impact level is secured in accordance with federal or state regulations and guidelines

Data access (in conjunction with data custodians) — Develop data access guidelines for each data classification label

Data custodians — Technicians from the IT department or, in larger organizations, the Information Security office. Data custodians are responsible for maintaining and backing up the systems, databases and servers that store the organization's data. In addition, this role is responsible for the technical deployment of all of the rules set forth by data owners and for ensuring that the rules applied within systems are working. Some specific data custodian responsibilities include:

Access control — Ensure that proper access controls are implemented, monitored and audited in accordance with the data classification labels assigned by the data owner

Audit reports — Submit an annual report to the data owners that addresses availability, integrity and confidentiality of classified data

Data backups — Perform regular backups of state data

Data validation — Periodically validate data integrity

Data restoration — Restore data from backup media

Compliance — Fulfill the data requirements specified in the organization's security policies, standards and guidelines pertaining to information security and data protection

Monitor activity — Monitor and record data activity, including information on who accessed what data

Secure storage — Encrypt sensitive data at rest while in storage; audit storage area network (SAN) administrator activity and review access logs regularly

Data classification compliance (in conjunction with data owners) — Ensure that information with high and moderate impact level is secured in accordance with federal or state regulations and guidelines

Data access (in conjunction with data owners) — Develop data access guidelines for each data classification label

Data user — Person, organization or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended, and comply with this policy and all policies applicable to data use.

4. Data Classification Procedure

Describe each data classification procedure step by step. Detail who performs each step, how data is assessed for sensitivity, what to do when data doesn't fit an established category and so on.

Example of a detailed procedure:

1. Data owners review each piece of data they are responsible for and determine its overall impact level, as follows:

If it matches any of the predefined types of restricted information listed in Appendix A, the data owner assigns it an overall impact level of "High."

If it does not match any of the predefined types in Appendix A, the data owner should determine its information type and impact levels based on the guidance provided in Sections 5 and 6 of this document, and NIST 800-600 Volume 2. The highest of the three impact levels is the overall impact level.

If the information type and overall impact level still cannot be determined, the data owner must work with the data custodians to resolve the question.

2. The data owner assigns each piece of data a classification label based on the overall impact level:

Overall impact level	Classification label
High	Restricted
Moderate	Confidential
Low	Public

3. The data owner records the classification label and overall impact level for each piece of data in the official data classification table, either in a database or on paper.

4. Data custodians apply appropriate security controls to protect each piece of data according to the classification label and overall impact level recorded in the official data classification table.

Example of a basic procedure:

1. Data owners review and assign each piece of data they own an information type based on the categories in https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf .

2. Data owners assign each piece of data a potential impact level for each of the security objectives (confidentiality, integrity, availability), using the guide in Section 6 of this document. The highest of the three is the overall impact level.

3. Data owners assign each piece of data a classification label based on the overall impact level:

Overall impact level	Classification label
High	Restricted
Moderate	Confidential
Low	Public

4. Data owners record the impact level and classification label for each piece of data in the data classification table.

5. Data custodians apply information security controls to each piece of data according to its classification label and overall impact level.

5. Data Classification Guideline

Create a table that describes each type of information asset the agency stores, details the impact of each of the three security objectives, and specifies the impact levels and classification to be assigned to each type of asset.

Use this table to determine the overall impact level and classification label for many information assets commonly used in the organization.

Federal Budget Planning Documents			
Federal budget planning documents state the potential expenses for the following year. They include data about partners and suppliers, as well as analytical and research data.			
Information Types			
Funds Control	Funds Control documents include information about the management of the federal budget process, including the development of plans and programs, budgets, and performance outputs, as well as information about financing federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other mechanisms.		
Security Objectives	Confidentiality Impact	Integrity Impact	Availability Impact
Impact Description	Unauthorized disclosure of funds control information (particularly budget allocations for specific programs or program elements) can be seriously detrimental to government interests in procurement processes. In many instances, such	Funds control activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive	Funds control processes are generally tolerant of delay. Typically, disruption of access to funds control information can be expected to have only a limited adverse effect on

	unauthorized disclosure is prohibited by executive order or by law. Premature release of drafts of funds control information can yield advantages to competing interests and seriously endanger agency operations or even agency mission.	obligations or disbursements.	agency operations, agency assets or individuals.
Impact Level	Moderate	Moderate	Low
Overall Impact Level	Moderate		
Data Classification Label	Confidential		

6. Impact Level Determination

Provide a table that will help data owners determine the impact level for each piece of data by describing the security objectives you want to achieve and how failure to attain each objective would impact the organization.

Use this table to assess the potential impact to the company of a loss of the confidentiality, integrity or availability of a data asset that does not fall into any of the information types described in Section 5 and NIST 800-600 Volume 2.

Security Objective	Potential Impact		
	Low	Moderate	High

Confidentiality. Restrict access to and disclosure of data to authorized users in order to protect personal privacy and secure proprietary information.	Unauthorized disclosure of the information is expected to have limited adverse effects on operations, organizational assets, or individuals.	Unauthorized disclosure of the information is expected to have a serious adverse effect on operations, organizational assets, or individuals.	Unauthorized disclosure of the information is expected to have a severe or catastrophicadverse effect on operations, organizational assets, or individuals.
Integrity. Guard against improper modification or destruction of data, which includes ensuring information nonrepudiation and authenticity.	Unauthorized modification or destruction of the information is expected to have a limitedadverse effect on operations, assets, or individuals.	Unauthorized modification or destruction of the information is expected to have a serious adverse effect on operations, assets, or individuals.	Unauthorized modification or destruction of the information is expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
Availability. Ensure timely and reliable access to and use of information.	Disruption of access to or use of the information or information system is expected to have a limited adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have a serious adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have a severe or catastrophicadverse effect on operations, assets, or individuals.

7. Appendix A

Describe the types of information that should automatically be classified as “Restricted” and assigned an impact level of “High.” Having this list will make the data classification process easier for data owners.

Types of Information that Must be Classified as “Restricted”

Authentication information

Authentication information is data used to prove the identity of an individual, system or service. Examples include:

Passwords

Shared secrets

Cryptographic private keys

Hash tables

Electronic Protected Health Information (ePHI)

ePHI is defined as any protected health information (PHI) that is stored in or transmitted by electronic media. Electronic media includes computer hard drives as well as removable or transportable media, such as a magnetic tape or disk, optical disk, or digital memory card.

Transmission is the movement or exchange of information in electronic form. Transmission media includes the internet, an extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media.

Payment Card Information (PCI)

Payment card information is defined as a credit card number in combination with one or more of the following data elements:

Cardholder name

Service code

Expiration date

CVC2, CVV2 or CID value

PIN or PIN block

Contents of a credit card’s magnetic stripe

Personally Identifiable Information (PII)

PII is defined as a person’s first name or first initial and last name in combination with one or more of the following data elements:

Social security number

State-issued driver’s license number

State-issued identification card number

Financial account number in combination with a security code, access code or password that would permit access to the account

Medical and/or health insurance information

Revision History

Be sure to track all changes to your data classification policy.

8. Revision History

Version	Published	Author	Description