



CENTRAL INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET

POLICY NUM. TIC-019

DATE EFFECTIVE: 6 DE MARZO DE 2013
DATE REVISION: 15 DE AGOSTO DE 2013

TOPIC: DATA CLASSIFICATION & PROTECTION

DESCRIPTION

This policy serves to provide the agencies of the Commonwealth of Puerto Rico Government (CPRG) with a concise set of guidelines on how to analyze and determine if the data is of a sensitive nature and if deemed to give steps on how to protect such data.

The CPRG recognizes through its executive order *OE-2013-013* that there is a need to liberate the data. For this reason it is necessary to equip the *agencies* with an appropriate set of tools to determine the data that can be liberated and to enable agencies to perform TIC-016 "Guía de Interfaz de desarrollo en programación "Web API's"". The aim is to open the data in a manner that is consistent with the applicable laws and standards that allows the dissemination of data but at the same time providing the necessary privacy protection on the data that is deemed of a *personal for agency use only* or of *sensitive nature*.

66 To satisfy the need to protect this sensitive and personal data the CPRG will maintain a data classification and protection policy. This policy along with corresponding procedure(s) designed to enable the protection of data in different media and from unauthorized disclosure, use, modification, or deletion. The effective handling of the data and information within the CPRG will be made in accordance with this policy; however, agencies are still subject to any other requirement established by state or federal law, rules or regulations. This policy is divided into two parts: The first part deals with the management of the classification of data and the second part deals with protection mechanisms for information that is deemed sensitive in nature.

LEGAL BASE

Act No. 151 of June 22, 2004 states that the Office of Management and Budget shall have the power to implement, develop and deliver public policy to follow and guidelines governing the acquisition and implementation of systems, equipment and information programs technology for government agencies with the primary objective of achieving interconnection of agencies to facilitate and streamline services to the people.

PURPOSE

The purpose of this policy is to inform CPRG information stakeholders and data users about the data classification, the procedures to carry out the analysis to determine if data should be classified, and the protection elements needed by the CPRG for handling the sensitive and classified data generated, accessed, transmitted and stored.

The policy will inform all relevant parties on uniform data handling practices that will enable the security required of sensitive information and at the same time conform to local, state, and

federal regulations regarding privacy and confidentiality.

SCOPE

This data classification policy shall apply to all agencies within the CPRG in their use of the data in its various forms. These forms include written, verbal, and information stored in information systems.

FREQUENCY OF REVIEW

This policy will be reviewed and updated if necessary on an annual basis.

POLICY AND PROCEDURE

I. DATA CLASSIFICATION

Roles and Responsibilities

The CPRG policy must ensure that proper accountability to guarantee that the data is secure. To provide this accountability the following roles are defined:

1. Data Owner – the individual(s) that are responsible for the data/information that is: generated, gathered, transmitted, stored, or deleted. The owner is responsible for classifying, maintaining the data and information within the classification life cycle of the data exposed in this policy.
2. Data User – the individual(s) that has access to the data and performs an authorized task with the data. The data user is responsible for maintaining the classification of the data when it is within the custody of the user.
3. System Owner – the individual(s) responsible for the system where the data is stored and transmitted. The system owner is responsible for applying the system security necessary to support the protection of the data asset.

All significant information assets will have a nominated owner and should be accounted for. The owner must be a member of staff whose need to know is appropriate for the asset they own. The owner's responsibility for the asset and the requirement for them to maintain will be formalized and agreed.

Need to know for sensitive DATA

All information that is classified under this policy that is deemed sensitive will abide by the principle of least privilege. Under this principle the personnel that have access to the information must demonstrate the need to know and will get access to the least amount of information to complete the requirement of the need to know.

Rationale for Classification

The CPRG's response to the growing demand to carry out its mission depends on the free flow of information both within the CPRG, other Government agencies and to Puerto Rico's citizens. Nevertheless, throughout CPRG's operations it is often required that certain information be maintained in confidence in order to protect our citizens. It is also necessary to protect certain information with regards to the citizen's identity to comply with the laws and regulations that dictate such privacy. It is also necessary to establish the necessary protocol to disclose information that is of a sensitive nature to other parties that may have the need to know. It is also necessary to establish a protocol to release the information when its sensitivity classification expires.

68

The rationale for classification must also abide by existing laws and regulations concerning access and usage of information set forth by state or federal authority

Risk Assessment

Risk assessment is to be carried out by the data owner to determine the classification of the data. FIPS 199 defines three levels of impact that applies to the risk analysis of data in case of a security breach. This breach is translated into:

- Loss of Confidentiality
- Integrity Compromise
- Availability Denial

All data will be analyzed according to the potential impact on confidentiality, integrity, and availability and the possibility of breach as described above. The breach impact will then be classified per FIPS 199 as:

- Low
- Moderate
- Severe

Data/Information Classification

Medium of the data:

1. Systems data in transit or in storage
2. Radio data
3. Hard copy data

The data to be protected will be analyzed to be cataloged as:

1. Structured Data – data associated with a business application or system. Data that resides in fixed fields within a record or file. Relational databases and spreadsheets are examples of structured data.
2. Unstructured Data – data not associated with a business application or system. The unstructured data may be characterized as free fields containing narratives, paragraphs, miscellaneous information that does not contain a pre-required format. Examples of such unstructured data include but not limited to: email messages, blogs, web pages, Pdf files, word processing documents, etc.

Unified Classification Markings

All information assets will be assessed and classified using the risk assessment steps outlined previously. This step will be carried out by the data owner according to the practices outlined in this document and the content of the data. All information assets must be classified and labeled in accordance with the selected classification criteria. The classification scheme of Confidential, official agency, and Interoperability, and Public Domain Data is given but a more elaborated classification criteria can be required for some agencies in accordance to applicable law. All agencies within the CPRG are advised and instructed to adhere to any other classification scheme which apply to them based on sector and jurisdiction. If there are no agency-specific categorization of information requirements established by law or competent authority, the

66

proposed classification scheme described in this policy should be adopted by the agency.

Confidential Data

Confidential Data is information that must be protected in compliance to statutes, regulations, State policies, or contractual language. In addition, tactical law enforcement capabilities and sensitive investigations may fall under the heading of confidential data. Disclosure of Confidential Data internal to the CPRG should be on a need-to-know basis only and under certain circumstance also require background checks. Disclosure under this category should be informed to the <name of department or assigned personnel>.

Confidential data includes any data of which the inappropriate disclosure could have a material adverse effect on the CPRG operations, the conduct of agency programs, or the privacy to which individuals are entitled. For such reasons, confidential data will be considered sensitive information.

Official agency and Interoperability Data

GG
Official agency and Interoperability Data is information that must be guarded due to investigative, ethical or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official agency and Interoperability Data is information that is restricted but may be used throughout and shared across agencies and to provide services that have a legitimate purpose for accessing such data. Data Owners may designate data as **Official agency and Interoperability Data use only**. For such reasons, Official agency and Interoperability Data will be considered sensitive information.

Public Domain Data

Public Data is information that may be open to the general public. It is defined under this policy that it does not fall under the purview of the rationale for classification. Public domain data will be considered to be made accessible as **open data**. The openness of the data will be contingent on whether the particular agency involved has the necessary technological advances and proper funding for the project.

Marking of Data

All information, data, folders, storage facilities, etc. will be clearly marked and visible. The information marking will be positioned in a place where it is clearly visible during the handling of the document, data, folder, storage facility, etc. The marking will reflect the data classification category of the highest level of classification contained in the data.

How to classify the information

A data evaluation matrix provided in the data classification procedure will be used to evaluate the information of the agencies data when considering the classification of data. The data matrix will be filled evaluating each of the following elements (1) Attempts on the safety of citizens with possible loss of life. (2) Attempts on the safety of Government workers with possible loss of life. (3) Affects or hampers the delivery and operations of critical emergency services. (4) Affects or hampers the administration of the Agency. (5) Impact services offered by the Agency (6) Creates a negative effect on public finances. (7) Impact on private sector finances. (8) Damaging to standing or reputation of the Citizen. (9) Impacts the health information of citizens. (10) Damaging to the Identity of the Citizen.

The following rules dictate the data classification procedure to be carried out by agencies:

- Only when there is an impact on the confidentiality citizens, agencies or business using the criteria above should the data be assessed under the heading of severe.
- Only when there is a real possibility of permanent and severe compromise to the integrity of the data without possibility of recovery taking into account each of the criteria above should it be considered to be assessed as severe.
- Only when there is the possibility of sustained and permanent attempts on the availability of the data taking into account each of the criteria above should it be given an impact assessment of severe.

Each of the fields of the data assessment matrix provided in the procedure needs to be analyzed for the set data element contemplated to be classified. The guiding principles under this policy is:

- The data elements will be classified under the highest label obtained during the evaluation. If one element is severe the highest criteria will be selected
- If the impact assessment is severe, the element set will be evaluated to extract the elements that make the impact assessment severe and lower the impact assessment category. Those elements whose impact assessment category remains under the severe category will then be protected under the sensitive information criteria.
- If confidentiality is considered as severe the overall security determination will remain severe. If integrity or availability is considered severe it will remain severe until mitigation strategies are in place to lower the overall determination from severe. Once the mitigation strategy is implemented then the datum will be considered for reclassification to a lower classification determination.

The data to be classified will be evaluated for each of the categories to see if it applies or not. If the category applies to the data element then the impact level of low, moderate, or severe will be selected. Under the impact level each of the elements of security will be evaluated for the potential impact.

66

Classification Handling Criteria

The classification handling criteria will consist of the measures necessary to protect the information confidentiality integrity and availability according to the classification level of the information. Minimum level of protections will be applied to each category level that is not public domain data. Protection mechanisms will consist of:

- Physical
- Media in transit
- Media in storage

II. SENSITIVE DATA PROTECTION

Physical Protection

Except where impracticable physically tangible information will be stored on centralized facilities to ensure enhanced confidentiality, integrity and availability as outlined within this policy and the policies outlined in the section on **Policy dependencies**.

Staff should not be allowed to access information until their supervisor is satisfied that they understand and agree the responsibilities for the information that they will be handling as outlined in this policy. Files which are classified as a **Confidential Data** or **Official agency and Interoperability Data** will only be stored on secure network or segregated areas of the network that are classified to handle such data.

Printing transforms digital data into printed data and as such the data is transferred from one medium to another. Such transference of medium does not change the need for physical protection. The **Confidential Data** or **Official agency and Interoperability Data** will have limitations on printing as specified on a document basis.

Faxing of data consist of two parts which is the transmission and the printing of the document. All transmission including faxed documents will conform to the Security of Media in Transit section. The Printing of the document will conform to the Printing Protection subsection above.

Security of Media in Transit

Media in transit refers to information or data that uses communications and data transmission processes. All media in transit will be evaluated for transmission security according to the data/information classification level. In addition each transmission must be validated that it goes to an appropriate individual or entity that has the need to know and has the appropriate level of clearance to view the data.

Communications Transmission through the Internet include but are not limited to email, instant messaging, chat, all variations of FTP (file transfer protocol) , all variations of P2P (peer-to-peer) processes, and streaming media processes. Each of these protocols will be validated that they carry the appropriate security according to the **Policy dependencies** and **Standards followed**.

CB

Radio transmissions that are being used as part of the CPRG will be subject to revision to determine the classification level of such information. All information deemed **Official agency and Interoperability Data** or **Confidential Data** will abide by the standards established communications security outlined in the **Policy dependencies** and **Standards followed**.

Except where impracticable electronic information will be stored on centralized facilities to ensure enhanced confidentiality, integrity and availability as outlined within this policy and the policies outlined in the section on **Policy dependencies** and **Standards followed**. All classified information will be evaluated for acceptable use of encryption as outlined in this policy and encryption standards. All software as well as operating system configuration and hardware will conform to the appropriate security level established for each classification category.

ff
Staff should not be allowed to access information until their supervisor is satisfied that they understand and agree the responsibilities for the information that they will be handling as outlined in this policy. Files which are classified as a **Confidential Data** or **Official agency and Interoperability Data** will only be stored on secure network areas and appropriate storage medium that are classified to handle such data.

Regular backups of all electronic information will take place as outlined within the Communications and Operations security policy Records management and retention guidance will be followed as defined in the Data Retention schedule.

Encryption

All encryption devices shall comply with FIPS 140-2 standard.

Encryption Strength

The minimum encryption to be applied to sensitive information is 128 bit.

Transmission of Data

When sensitive data is transmitted outside the boundary of a secure location, the data shall be protected via encryption unless the device is not capable and falls under the exceptions of the applicable standards. All sensitive data over unencrypted channels will be notified to <name of department or assigned personnel> for assessment and approval.

PKI

Whenever it is deemed necessary to implement PKI the <name of department or assigned personnel> shall develop and implement a certificate policy (CP) and certification practice statement (CPS) for the issuance of public key certificates used in the information system. The <name of department or assigned personnel> shall verify that the registration process to receive a public.

key certificate shall :

- Have justification according to the security level of the person and the classification of the data. This justification must be approved by <name of department or assigned personnel>.
- The infrastructure must comply with the appropriate security measures according to the security classification.
- Ensure that the registration authority verifies the identity of the person and that the certificate is issued to the intended party.

Interoperability between Organizations

Interoperation between organizations will be evaluated by <name of department or assigned personnel> for compatibility between data classification levels and protection mechanisms. If the organizations have compatibility of policies, a signed Memorandum of understanding will be signed agreeing to the exchange of data. This agreement will specify the data to be shared and the classification level of the data to be shared.

Only individuals and entities designated have approved access rights to the transmitted data between organizations. The <name of department or assigned personnel> will verify that the organization has a need to know and should receive, distribute, store or have in their possession this type of data. Information should be accessed only from a controlled access area.

Removing Classification Category

Data shall have its classification removed or downgraded by the data owner or <name of department or assigned personnel> when it complies with the requirements described in this section.

It will be assumed that the information that continues to meet the classification requirements under this policy requires continued protection.

The information will be removed or downgraded if:

1. The information must be disclosed due to legal proceedings and becomes a public document.
2. Have exceeded a useful life of 25 years

The classification can be exempt from being removed or downgraded due to:

1. Special law enforcement operations
2. Records containing classified information that originated with other agencies
3. Information from citizens that is deemed personally identifiable information, and will continue being considered as such.

Information that is exempted from automatic removal or downgrade under this section shall remain subject to the mandatory and systematic declassification review that will take place on an annual basis.

Disposal of Data

Electronic documents

All storage media, such as computer hard drives, flash drives, or CD/DVDs, containing

66

CPRG data in electronic form should be sent to the _____ <name of department or assigned personnel>_____ for secure deletion. The _____ <name of department or assigned personnel>_____, under guidance of the Security Information Officer, will delete the CPRG data from the media in accordance with current **NIST Special Publication 800-88**. Any media which cannot be processed according to this standard will be destroyed; either smashed or degaussed, by the CPRG Security Information Officer or his/her representative.

Since there is no way to know exactly what data is stored on computers used at specific computer media of the CPRG, all computers will be considered to contain **confidential data**. All computers must have all attached electronic storage media erased prior to redeployment or disposal.

Paper documents

All CPRG **confidential data** existing in paper form must be disposed of by **shredding**. All documents should be dropped off in **designated containers** where afterwards they will be shredded using appropriate shredding equipment. If a department does not have access to designated shredding containers, the department head or his/her designee shall consult with existing divisions of equal sensitive information handling rights for shredder access.

Documents taken outside of CPRG

65
Any paper or electronic documents containing CPRG Protected or Sensitive data taken outside of CPRG by employees, consultants or agents of CPRG must be cleared to take such information outside the premises of the agency. All equipment used must meet with the required security protection mechanisms outlined in this document and its dependencies. Any paper or electronic documents containing CPRG Protected or Sensitive data that are taken outside of CPRG by parties who are contractually bound to handle data produced by CPRG must dispose of paper documents through a licensed document destruction company and electronic documents through a method that meets or exceeds the standards in the CPRG Secure Deletion standards. Alternatively, the documents can be returned to CPRG for proper destruction.

All external personnel and contracting agents will be bound by this policy whenever handling sensitive data.

Loss of sensitive data

All loss of sensitive data must be immediately reported to _____ <name of department or assigned personnel> for immediate evaluation of risk and appropriate mitigation procedures.

CPRG Public Domain Data and recycling policy

Paper documents will be verified that they do not contain sensitive data that is classified as **sensitive**. After this check has been carried out the paper should be recycled whenever it is possible.

Authorization of Destruction or recycling

Data shall be reviewed to verify that the retention period or declassification process for the data in question has been properly carried out. All known audits and audit discrepancies regarding data scheduled for destruction must be settled before the records can be destroyed; all known investigations or court cases involving said data must be resolved before the records can be destroyed.

Departments will record that the data was destroyed, the date of destruction, and method of destruction. Methods of destruction for specific data types must comply with the data destruction policy outlined below and afterwards can be recycled if possible.

Minimal Destruction Policy

All paper and electronic media destruction devices will comply with **NIST Special Publication 800-88**. All documentation that cannot be determined to be public domain data will be treated as sensitive and will follow the procedures outlined above for handling sensitive data.

Compliance

The information security team and audit services will review compliance of this policy with random spot checks and advice to services.

66 Failure to comply with policies relating to information systems could result in penalties and / or suspension of personnel. External consultants or agents of the agency may incur in penalties including but not limited to contract termination.

Definitions

Availability - Ensuring timely and reliable access to and use of information.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity - Guarding against improper information modification or destruction and includes ensuring information non- repudiation and authenticity.

Secure location - Secure locations means any building or government infrastructure that has a data protection policy that is equivalent to the CPRG data policy and is recognized by the CPRG as a secure location.

Sensitive data - Sensitive data refers to any type of data that has been classified according to this policy that is not public domain data

Open data - data that is freely available without any restriction for its consumption and use.

Consulted Standards

This policy draws its guidance from:

- FIPS PUB 199
- FIPS PUB 140-2
- NIST Special Publication 800-122
- NIST Special Publication 800-88

Policy dependencies

This policy is dependent on other policies that complement its content. The Data

Classification and Protection Policy depend on:

- IT Infrastructure security policy
 - SP 800-123 Guide to General Server Security
 - SP 800-44 Version 2 Guidelines on Securing Public Web Servers
 - SP 800-83 Rev. 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- Communications and Operations Security policy
 - FIPS 191 Guideline for The Analysis of Local Area Network Security
 - SP 800-153 Guidelines for Securing Wireless Local Area Networks (WLANs)
- Remote and mobile working Acceptable use policy
 - SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
 - SP 800-77 Guide to IPsec VPNs
- Software security policy developed by the agency
- Recruitment policy developed by the agency
- Guide TIC-016 "Interfaz de desarrollo en Programación "Web API's"

Additional References

- SOCITM Local Authority Impact Levels
- Example of Crime Data Analysis for Puerto Rico Police Department

Attached

- Procedure – data classification (template)

Purpose

The purpose of this operating procedure is to document the decision matrix for classifying data in a consistent manner across all domains of the Commonwealth of Puerto Rico Government (CPRG). The document also serves the purpose to inform CPRG personnel on the categories that need to be evaluated when making the decision to classify the data.

Frequency of Review

This procedure will be reviewed and updated if necessary on a bi-annual basis.

Classification of Data

The data matrix in the table below serves as a guideline on the fields that need to be evaluated when considering the classification of data. Each of the fields needs to be filled for each data element to be classified.

The data to be classified will be evaluated for each of the categories to see if it applies or not. If the category applies to the data element then the impact level of low, moderate, or severe will be selected. Under the impact level each of the elements of security will be evaluated for the potential impact.

Note: a category may have impacts on all elements of security at different impact levels.

Steps for the Summary section of the template

1. Fill in the agency field with the name of the agency
2. Provide a general description in the description field. The description should state the nature of the data that is being analyzed.
3. In the specific fields contemplated in the analysis, each of the data elements should be explicitly entered in the table below. Each of the elements will also include a brief **description per field** and the data type of the data (Numeric alphanumeric, date, coordinate, etc.)
4. The temporal frequency of the update will be stated in the temporal nature of the data field. If it is non-real or backup data the frequency of update will be explicitly stated.

Steps for the Analysis Section

5. All the analysis boxes will be completed according to the criteria established in the data classification policy. All the analysis boxes will be completed according to the criteria established in this data classification policy.
 1. Fill in the Information Type Name by providing the individual Datum name.
 2. Provide the overall impact rating (i.e., the high water mark) for each security objective based on the loss of the same in case of a breach.

Confidentially - The loss of confidentiality will contemplate if Data classification can be re-established by modifying the data (e.g. Loss of confidentiality on location data of a sensitive event can be mitigated and confidentiality can be re-established by moving the location of the event). [Select: LOW, MODERATE, SEVERE or NOT APPLICABLE]

Integrity - The loss of integrity will contemplate if: (i) Data is altered at the source or at a replication site; (ii) If backup data exists; (iii) If damage is temporary or permanent; (iv) Whether a substantial damage can occur by the loss of integrity. [Select: LOW, MODERATE or SEVERE]

Availability - The loss of availability will contemplate if: (i) Availability denial is temporary or permanent; (ii) The time it will take in order to reestablish availability; (iii) The amount of losses incurred during the availability denial [Select: LOW, MODERATE or SEVERE]

3. For each datum fill in the rationale for the security objective classification justifying each and every one of the 10 criteria elements described in the section how to classify the information of the data classification policy

4. Based on the security objectives impact levels, and the rationale for selecting the categorization, fill in the determination field as:

- a) Confidential Data
- b) Official Agency and Interoperability Data
- c) Public Domain Data
- d) Other classification

The other classification marking will only be used if there is an applicable law or regulation that establishes a different classification scheme than the one presented in this data classification policy. All agencies within the CPRG are advised and instructed to adhere to any other classification scheme which applies to them based on sector and jurisdiction.

66

Summary Section

Agency: _____

General Field description: _____

Specific fields contemplated in the analysis

Field Number	Description	Type

fb

Temporal nature of the data

- a) Real time data _____
- b) Non real time data _____
- c) Archival/Backup data _____

Roles and Responsibilities

Data Owner: _____
Data User: _____
System Owner: _____

Change Management

Revision:
Change Description:
Created / Edited by:
Date:
Approved By:

Analysis Section

Information Type Name	Security Objective	Individual Determination Rationale for Selecting or Adjusting Security Categorization Levels	Overall Determination
	Confidentiality		
	Integrity		
	Availability		
	Confidentiality		
	Integrity		
	Availability		
65	Confidentiality		
	Integrity		
	Availability		
	Confidentiality		
	Integrity		
	Availability		
	Confidentiality		
	Integrity		
	Availability		
	Confidentiality		
	Integrity		
	Availability		