



GOBIERNO DE PUERTO RICO
MUNICIPIO AUTÓNOMO DE MAUNABO
LEGISLATURA MUNICIPAL

PROYECTO DE ORDENANZA: 5
ORDENANZA NÚMERO: 3

SERIE 2024-2025
SESIÓN ORDINARIA

DE LA HONORABLE LEGISLATURA MUNICIPAL DE MAUNABO, PUERTO RICO, PARA APROBAR CUATRO POLÍTICAS INTERNAS ADMINISTRATIVAS PARA EL MANEJO DE FONDOS DE ASISTENCIA PÚBLICA PARA DESASTRES DEL MUNICIPIO AUTÓNOMO DE MAUNABO; Y OTROS FINES.

POR CUANTO: El inciso (c) del Artículo 1.010 de la Ley Número 107 del 14 de agosto de 2020, según enmendada, conocida como "Código Municipal de Puerto Rico", dispone que corresponde a cada Municipio ordenar, reglamentar y resolver cuando sea necesario o conveniente para atender las necesidades locales y para su mayor prosperidad y desarrollo.

POR CUANTO: El Gobierno Municipal de Maunabo entiende que es su responsabilidad y una prioridad gestionar adecuadamente los fondos de asistencia para responder de manera eficaz ante situaciones de desastre y emergencia e implementar medidas que aseguren la eficiencia de recursos en las actividades de asistencia en los desastres. Es necesario contar con políticas claras y de transparencia para la administración de dichos fondos, garantizando su uso adecuado en beneficio del Municipio Autónomo de Maunabo.

POR CUANTO: El Municipio Autónomo de Maunabo, desea adoptar las cuatro políticas que se mencionarán a continuación:

- Personally Identifiable Information PII
- Política sobre el Proceso de Pagos
- Política sobre el Pareo de Fondos
- Política sobre Presentación de Quejas

POR CUANTO: Es meritorio contar con políticas de la Agencia Federal para el Manejo de Emergencias (FEMA), ya que aseguran un desempeño efectivo. Pues las políticas proporcionan directrices claras sobre cómo gestionar fondos y recursos, asegurando que los empleados municipales encargados de trabajar con Proyectos Federales, tenga una referencia y sigan el mismo procedimiento para cumplir con todos los requerimientos necesarios de manera efectiva.

POR TANTO: **ORDÉNESE POR ESTA LEGISLATURA MUNICIPAL DE MAUNABO, PUERTO RICO, REUNIDA EN SESIÓN ORDINARIA HOY 18 DE NOVIEMBRE DE 2024.**

Sección 1ra: Aprobar cuatro políticas fundamentales para el manejo adecuado de los fondos de asistencia pública destinados a desastres, con el fin de garantizar su correcta administración y uso en situaciones de emergencia. Las políticas antes mencionadas son las siguientes:

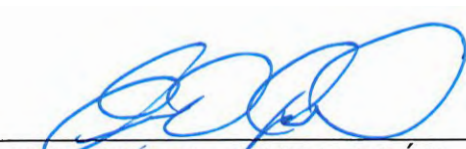
- Personally Identifiable Information PII
- Política sobre el Proceso de Pagos
- Política sobre el Pareo de Fondos
- Política sobre Presentación de Quejas

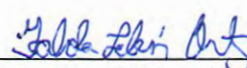
Sección 2da: Cualquier Ordenanza o Resolución que entre en conflicto con la Ordenanza aquí aprobada queda por la presente derogada.

Sección 3ra: Esta ordenanza comenzará a regir inmediatamente después de su aprobación por la Legislatura Municipal y firmada por el Hon. Eric O. Cruz Lebrón, Presidente y del Hon. Angel O. Lafuente Amaro, Alcalde.

Sección 4ta: Copia certificada de la misma será enviada a todas las Oficinas Municipales concernientes para la acción correspondiente.

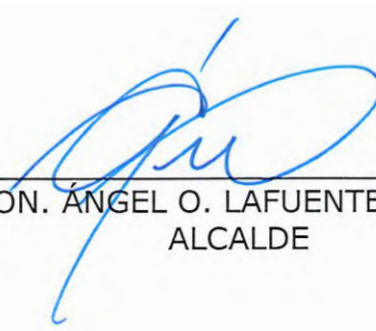
APROBADA POR LA LEGISLATURA MUNICIPAL DE MAUNABO, HOY 18 DE NOVIEMBRE DE 2024, EN MAUNABO, PUERTO RICO.



HON. ERIC O. CRUZ LEBRÓN
PRESIDENTE
LEGISLATURA MUNICIPAL

SRTA. FÁTIMA LEBRÓN ORTIZ
SECRETARIA
LEGISLATURA MUNICIPAL

FIRMADA POR EL ALCALDE EL 20 DE NOVIEMBRE DE 2024.



HON. ÁNGEL O. LAFUENTE AMARO
ALCALDE



CERTIFICACIÓN

Yo, Fabiola Lebrón Ortiz, Secretaria de la Legislatura Municipal de Maunabo, Puerto Rico, CERTIFICO lo siguiente:

ORDENANZA NÚMERO 3 SERIE 2024-2025

De la Honorable Legislatura Municipal de Maunabo, Puerto Rico, para aprobar cuatro políticas internas administrativas para el manejo de fondos de asistencia pública para desastres del Municipio Autónomo de Maunabo; y otros fines.

Es copia fiel y exacta, según aprobada por la Legislatura Municipal en Sesión Ordinaria el día 18 de noviembre de 2024, y con los votos afirmativos de los siguientes Legisladores Municipales:

A Favor: (9)

Hon. Eric O. Cruz Lebrón
Hon. Denise Y. Rodríguez Steidel
Hon. Claribel Vega Nieves
Hon. Mayra L. Soto Vázquez
Hon. José O. Rodríguez Morales
Hon. Victoria García Burgos
Hon. Zoraida Figueroa Álvarez
Hon. Esteban Cruz Sánchez
Hon. Nelson Vázquez Rodríguez

En contra: (0)

Abstentionados: (2)

Hon. Niavelis Castro Meléndez
Hon. Sonia I. Rodríguez Ruiz

Ausentes: (0)

Vacantes: (1)

Firmada por el Hon. Ángel O. Lafuente Amaro, Alcalde del Municipio de Maunabo, el 20 de noviembre de 2024.

Y para que así conste, expido la presente CERTIFICACIÓN en Maunabo, Puerto Rico, hoy 20 de noviembre de 2024.

Srta. Fabiola Lebrón Ortiz
Secretaria
Legislatura Municipal

Personally Identifiable Information (PII)

*MUNICIPALITY
OF MAUNABO*

October 2024

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Scope & Purpose

When Non-Federal Entities ("NFEs") apply for Federal grant funds, they agree to comply with all applicable statutes, regulations, and guidelines. This includes developing policies and procedures specifically tailored to properly manage the Subrecipient's grants disbursed by Central Office for Recovery, Reconstruction and Resiliency ("COR3"). The purpose of this guide is to provide step-by-step guidance and establish the requirements to safeguard all Personally Identifiable Information ("PII"), as set forth in the Privacy Act of 1974, 5 U.S.C. § 552a, as amended, the Code of Federal Regulations ("C.F.R.") and the guidance issued by the Office of Management and Budget ("OMB").

These guidelines apply to all of our employees and contractors who handle, control, or access documents, records, or information technology ("IT") systems that contain PII or information subject to the Privacy Act of 1974.

Overview

In accordance with Title 2 of the C.F.R., §200.303 (e), NFEs must take reasonable measures to safeguard protected PII and other information the Federal awarding agency or pass-through entity designates as sensitive, or that the NFE considers sensitive, consistent with applicable Federal, state, local and/or tribal laws regarding privacy and confidentiality responsibility.

As such, and as subgrantees of the Federal Emergency Management Agency's ("FEMA") Public Assistance ("PA"), and Hazard Mitigation ("HMGP") grant funds, the Municipality of Maunabo is responsible for protecting the privacy of PII. In the course of daily duties, our staff are often exposed or have access to confidential and/or sensitive information. Accordingly, appropriate measures must be taken to ensure authorized access and proper use of documents that may include confidential and/or sensitive information.

Applicable Regulation

- Privacy Act of 1974, 5 U.S.C. § 552a
 - Code of Federal Regulations, 2 C.F.R. Part 200
 - OMB M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017
 - OMB Circular A-130 (Revised): Managing Information as a Strategic Resource
 - Department of Homeland Security ("DHS") Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017
 - Puerto Rico Government Open Data Act, Act No. 122-2019
-

Definitions

1. **Applicant:** a non-Federal entity applying for assistance under the Recipient's Federal award.
2. **Breach:** the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for other than the authorized purpose. *See page 9 (C) of OMB M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017).*
3. **Breach Response Plan:** formal document that includes the entity's policies and procedures for reporting, investigating, and managing a breach; it should be specifically tailored to the entity and address the entity's mission, size, structure, and functions. An entity's breach response plan shall be part of the entity's formal incident response plan. *See page 15 (VII) of OMB M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017).*
4. **Contract:** for the purpose of Federal financial assistance, a legal instrument by which the Municipality of Maunabo purchases property or services needed to carry out the project or program under a Federal award. For additional information on Subrecipient and contractor determinations. *See 2 CFR § 200.331 and § 200.1.*
5. **Contractor:** an entity that receives a contract as defined in 2 CFR § 200.1
6. **Federal Awarding Agency:** Federal agency that provides a Federal award directly to a non-Federal entity.
7. **Information Technology ("IT"):** (1) with respect to the Municipality of Maunabo as an entity, means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the entity, if the equipment is used by the entity directly or is used by a contractor under a contract with us that requires the use (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (2) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but (3) does not include any equipment acquired by a Federal contract incidental to a Federal contract. *See page 5 (1.4.11) DHS Sensitive Systems Policy Directive 4300A, version 13.1, July 27, 2017.*
8. **Personally Identifiable Information ("PII"):** information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the entity shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available - in any medium or from any source - that would make it possible to identify an individual. *See page 8 (B) OMB M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017).*
9. **Protected Personally Identifiable Information ("Protected PII"):** an individual's first name or first initial and last name, in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts.

This does not include PII that is required by law to be disclosed. *See also the definition of Personally Identifiable Information (PII) in this section. See 2 CFR § 200.1.*

10. **Public Data:** information documented, or to be documented, by a public servant from the Municipality of Maunabo or by a third party authorized by law or by the public servant; includes any document, whether in physical or electronic form, which is originated, retained or received by any governmental body in accordance with law or in connection with the conduct of public affairs, and which is required to be retained as evidence of transactions or their legal value, in accordance with the provisions of Act No. 5 of December 8, 1955, as amended, known as the "*Public Records Management Act of Puerto Rico*"; also includes all information of public origin, or that arises from the exercise of public authority, or as a result of the use of public authority, or as a product of the use of public resources or public authority, directly or indirectly delegated. It includes documents, data, any other type of visible electronic information, or any other similar information detailing the product of public initiative or management, the use of public resources, and the exercise of the Municipality's authority, directly or indirectly delegated. Personnel files or any information of this nature will not be Public Data. At the time of submitting any data that is understood to be public, the Municipality of Maunabo shall ensure that it takes the necessary safeguards so as not to include any type of information or data of this nature, include any type of information or data that may contain information that is confidential, prohibited by law, or that is within the prohibited by any law, or that falls within any of the exceptions set forth in Article 4 of the Puerto Rico Government Open Data Act. *See Article 3 (c) of Puerto Rico Government Open Data Act, Act 122-2019.*
11. **Recipient:** non-Federal entity that receives a Federal award directly from a Federal awarding agency to carry out an activity under a Federal program; it does not include Subrecipients. *See 2 CFR § 200.69.*
12. **Record:** any item, collection, or grouping of information about an individual that is maintained by the Municipality, including, but not limited to, their education, financial transactions, medical history, and criminal or employment history, and that contains their name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph. *See The Privacy Act of 1974 as amended, 5 U.S.C. § 552a (a) definitions (4).*
13. **Routine use:** with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. *See the Privacy Act of 1974, as amended, 5 U.S.C. § 552a (a) definitions (7).*
14. **Sensitive Information:** any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. *See page 7 (1.4.19) of DHS Sensitive Systems Policy Directive 4300A, version 13.1, July 27, 2017.*
15. **Sensitive PII ("SPII"):** PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. *See page 7 (1.4.20) DHS Sensitive Systems Policy Directive 4300A, version 13.1, July 27, 2017.*
16. **Subrecipient:** entity, usually but not limited to non-Federal entities, that receives a subaward from a pass-through entity to carry out part of a Federal award, but does not include an individual that is a beneficiary of such award. The Municipality of Maunabo is to be considered that entity. And as such, may also be a Recipient of other Federal awards directly from a Federal awarding agency. *See 2 CFR § 200.1.*

17. **System of records:** group of any records under the control of any agency or entity from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. *See the Privacy Act of 1974, as amended, 5 U.S.C. § 552a (a) definitions (5).*

Guidelines

Responsibility to Safeguard PII

As set forth in 2 C.F.R. § 200.303 (e), the Municipality of Maunabo shall take reasonable measures to safeguard protected PII and other information the Federal awarding agency (FEMA) or pass-through entity (COR3) designates as sensitive, or the non-Federal entity considers sensitive consistent with applicable Federal, State, local, and/or tribal laws regarding privacy and responsibility over confidentiality.

Categorizing Personally Identifiable Information (“PII”)

As FEMA PA and HMGP subgrantees, the Municipality of Maunabo may collect, maintain, use, retrieve and disseminate information that may contain PII and SPII.

As established on OMB memorandum M-17-12, the term PII refers to “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual”. Likewise, DHS Sensitive Systems Policy Directive 4300A of 2017, defines SPII as “PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual”.

As such, SPII requires stricter handling guidelines because of the increased risk to an individual or entity if the data is inappropriately accessed or compromised. Some categories of PII are sensitive as stand-alone data elements, including social security number and driver’s license, state identification number, Alien Registration Numbers, financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII.¹

The tables below show examples of PII and SPII and how they may become more sensitive.

PII	Stand-alone sensitive PII
Name	Social security number
Work e-mail	Driver’s license or state ID numbers
Address	Passport numbers
Phone number	Alien Registration numbers
---	Biometrics identifiers

¹ United States Homeland Security Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007, Rev. 3 Page 5, December 4, 2017, and United States Homeland Security Sensitive Systems Handbook, version 12.0, November 15, 2015.

Any grouping of information that contains an individual's name or other unique identifier with the following elements, becomes SPII:

Citizenship or immigration status - Medical information - Ethnic or religious affiliation - Account passwords - Last 4 digits of the SSN - Date of birth - Criminal History – Personal Identification Numbers (PIN) – Bank account numbers

SPII Breach

A privacy incident or breach is defined by OMB Memorandum M-17-12 as the actual or potential loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or access to SPII, in physical or electronic form. A breach occurs primarily when employees fail to use appropriate controls while accessing, using, or sharing SPII, or when they use SPII for unauthorized purposes.

Per OMB Memorandum M-17-12, common examples of a breach include:

- a laptop or portable storage device storing PII is lost or stolen;
- an email containing PII is inadvertently sent to the wrong person;
- a box of documents with PII is lost or stolen during shipping;
- an unauthorized third party overhears the entity's employees discussing an individual seeking employment or information related to Federal assistance programs;
- a user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;
- an IT system that maintains PII is accessed by a malicious actor; and
- PII that should not be widely disseminated is posted inadvertently on a public website.

SPII Collection

As established in the Privacy Act of 1974 and OMB Circular No. A-130, to ensure compliance with PII regulations, the collection of SPII should be limited to the intended purposes. Furthermore, this information should not be collected or maintained without the proper authorization.

When collecting or maintaining SPII, the Municipality of Maunabo's staff shall ensure they have the legal authority to do so and limit their access to only the SPII necessary to perform their duties; staff shall not view or use SPII for any purpose other than to perform their duties. The collection, maintenance, use, and dissemination of Social Security numbers, Employer Identification numbers, income information, or any information derived of the former, shall be conducted, to the extent applicable, in accordance with the Privacy Act and all other applicable provisions of Federal, state, and local Law.

Staff shall only retain in their records PII that is relevant and necessary to fulfill the entity's purpose as required by law or the President's executive order.

Using, Sharing, and Protecting SPII

In accordance with the Privacy Act of 1974, Section (b) Conditions of Disclosure, no record contained in a system of records shall be disclosed by any means of communication to any person or another agency or entity, except pursuant to a written request or with prior written consent of the individual to whom the record pertains, unless the

disclosure of the record would be:

- To officers and employees of the entity that maintains the record and have a need for the record in the performance of their duties;
- Required under section 522 of the Privacy Act of 1974;
- For routine use;
- To the United States Census Bureau for purposes of planning or conducting a census or survey, or related activity;
- To a Recipient who has provided the entity with written assurance that the record will only be used as statistical research or information record, and the record is transferred in a form that is not individually identifiable;
- To the National Archives and Records Administration as a record with sufficient historical or other value to warrant continued retention;
- To an agency or instrumentality under control of the United States, for a civil or criminal law enforcement activity that is authorized by law and has a written request by the head of the entity to the agency or instrumentality that maintains the record, specifying the particular information sought;
- To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual, if following such disclosure a notice is transmitted to the last known address of such individual;
- To either House of Congress;
- To the Comptroller General;
- Pursuant to the order of a court with competent jurisdiction;
- To a consumer reporting agency;

Routine use is an exception that permits some limited disclosure of PII without the individual consent from the applicant. Routine uses must be consistent with the reason why the entity collects the information, which may include government process, oversight and management, or disaster coordination; as such, routine may not be issued for any reason.

Routine use also allows for information sharing with external partners to enable them to provide benefits and services, sharing with Federal, state, and local governments in support of mitigation activities, and other information sharing for necessary governmental activities such as audits.

Additionally, to avoid duplication of benefits, the entity may disclose PII to a third party for implementation of hazard mitigation measures, including planning and enforcement of hazard specific provisions of building codes and ordinances.

Protection of SPII

To ensure the protection of digital SPII, staff shall have to login their password-protected computers and ensure documents are not accessible to casual visitors, passersby, or other individuals within the office without a "need to know basis." If an employee leaves his/her work area for any reason or at the end of his/her shift, the password-protected computer must be activated, or the laptop closed.

In addition, staff shall ensure privacy during intra-office or telephone conversations related to confidential information and/or SPII.

The most common PII incidents/breaches are disclosure of information via email, theft or loss of laptops and other computer gear, and system compromise/unauthorized access. To avoid these, or any other type of PII breach, the

following guidelines must be followed:

1. Appropriate use of email for sharing SPII

a. Sending SPII inside or outside of the entity:

- When sending SPII outside of the entity by email, it shall be stored in a separate document and be password-protected or encrypted. The encrypted document must be sent as an attachment to the email and the password must be provided to the Recipient in a separate email or by phone.

- Emails shall contain a Confidentiality Notice at the bottom. An example of the notice is included below:

"CONFIDENTIALITY NOTICE: This transmission is confidential and intended solely for the person to whom it is addressed. It may contain privileged and confidential information. If you are not the intended recipient, you should not copy, distribute, or take any action in reliance on it. If you believe that you have received this transmission in error, please notify the sender."

"AVISO DE CONFIDENCIALIDAD: Este envío es confidencial y está destinado únicamente a la persona a la que ha sido enviado. Puede contener información privada y confidencial. Si usted no es el destinatario al que ha sido remitida, no puede copiarla, distribuirla ni emprender con ella ningún tipo de acción. Si cree que lo ha recibido por error, por favor, notifique al remitente."

b. Staff shall never send SPII to a personal email account or from a personal email account:

- If an employee needs to work with SPII outside of the workplace, they must access it through the VPN on their official laptop.

2. Protection of hard copy SPII

Personnel should not leave SPII unattended on desks, printers, fax machines, or photocopiers. SPII shall be kept in a locked desk drawer, file cabinet, or similar locked enclosure when not in use. If an employee is working with SPII, it should be kept in an area where access is controlled and limited to people on an official need-to-know basis. To the extent possible, faxing SPII should be avoided.

3. Proper use of the U.S. mail and other regular mailing options to share SPII

SPII stored on CDs, DVDs, hard drives, USB flash drives, or other removable media, must be encrypted before mailing or sharing. It's not recommended that a paper document containing SPII be sent by regular mail; SPII should be sent in messenger or courier envelopes if it is an internal communication or sealed in an opaque envelope or container and mailed using a traceable commercial delivery service such as UPS or FedEx, if it is an external communication.

4. Safeguarding media

SPII shall only be saved, stored, or hosted on portable electronic devices ("PEDs") previously approved by the entity, such as laptops, USB flash drives, and external hard drives, all of which must be encrypted. No personally owned computers or USB flash drives should be used, unless authorized by IT personnel.

If a laptop or PED needs to be transported and left in a car, it should be stored in the trunk, out of sight, and not left overnight. In the event of theft or loss of the laptop or PED, it must be reported immediately as a lost asset according to the entity's PII Incident Response Plan.

5. Posting SPII on websites and shared drive clouds

SPII shall not be posted on the Internet (including social networking sites), on shared drive clouds other than the entity's preferred file sharing and/or storage service, or on multi-access calendars that can be accessed by individuals not on a need-to-know basis.

6. Social engineering/phishing

Staff should be alert to any phone calls or emails from individuals claiming to be entity employees or COR3 employees, and/or contractors who attempt to obtain personal or non-public information or ask to verify such information.

a. The following are recommendations on how to handle phishing email accounts:

- Do not open suspicious messages on any of your devices, including computer, mobile/cell phone, or Outlook via web ("OWA").
- Do not click on links/links contained in unknown or unexpected emails.
- Delete the message from your Inbox and Deleted Items.
- If you clicked on any link included in the referral email, notify immediately by email to the entity's IT or technical support personnel.
- Report any unusual or suspicious situation with your computer or device via email to the entity's IT or technical support personnel.
- If you receive any other suspicious or potentially malicious email, refer it to the entity's IT or technical support personnel.

7. Sharing usernames and/or passwords

Staff must not share account information, especially logins or passwords, with anyone. Login or password information must not be accessible to others (e.g., a sticky note with the password on a computer). Passwords should not remain in effect longer than ninety (90) days.

8. Remote working and personal computers

Staff must not transfer files to their home computer and/or personal laptops or print entity records on their home printer. Staff should never use their personal email account to conduct official business. Controls should be implemented to ensure that only authorized persons can participate in each video conference.

Process for Sharing Documentation that Contains PII

In cases where PII sharing is not permitted, COR3 contractors and the Municipality of Maunabo shall take additional steps to ensure the protection of PII. It is the entity's responsibility to remove all PII related to its Federal funds prior to sharing the documentation. As such, COR3 is not responsible for protecting PII shared by the Municipality. The process for removing PII is as follows:

1. Verify every document to be e-mailed, uploaded to a system, platform, cloud or storing and/or sharing service (like COR3's Disaster Recovery Solution system, "DRS") and/or shared in any way.
2. If the documentation to be shared contains PII, it must be redacted. An illustration of a redacted document is shown below.

[illegible]

Access to Records

In compliance with the Privacy Act of 1974, (d), (j), (k), an agency that maintains a system of records, shall permit any person to have access to its records or any information relating to them unless one of the following exemptions applies:

1. Information compiled in reasonable anticipation of a civil action or proceeding;
2. Whether the system of records is maintained by the Central Intelligence Agency;
3. Whether the system of records is maintained by an agency, or component thereof, that performs law enforcement activities;
4. Whether the system of records is classified information;
5. Whether the system of records is investigative material collected for law enforcement;
6. Whether the system of records is maintained in connection with the provision of protective services to the President of the United States or other persons pursuant to section 3056 of Title 18;
7. Whether the system of records is required by law to be maintained and used solely as statistical records;
8. Whether the system of records is investigative material compiled solely for the purpose of determining suitability, eligibility or other qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence;
9. Whether the system of records is testing, or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service;
10. Whether the system of records is evaluation material used to determine potential for promotion in the armed services.

Likewise, Article 4 of Act 122 of 2019, the Puerto Rico Government Open Data Act, provides that state entities must disclose their public data unless a confidentiality or privilege is alleged under a law, it is a privilege under the rules of evidence, an allegation that a fundamental right of third parties may be injured, and/or a confided identity or official information may be disclosed, as established by Rule 514 of the Puerto Rico Rules of Evidence.

Other exceptions to disclosure of public data, per Act 122, are information classified as national security, internal personnel rules or practices of a government entity, or internal communications between state entities, as well as public information for which applies any of the privileges recognized in the United States Constitution or the Constitution of the Commonwealth of Puerto Rico, applicable laws and Rules of Evidence, including official information and official-decisional information in deliberative proceedings on public policy, as recognized by case law.

Disposition of SPII

SPII, including that found in archived emails, shall be disposed of when no longer needed, in accordance with applicable records disposition schedules. If destruction of SPII is required, the following steps shall be followed:

- Shred documentation containing SPII; do not recycle or deposit it in garbage containers. Staff shall be especially vigilant during office moves and transition periods when large numbers of records are at risk.
- Before transferring a computer or PED to another employee, ask IT personnel to wipe SPII from computer drives and other electronic storage devices in accordance with the component's information security standards.

Termination of Personnel

Staff termination process shall involve Human Resources, Administration, IT, the corresponding division/department director, and any other identified divisions/departments that has or has had access to any system of records. Access to this system of records, like DRS account, FEMA Grants Portal account and Outlook account, among others, shall be properly deactivated. The Municipality of Maunabo shall be responsible for requesting this deactivation, including, if applicable, their contractors' and employee's mobile phone if it had access to PII. This will be completed by the POC.

During the termination process:

- The importance of confidentiality should be reinforced.
- Information in the contractors' and/or employee's possession shall be requested.
- Devices such as tablets, laptops, PEDs and USB flash storage devices shall be requested and collected.
- Keys, ID cards, badges and any other access device shall be collected.

Reporting Privacy Incidents

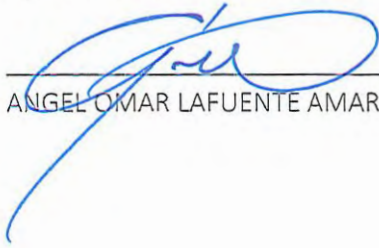
As stated in OMB M-17-12, each agency or entity shall require all persons with access to information systems or system of records to report suspected or confirmed breaches as soon as possible and without unreasonable delay. Staff shall not wait until it is confirmed that a breach has occurred to report it, as such a delay may impair the ability to implement preventive and corrective measures to protect PII. As such, staff shall promptly notify privacy incidents or breaches to their immediate supervisor. If the supervisor is not available, or if there is a potential conflict of interest, the division/department director, administrator, or any other leadership personnel shall be informed of the incident. Records and documentation of the information and actions related to the incident shall be maintained.

The incident report must contain:

- The person or entity who was responsible for the incident.
- The person or entity who was harmed by the incident, if any.
- The date and time that the incident occurred.
- The date and time that the incident was detected.
- The date and time that the incident was reported.
- How the information was accessed.
- How the incident was detected.

To facilitate prompt notification of a suspected or confirmed breach to staff, the entity shall establish a dedicated incident response email and develop and implement an Incident Response Plan.

Approved on this 2nd day of October, 2024 by the Mayor Angel Omar Lafuente Amaro.



ANGEL OMAR LAFUENTE AMARO

POLÍTICA SOBRE EL PROCESO DE PAGOS

Proceso de Pagos - 2 CFR 200.305

Esta Política explica cómo se deben utilizar los fondos federales que recibe el Municipio de Maunabo. Las reglas están diseñadas para asegurar que los fondos se utilicen de manera eficiente y cumpliendo con los requisitos de las agencias federales que otorgan estos fondos.

- a) Tomando en cuenta que el Municipio Autónomo de Maunabo es una entidad no estatal para el 2 CFR 200.305, debe seguir los acuerdos y procedimientos específicos establecidos por el Tesoro de los Estados Unidos, como el Treasury-State Cash Management Improvement Act (CMIA), así como el Capítulo 7 para Pagos del COR3. Estos acuerdos aseguran que los fondos sean recibidos y utilizados a tiempo y de manera adecuada.
- b) Para las entidades no estatales, los métodos de pago deben minimizar el tiempo entre la transferencia de fondos desde el Tesoro de los Estados Unidos o la entidad intermediaria (quien pasa los fondos), y el desembolso por parte del Municipio. Esto aplica tanto si el pago se realiza mediante transferencia electrónica de fondos, emisión o redención de cheques, órdenes de pago o cualquier otro medio.

Además, las agencias federales requieren que el Municipio como subreceptor de estos fondos utilicen únicamente solicitudes de pago aprobadas por la Oficina de Gestión y Presupuesto (OMB), que son de uso general para todas las entidades gubernamentales.

- 1) Métodos de pago:
 - i. Pago por adelantado:
 - ii. La entidad debe demostrar capacidad para manejar fondos adecuadamente.
 - iii. Los adelantos deben limitarse al mínimo necesario.
 - iv. Deben coincidir lo más posible con los gastos reales del proyecto.
 - v. La entidad debe pagar a tiempo a sus contratistas.
- 2) Cuentas de depósitos: El Municipio, como Subreceptor, mantendrá los anticipos de fondos federales en cuentas de depósitos aseguradas. Deberá estar dispuesto a proveer información sobre los fondos obligados, los fondos recibidos y los fondos gastados que correspondan a cada desastre declarado por el cual hayan aceptado una subvención. A continuación, ejemplos:
 - i. Por desastre: DR 4339 y DR 4671
 - ii. Por tipo de subvención: FEMA PA, FEMA Mitigación, HUD, CDBG-DR, etc.
- 3) Adelantos: Si el Municipio tiene los procedimientos y sistemas financieros adecuados para garantizar el uso correcto del dinero, puede recibir los fondos antes de necesitarlos, pero solo en las cantidades mínimas requeridas para cumplir con los proyectos. Deberá mantener un registro acumulativo de todos los fondos adelantados. También cumplirá con las guías y políticas establecidas para el manejo de esos fondos.
- 4) Devolución de fondos: El Municipio devolverá aquellos fondos que no cumplan con el programa o que la entidad federal y/o el COR3, el Department of Homeland Security (DHS), FEMA y/u otra

entidad federal monitorea que determine que el pago fue impropio. Los fondos reembolsados por el Municipio al COR3 serán devueltos a la agencia federal mediante el Federal Department of Health and Human Services Payment Management System (PMS). El Municipio reconoce que el incumplir la devolución de los fondos requeridos en un término de treinta (30) días a partir de la Notificación de Cobro ('Notice of Collection'), podrá estar sujeta a medidas por el COR3, tales como:

- i. Retención de fondos elegibles a pagos a favor del Municipio;
 - ii. Referido al trámite de exclusión y suspensión de la agencia federal que provea la subvención;
 - iii. Referido a la Agencia Federal para la retención de otras subvenciones para proyectos y/o programas;
 - iv. Referido a la Agencia Federal para la retención de subvenciones para futuros desastres;
 - v. Iniciar otras medidas legales disponibles; y/o
 - vi. Aumentar la clasificación del Municipio como entidad riesgosa.
- 5) Retención de pagos:
- i. Solo permitida en casos específicos, como incumplimiento de objetivos o deudas pendientes con EE.UU.
 - ii. Los pagos deben reanudarse cuando se corrijan las condiciones.
- 6) Adelantos de Capital de Trabajo: Si el Municipio no tiene suficiente capital de trabajo para cubrir los costos iniciales, puede recibir fondos como anticipos para cubrir las necesidades inmediatas, recibiendo más dinero según avance la ejecución del

proyecto. El Municipio cumplirá las guías establecidas para el Programa de Anticipo, hará los reembolsos dentro de los términos aplicables y proveerá los informes requeridos por el COR3, según sea necesario.

7) Intereses ganados: Como Subreceptor de fondos de asistencia pública para desastres y de mitigación, el Municipio debe mantener los adelantos recibidos con fondos federales en cuentas de depósito que generan intereses, excepto que aplique lo siguiente:

- i. El Municipio recibirá menos de \$250,000.00 anuales en fondos federales;
- ii. La mejor cuenta de depósitos disponible no generará intereses en exceso de \$500.00 anuales por esos fondos federales; o
- iii. La institución depositaria requerirá un balance promedio o mínimo tan alto que no es conveniente para los depósitos esperados por fondos federales e ingresos propios en efectivo.

De los intereses generados en dichas cuentas de depósitos, el Municipio podrá retener la suma de \$500.00 para atender los gastos administrativos. Cualquier interés adicional generado por los adelantos de fondos federales serán remitidos anualmente al COR3 y/o al Department of Health and Human Services Payment Management System (PMS) conforme a la política y las instrucciones aplicables.

Aprobado internamente en Maunabo, Puerto Rico el 2 de octubre de 2024.


Ángel Omar Lafuente Amaro
Alcalde

PO BOX 8 MAUNABO, PUERTO RICO 00707 | 787.861.0825 / 787.861.0333 EXT. 1002 | alcalde@maunabopr.com



Municipio de Maunabo, no discrimina de ninguna manera por razón de edad, raza, color, sexo, nacimiento, condición de veterano, ideología política o religiosa, origen étnico, condición social, orientación sexual o identidad de género, discapacidad o impedimento físico o mental; ni por ser víctima de violencia doméstica, agresión sexual o acoso.



POLÍTICA SOBRE EL PAREO DE FONDOS (Cost Sharing or Matching) - 2 CFR 200.306

Page | 1

El pareo de fondos o "Cost Sharing" es un mecanismo que permite que una entidad no federal, como el Municipio de Maunabo, contribuya con recursos propios o de terceros para cumplir con los requisitos financieros de un proyecto financiado con fondos federales. A continuación, se detalla una guía en base a los principios del 2 CFR 200.306 para asegurar su cumplimiento:

Principios Generales:

En las propuestas de Fondos Federales, no se requiere el aporte voluntario de fondos compartidos. Este no se utilizará como criterio durante la evaluación de mérito de las solicitudes, salvo que esté en conformidad con las regulaciones de la agencia federal otorgante y se especifique en la convocatoria de financiamiento. Los criterios para evaluar el aporte voluntario de fondos compartidos, así como cualquier otro factor de política del programa, deben estar claramente detallados en la convocatoria de financiamiento. Ver también §§ 200.414 y 200.204, y el apéndice I de esta sección.

1. Criterios para aceptar costos compartidos:

Para todos los premios federales, los costos compartidos o fondos de pareo, incluyendo contribuciones en efectivo o en especie de terceros, deben cumplir con los siguientes criterios para ser aceptados:

- Son verificables en los registros de la entidad no federal.
- No se usan como contribución para otro premio federal.
- Son necesarios y razonables para cumplir los objetivos del proyecto o programa.
- Son permitidos bajo las reglas de la subparte E.
- No son pagados por el Gobierno Federal bajo otro premio, a menos que una ley lo permita.
- Están incluidos en el presupuesto aprobado, cuando sea requerido.
- Cumplen con otras normativas aplicables.

Los costos indirectos no recuperados, incluidos los relacionados con el pareo de fondos, solo pueden incluirse con la aprobación previa de la agencia federal. Los costos indirectos no recuperados son la diferencia entre lo que se cobró al premio federal y lo que se podría haber cobrado según la tasa aprobada de la entidad no federal. Los valores de las contribuciones de servicios y propiedades de una entidad no federal deben establecerse según las reglas de costos de la subparte E del 2 CFR 200.

PO BOX 8 MAUNABO, PUERTO RICO 00707 | 787.861.0825 / 787.861.0333 EXT. 1002



El Municipio de Maunabo, no discrimina de ninguna manera por razón de edad, raza, color, sexo, nacimiento, condición de veterano, ideología política o religiosa, origen étnico, condición social, orientación sexual o identidad de género, discapacidad o impedimento físico o mental; ni por ser víctima de violencia doméstica, agresión sexual o acoso.



MAUNABO
- COSTA DEL SOL NACIENTE -

Si una agencia federal autoriza a donar edificios o terrenos para proyectos de construcción o uso a largo plazo, el valor de la propiedad donada para el pareo de fondos debe ser el menor entre:

- El valor restante de la propiedad según los registros contables de la entidad al momento de la donación.
- El valor actual de mercado, aunque con suficiente justificación, la agencia federal puede aprobar usar el valor de mercado actual.

Page | 2

Cuando una organización externa proporciona los servicios de un empleado, estos deben valorarse según su salario regular más los beneficios y costos indirectos, siempre que se utilicen las mismas habilidades por las que normalmente se le paga. Si los servicios donados se consideran costos indirectos, deben separarse para no recibir reembolso por ellos.

Las donaciones de propiedad de terceros pueden incluir equipos, suministros de oficina o de laboratorio. El valor de la propiedad donada no debe exceder su valor de mercado en el momento de la donación.

Para equipos, edificios o terrenos donados en los que la entidad no federal recibe la propiedad, el método de valoración puede cambiar según el objetivo del premio federal:

Si el objetivo es adquirir estos activos, el valor total de la donación se puede usar para el pareo de fondos.

Si el objetivo es usar estos activos, solo se pueden contabilizar los cargos por depreciación, salvo que la agencia apruebe el uso del valor de mercado.

El valor de la propiedad donada debe establecerse según las políticas contables de la entidad no federal, con algunas condiciones:

- El valor de terrenos y edificios no debe exceder su valor de mercado, certificado por un tasador independiente.
- El valor del equipo no debe superar el de equipos similares en la misma condición.
- El valor del espacio donado no debe exceder el alquiler justo de un espacio similar en la misma área.
- El valor de equipo prestado no debe exceder su alquiler justo.

Finalmente, las contribuciones en especie de terceros deben documentarse y valorarse según los mismos métodos que la entidad no federal usa para sus propios bienes y servicios.

Cordialmente,



Ángel Omar Lafuente Amaro
Alcalde

Aprobado en Maunabo, Puerto Rico,
Miércoles, 2 de octubre de 2024.

PO BOX 8 MAUNABO, PUERTO RICO 00707 | 787.861.0825 / 787.861.0333 EXT. 1002



El Municipio de Maunabo, no discrimina de ninguna manera por razón de edad, raza, color, sexo, nacimiento, condición de veterano, ideología política o religiosa, origen condición social, orientación sexual o identidad de género, discapacidad o impedimento físico o mental; ni por ser víctima de violencia doméstica, agresión sexual o asedio.

The coat of arms of Maunabo is partially visible on the left side of the page. It features a purple stone wall with green arched windows at the top. Below this is a green shield containing a white lighthouse on the left and a yellow dollar sign with a white treble clef on the right. The bottom of the shield is a large green chevron. At the very bottom of the page, there is a horizontal bar with four colored squares (orange, yellow, red, green) followed by a long blue rectangle.

**GOBIERNO DE PUERTO RICO
MUNICIPIO AUTÓNOMO DE MAUNABO**

POLÍTICA SOBRE PRESENTACIÓN DE QUEJAS

The logo for Maunabo features a stylized map of the municipality above the word "MAUNABO" in green capital letters. Below the name is the tagline "- COSTA DEL SOL NACIENTE -" in orange capital letters.

MAUNABO
- COSTA DEL SOL NACIENTE -

Índice

1	Propósito.....	3
2	Definiciones/Siglas	3
3	Política.....	4
4	Quejas	5
	Requisitos para la presentación de quejas	5
	Envío de quejas.....	6
5	Responsabilidades	7
6	Investigación de la queja.....	7
7	Referidos.....	7
8	Registros	8
9	Medidas cautelares.....	8

1 Propósito

Esta política describe la responsabilidad del Municipio de Maunabo, como recipiente de subvenciones con fondos CDBG/MIT, fondos de Mitigación y fondos de Asistencia Pública para Desastres del COR3 y FEMA, de garantizar que todas las quejas se atiendan con prontitud y de manera uniforme y que, como mínimo y en la medida posible, se brinde una respuesta sustancial y oportuna a todas las quejas presentadas por escrito, en un plazo de **quince (15) días laborables**. 24 C.F.R. § 91.115(h).

Por consiguiente, el objetivo de esta Política es servir de guía para la supervisión responsable, eficiente y transparente de las quejas de los ciudadanos mediante la implementación de una estructura que organice adecuadamente las políticas y los sistemas necesarios para cumplir con dicha responsabilidad. De igual forma, esta Política alienta a las personas a expresar sus inquietudes con respecto a cualquier asunto relacionado con la administración general de sus fondos propios y aquellos provenientes de fondos federales, de manera que se atiendan sus quejas y que se tome acción según corresponda.

2 Definiciones/Siglas

Auditoría Interna – Oficina del Municipio que ayudará y dará apoyo a las respuestas a las quejas de los ciudadanos, además de recopilar información y documentación relevante.

CDBG-DR - fondos de la Subvención en Bloque para Desarrollo Comunitario y Recuperación ante Desastres.

CDBG-MIT – fondos de la Subvención en Bloque para Desarrollo Comunitario y Mitigación.

Confidencialidad – La protección de información personal o delicada, según se define en la Política sobre Información de Identificación Personal, Confidencialidad y No Divulgación.

COR3 – Central Office for Recovery, Reconstruction, and Resiliency

FEMA – Federal Emergency Management Agency

HUD – Se refiere al Departamento de Vivienda y Desarrollo Urbano de los Estados Unidos.

Plan de Acción – Una descripción exhaustiva sobre un proyecto que incluye sus actividades, logros, fuentes de financiamiento y usuarios de los fondos.

POC – Siglas en inglés para “Punto de Contacto”.

Política AFWAM (por sus siglas en inglés) – Política Anti-Fraude, Desperdicio, Abuso o Malversación.

Política de Retención de Documentos - Política sobre Manejo, Administración y Accesibilidad de Documentos.

Política de PII (por sus siglas en inglés) - Política de confidencialidad, información de identificación personal y no divulgación.

Queja – Una declaración formal presentada por escrito con relación a un agravio, la cual será documentada, procesada, archivada y se contestada de acuerdo con lo estipulado en 24 C.F.R. § 91.115(h).

Quejas anónimas - quejas con datos insuficientes y/o enviadas por un tercero sin legitimación en el asunto que se presenta y que no necesitan ser aceptadas o revisadas.

Quejoso – Toda persona natural o legal y/o su representante autorizado que presente una queja. También se conoce como la “persona agraviada” o la persona que está sujeta a la situación que es el fundamento de la queja.

Vivienda – Se refiere al Departamento de la Vivienda de Puerto Rico.

3 Política

Como parte de sus esfuerzos para promover la participación ciudadana, el estatuto federal que rige a los programas CDBG-DR/MIT de Vivienda, Mitigación y de Asistencia Pública para Desastres de FEMA y administrados por el COR3, requiere que los gobiernos locales “[p]roporcionen a los ciudadanos la dirección, el número de teléfono y los horarios en los cuales pueden presentar quejas y agravios, además de responder prontamente por escrito a las quejas y agravios presentados por escrito, en un plazo de **quince (15) días laborables**, en la medida de lo posible”. 24 C.F.R. § 570.486(a)(7).

Tanto, el Vol. 83 Núm. 28 del Registro Federal (9 de febrero de 2018), 83 FR 5844, como el Vol. 84 Núm. 169 del Registro Federal (30 de agosto de 2019), 84 FR 45838, introdujeron la exención al requisito de participación ciudadana (lo cual incluye el estatuto antes mencionado) y requisitos alternativos. No obstante, conservan la estipulación sobre los **quince (15) días**: “[e]l destinatario de los fondos responderá prontamente por escrito a todas las quejas de los ciudadanos. Dicha respuesta debe emitirse dentro de **quince (15) días laborables** a partir del recibo de la queja”. 83 FR 5844, 5855; 84 FR 45838, 45854.

Las personas tienen derecho a expresar sus opiniones y sus posturas en cualquier

momento durante el desarrollo y la implementación de los programas CDBG-DR/MIT, Mitigación y Asistencia Pública para Desastres de FEMA y administrados por COR3.

El Municipio de Maunabo implementa esta Política para atender las quejas recibidas con prontitud y de manera responsable y confidencial. Se mantendrá la confidencialidad de la identidad y las circunstancias del querellante, a menos que se obtenga autorización previa del participante por escrito. Al responder a una queja, el Municipio de Maunabo tratará a los ciudadanos de manera justa y con cortesía. El objetivo de esta política es atender los asuntos de una manera que muestre sensibilidad hacia las necesidades del querellante y que sea completamente compatible con las leyes, reglamentos, códigos y ordenanzas federales y locales.

La política de no discriminación incluye el proceso de admisión y manejo de quejas. El Municipio de Maunabo no discrimina por razón de raza, color, creencias religiosas, creencias políticas, afiliación a uniones laborales, sexo, orientación sexual, género, discapacidad, situación familiar, estado civil, origen nacional o cualquier otro factor injustificado, por ejemplo: dificultades con el idioma, edad, embarazo, etc.

Ninguna persona podrá intimidar, amenazar, coaccionar o discriminar en contra de otra persona por haber presentado una queja, testificado, ayudado o participado en algún asunto, investigación, procedimiento o vista relacionada con una queja.

4 Quejas

Durante el transcurso de la ejecución de los programas con fondos propios y fondos federales, tales como: CDBG-DR/MIT, Mitigación y Asistencia Pública para Desastres de FEMA y administrados por el COR3, es posible que los ciudadanos deseen presentar quejas por escrito mediante una declaración de agravio. El Municipio de Maunabo aceptará quejas sobre cualquier asunto relacionado con la administración general del Programa. Cualquier persona y/o su representante autorizado puede presentar una queja.

Requisitos para la presentación de quejas

Para que la Oficina de Auditoría Interna pueda procesar y revisar una queja, debe cumplir con los siguientes requisitos:

1. La queja debe presentarse por escrito.
2. Debe tener el nombre completo del querellante.
3. Debe incluir la información de contacto del querellante y el método preferido para recibir comunicaciones relacionadas con la queja (teléfono, en persona, por correo o por correo electrónico).

4. Debe indicar la naturaleza de la queja (Programa(s) CDBG-DR/MIT, Mitigación y/o Asistencia Pública para Desastres / Otro, por favor, especifique).
5. Debe incluir un resumen de la queja y el remedio solicitado.
6. Debe indicar los nombres de las personas con las que se comunicó anteriormente con relación a la queja (Personal de los programas CDBG-DR/MIT, Mitigación y/o Asistencia Pública para Desastres / Gerente de proyecto / Personal de Municipio de Maunabo / y / u otra persona, si corresponde).
7. Debe incluir pruebas o documentación de apoyo.

Los requisitos 1 al 5 son obligatorios. El querellante o una persona autorizada por el querellante debe presentar la querella. Toda persona que presente una queja a nombre de otra persona o entidad debe presentar la documentación adecuada que confirme que tiene autoridad para representar al querellante.

A fin de asegurar una comunicación adecuada con las personas con discapacidades, los querellantes con discapacidades pueden solicitar formatos alternativos según sea necesarios. Esto incluye permitir que se reciban quejas verbales. El personal de los Programas CDBG-DR/MIT, Mitigación y/o Asistencia Pública para Desastres u otras entidades relacionadas que reciban dicha queja deben asegurarse de que se cumplan todos los requisitos antes descritos.

Envío de quejas

Los ciudadanos que deseen presentar una queja sobre cualquier asunto relacionado con la administración general de los fondos CDBG-DR/MIT, Mitigación y/o Asistencia Pública para Desastres pueden hacerlo por escrito a través de cualquiera de los siguientes métodos:

- Por correo electrónico a: auditoria@maunabopr.com
- Por escrito, a: Oficina de Auditoría Interna, calle Santiago Iglesias #1, Maunabo, Puerto Rico

Si el quejoso no puede presentar una queja por escrito (esto podría deberse a una discapacidad y/u otra circunstancia especial), la queja debe formalizarse por escrito a través de un proceso de entrevista.

Si se solicita, la queja puede presentarse verbalmente vía:

- Telefónica: 787-861-0825
- Personalmente: En la Oficina de Auditoría Interna del Municipio de Maunabo

Quejas recibidas de terceros

Las quejas que se reciban en cualquiera de las oficinas del Municipio de Maunabo deben notificarse de inmediato a la Oficina de Auditoría Interna por correo electrónico o correo regular, a las direcciones antes mencionadas. El/La Auditor(a) Interno(a) evaluará las quejas que le envíen y las manejará adecuadamente.

Quejas que carecen de legitimación o de datos

Las quejas con datos insuficientes o enviadas por un tercero sin legitimación en el asunto que se está presentando no necesitan ser aceptadas o revisadas. No se atenderán quejas anónimas.

5 Responsabilidades

El Municipio de Maunabo ha establecido las medidas adecuadas y viables para manejar las quejas de los ciudadanos. Al recibir una queja, el Municipio se esforzará por brindar prontamente una respuesta sustancial por escrito dentro del período establecido de **quince (15) días laborables**, de acuerdo con lo estipulado en 24 C.F.R. § 91.115(h).

6 Investigación de la queja

En los casos en los que la Oficina de Auditoría Interna lo considere necesario, se dará seguimiento a las partes involucradas para obtener información adicional y/o la evidencia necesaria para responder a la queja de manera responsable. Las demoras en proporcionar la información adicional y/o evidencia solicitada pueden resultar en una contestación a la queja después del período de **quince (15) días laborables**.

7 Referidos

Dependiendo del tipo de queja presentada y del remedio solicitado, el/la Auditor(a) Interno(a) puede utilizar distintos enfoques para generar prontamente una respuesta sustancial por escrito. Al evaluar las quejas caso por caso, según corresponda, para que proporcionen los datos pertinentes para la respuesta. Algunos ejemplos de estos referidos incluyen:

- Las quejas relacionadas con el personal pueden referirse a la Oficina de Recursos Humanos.
- Las quejas relacionadas con contratos y adquisiciones pueden referirse a la Secretaría Municipal.
- Las quejas relacionadas con un solicitante de un programa pueden referirse al programa específico.

Las quejas sobre asuntos relacionados con fraude, desperdicio, abuso o malversación deben seguir las directrices de la Política Anti-Fraude, Desperdicio, Abuso o Malversación (**AFWAM**, por sus siglas en inglés). No obstante, si cualquier otra oficina que atienda los asuntos relacionados a los Programas CDBG-DR/MIT, Mitigación y/o Asistencia Pública para Desastres recibe estas quejas, se referirán inmediatamente a la Oficina de Auditoría Interna.

Las quejas sobre asuntos relacionados con conflictos de intereses deben seguir la Política sobre Conflictos de Intereses y Estándares de Conducta. No obstante, si la Oficina de Auditoría Interna recibe estas quejas, estas se manejarán de acuerdo con las políticas y procedimientos establecidos por el Programa federal aplicable a estos asuntos.

Las quejas sobre asuntos relacionados con la Ley de Vivienda Justa deberán seguir la Política de Equidad de Vivienda e Igualdad de Oportunidades (FHEO, por sus siglas en inglés). No obstante, si la Oficina de Auditoría Interna recibe estas quejas, se referirán a la Oficina de Programas Federales responsable del programa HUD en un plazo de **dos (2) días laborables**.

8 Registros

La Oficina de Auditoría Interna mantendrá un registro de las quejas recibidas y contestadas. Se documentarán, procesarán y archivarán todas las quejas recibidas de acuerdo con la Política sobre Manejo, Administración y Accesibilidad de Documentos.

9 Medidas cautelares

El Código Anticorrupción para el Nuevo Puerto Rico, Ley 2-2018, según enmendada, consolidó las distintas legislaciones anticorrupción en un solo código.

El Código establece protecciones para los denunciantes que prohíben a las entidades privadas y funcionarios gubernamentales "hostigar, discriminar, despedir, amenazar o suspender algún beneficio, derecho o protección" a una persona que ha provisto información, ha cooperado o ha actuado como testigo en una investigación que conduzca a una denuncia, acusación, convicción, acción civil o administrativa, con relación al uso ilegal o apropiación indebida de fondos públicos u otros actos de corrupción. El Código también permite a los denunciantes reclamar daños civiles por violaciones a las prohibiciones establecidas contra las represalias. De igual forma, el Código reconoce el derecho de los denunciantes a solicitar y recibir asesoramiento y/o representación legal del Departamento del Trabajo y Recursos Humanos de Puerto Rico para iniciar o participar en algún procedimiento civil, penal, o administrativo que surja de conformidad con el Código.

Para obtener más información sobre las protecciones y remedios reconocidos para los denunciantes en el Código Anticorrupción para el Nuevo Puerto Rico, consulte la Ley 2-2018, según enmendada.

La Ley Federal para el Mejoramiento de la Protección a Denunciantes de 2012 ("Whistleblower Protection Enhancement Act") protege a los empleados federales que revelen evidencia de desperdicio, fraude o abuso. Estas estipulaciones son compatibles con, y no sustituyen ni están en conflicto ni alteran de ninguna manera, las obligaciones, derechos o responsabilidades de los empleados según establecidas por un estatuto u Orden Ejecutiva existente con relación a (1) información confidencial, (2) comunicaciones con el Congreso, (3) informar a un Inspector General sobre la violación de una ley, regla o reglamento, o sobre la mala administración de fondos, despilfarro de fondos, abuso de autoridad o un peligro considerable y específico para la salud o la seguridad pública, o (4) cualquier otra protección a denunciantes. Las definiciones, requisitos, obligaciones, derechos, sanciones y responsabilidades establecidas mediante Órdenes Ejecutivas y disposiciones legales aplicables son determinantes.

Asimismo, como parte de la Ley de Autorización de Defensa Nacional de 2013, de acuerdo con lo estipulado en 41 U.S.C. § 4712, es ilegal despedir, degradar o discriminar de cualquier otra manera contra un empleado de un contratista, subcontratista, recipiente o subrecipiente de fondos federales como represalia por divulgar información en su carácter de denunciante protegido. Para estar protegido bajo las disposiciones de 41 U.S.C. § 4712, la divulgación debe hacerse a un funcionario administrativo o a otro empleado del contratista, subcontratista o recipiente de fondos que tiene la responsabilidad de investigar, descubrir o atender los casos de conducta indebida.¹¹

Aprobado en Maunabo, Puerto Rico el **2** de octubre de 2024.



ANGEL OMAR LAFUENTE AMARO
Alcalde del Municipio de Maunabo

¹¹ Para que un denunciante esté protegido bajo las disposiciones de 41 U.S.C. § 4712, la divulgación de información debe hacerse a uno de los siguientes: (1) un miembro del Congreso o un representante de un comité del Congreso; (2) la Oficina del Inspector General; (3) la Oficina de Responsabilidad del Gobierno de los Estados Unidos (GAO); (4) un empleado federal a cargo de la supervisión o manejo de los contratos o subvenciones en la agencia pertinente; (5) un

funcionario autorizado del Departamento de Justicia de los Estados Unidos u otra agencia del orden público; (6) un tribunal o un gran jurado; 0 (7) un funcionario de administración u otro empleado del contratista, subcontratista o destinatario de fondos que tiene la responsabilidad de investigar, descubrir o atender asuntos de conducta indebida.