Personally Identifiable Information (PII) Policy

Policy #		Effective Date		Email	
Version	1.0	Contact		Phone	

Table of Contents

PURPOSE

This policy establishes the information security-related requirements for the City of Deer Park Personally Identifiable Information or PII.

SCOPE

All City of Deer Park employees, contractors, vendors, and subrecipients handling PII must comply with PII requirements as outlined in this document.

POLICY

PII Handling

Per the NIST SP 800-122, which provides government-wide standards for protection of agency PII, the City of Deer Park requires strict PII handling guidelines for employees, subrecipients, and contractors due to the nature of the data collected and used to determine eligibility and allocate awards, and the increased risk to an individual if sensitive or personal data were to be compromised.

General Handling

1. Store PII on secure servers accessible by password only with time-out features. Ensure access to the server is granted only to City of Deer Park employees who have completed PII training and have a need for access.

2. Secure paper PII data by locking it in desks and filing cabinets when not in immediate use. Remove visible PII from desks and office spaces when not in use. The building and room/area in which PII data is being stored should also have restricted access.

3. Destroy PII by shredding and delete electronic PII by emptying computer 'recycle bin'.

4. Only use City of Deer Park assigned emails for conducting official business and encrypt PII on computers, media, and other devices, especially when sending data outside of network.

5. Documentation will be stored securely and adhere to for the length of time specified in the SLFRF/ARPA Terms & Conditions.

Minimization

Use and collection of PII will be minimized as much as possible; and will be limited only to what is needed to ascertain identity, assess eligibility, determine needs, and award funds. Certain application information may need to be collected such as name, contact information, and income documentation. Information not explicitly needed (such as SSN or bank account numbers) should be redacted prior to filing (either electronically or physically). Collection of SSN should be avoided as much as possible, but should it be needed, the project file shall include a Social Security Number Justification Memo.

Privacy Advisory Statements are required when soliciting an individual's SSN for authentication purpose only and will not be maintained in a System of Records. The Privacy Advisory Statement informs the individual why the information is being solicited and how it will be used.

1. The authority (whether granted by statute or by Executive Order) for soliciting the information and whether disclosure is mandatory or voluntary;

2. The principal purpose(s) for which the information is intended to be used; and

3. The effects on the individual, if any, of not providing all or any part of the requested information.

The information above must be included on the information collection form itself, or in a separate form which can be retained by the individual whose information is being collected.

Transparency/Notification

The City of Deer Park will be transparent about the use, storage, and destruction of PII collected for the program. PII shall only be stored long enough to complete analysis and with an alternative reference code (Alpha-Numeric identifier) used when referring to the beneficiary. Someone providing PII data will be able to review policies and procedures related to the data collection at any time.

Upon collection of PII, the person providing the data will review and confirm receipt of the use of PII being requested and their specific purpose for collection.

1. **Disclosure Request**
   If an individual who has provided their PII request to see a copy of their record; then a full copy of their records shall be made available to them.

2. **Privacy Act Exceptions to Conditions of Disclosure**
   The City of Deer Park shall not provide an individual's PII without prior written consent, unless the disclosure is due to statutory exceptions as listed in The Privacy Act and exceptions to disclosure included in The Texas Public Information Act.

3. **Annual Review of PII Policy & Procedure**
   This document shall be reviewed and updated on a regular basis and as needed, or at least annually.

PERSONNEL TERMINATIONS

Employee Termination Procedure - In the event that an employee, consultant, or contractor is terminating his or her relationship with City, the person's immediate supervisor must notify Human Resources and Information Technology, and initiate the IT Status Change Form Procedure.

Notification To Third Parties of Employee Terminations - If a terminated employee had authority to direct contractors, consultants, or temporaries, or if this same employee had the authority to bind City in a purchase or another transaction, then the Human Resources Department or the person's immediate supervisor must promptly notify all relevant third parties that the terminated employee is no longer employed by City.

Involuntary Terminations - In all cases where information technology employees are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all City equipment and information, and escorted while they pack their belongings and walk out of City facilities.

VIOLATIONS

Any violation of this policy will be investigated by the appropriate City staff and if a violation is established, disciplinary action up to termination from employment may result. An Authorized User must report an actual or suspected violation of this policy and procedures to his or her supervisor and IT or the IT Oversight Committee. The City will not discipline an Authorized User for making a good faith report of a potential violation of this policy and procedures or the Standards.

DEFINITIONS

Personally Identifiable Information (PII) - is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Set forth below is a nonexclusive list of information that may constitute PII on its own or in combination with other information.:

- Age
- Alias
- Audio recordings
- Biometric identifiers (e.g., fingerprints, iris image)
- Certificates (e.g., birth, death, marriage)
- Credit card number
- Criminal record information
- Date of birth
- Device identifiers (e.g., mobile devices)
- Driver's License/State ID Number
- Education records
- Email address
- Employee identification number
- Employment status, history, or information (e.g., title, position)
- Fax number
- Financial information
- Foreign activities
- Full name
- Gender
- Geolocation information
- Home address
- Internet cookies containing PII
- Investigation report or database
- IP/MAC address
- Legal documents or records
- Marital status
- Military status or other information
- Mother's maiden name
- Passport information
- Phone numbers
- Photographic identifiers
- Place of birth
- Protected health information
- Race/ethnicity
- Religion
- Salary
- Sex
- Social security number (SSN)
- Taxpayer ID
- User ID
- Vehicle identifiers
- Web uniform resource locators
- Work address or other business contact information. (HUD does not engage with individuals in an entrepreneurial capacity, but business contact information may still constitute PII because it identifies individuals.)

REFERENCES

RELATED DOCUMENTS

APPROVAL AND OWNERSHIP

Owner	Title	Date
Approved By	**Title**	**Date**

REVISION HISTORY

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version			