ATTACHMENT A
Administrative Policy Manual
Policy No: A-37
Update as of: 1-14-2021
Approved: Mark Scott

SUBJECT: **Handling of Sensitive Personally Identifiable Information**

1. Purpose: The purpose of this sensitive personally identifiable information (SPII) handling policy is to define what is SPII, identify proper handling of SPII, and ensure uniform handling of SPII throughout the City of Indio and all of its entities. This policy outlines the minimum requirements for the handling of SPII by the City.
2. Scope: This policy covers appropriate handling of any SPII collected, received, or sent and applies to all employees, vendors, and agents operating on behalf of the City of Indio and all of its entities.
3. Definitions and Terms
    a. Sensitive Personal Identifying Information (SPII) is defined as information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
    b. There are two (2) categories of Sensitive Personally Identifiable Information (SPII), 1) Stand-Alone; 2) Personally Identifying Information paired with another identifier such as an individual's first name (or first initial) plus the last name and any one or more of the following:

Stand Alone (no other identifier required)	
Social Security Number	Driver license or state ID number
Military ID number	Passport number
Credit/Debit Card number, CVV2, and expiration date	Financial account numbers
Customer account numbers	Biometric identifiers
Alien Registration number	
In Combination with an Identifier (First/Last Name)	
Date and/or place of birth	Mother's maiden name
PINs or passwords	Password challenge question responses
Account balances or histories	Digital or physical copies of handwritten signatures
Medical records numbers	Unlisted phone number
Credit or payment history data	Medical histories
Insurance policy numbers	Religious affiliations(s)

In general, protected personally identifiable information does not include information that is lawfully obtained from publicly available records, or from federal, state or local government records lawfully made available to the general public

4. Policy:

   4.1 Staff must minimize the use of SPII whenever possible. The use, collection, and retention of SPII should be minimized to what is strictly required to accomplish the business purpose for which it is required.

   4.2 Electronic storage of SPII must reside within an encrypted file share. Physical storage of protected SPII must reside in a locked file cabinet or room when not being actively viewed or modified.

   4.3 SPII is not to be downloaded to personal or vendor electronic devices, including but not limited to laptops, USB thumb drives, tablet, or mobile phone.

   4.4 If SPII must be sent via email, the email must be sent using the email system's encryption.

   4.5 If SPII is transmitted via radio, the radio traffic must be encrypted.

   4.6 SPII is not to be sent via text message, SMS message, instant messaging, or unencrypted email.

   4.7 Staff may not take pictures or recordings of SPII.

5. Policy Compliance

   5.1 The City of Indio IT team will verify compliance with this policy through various methods, including but not limited to: periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

   5.2 Any exception to the policy must be approved in advance by the City Manager or his designee, in writing.

   5.3 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Retention

   6.1 All items must be kept in accordance with the City's records retention policy.

7. Related Standards, Policies and Processes
   6.1 A-9 Computer Resources Policy
   6.2 A-38 Electronic Mail Policy