**AGENCY NAME**

**Title: Personally Identifiable Information (PII)**

**Number: XXX Effective: 6/01/16**

**Amends: XXX**

**Distribution: All**

**Standards**:

The purpose of this policy is to define PII and ensure that PII is protected and secure.

|  |
| --- |
| **Scope** |

This procedure shall apply to all Agency personnel.

|  |
| --- |
| **Discussion** |

The overriding goal of this policy is to comply with the CJIS Security Policy requirements. Due to the evolving nature of the CJIS Security Policy, it is necessary to separately communicate the requirements of the CJIS Security Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Standard Operating Procedures of AGENCY NAME. The Agency shall adhere, at a minimum, to the CJIS Security Policy. While the Agency may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy.

|  |
| --- |
| **Procedures** |

Personally Identifiable Information (PII) –is any information pertaining to an individual that can be used to distinguish or trace a person’s identity. PII is defined as any one or more of types of information including, but not limited to:

1. Social security number

2. Username and password

3. Passport number

4. Credit card number

5. Clearances

6. Banking information

7. Biometrics

8. Data and place of birth

9. Mothers maiden name

10. Criminal, medical and financial records

11. Educational transcripts

12. Photos and video including any of the above

All electronic files that contain PII will reside within the Agency’s physically secure location. All physical files that contain PII will reside within a locked file cabinet or room when not being actively viewed or modified. PII is not to be downloaded to workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the Agency. PII will also not be sent through any form of insecure electronic communication as significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted. All disposal of PII will be done by authorized Agency personnel.

All PII will be collected only when there is a legal authority and it is necessary to conduct Agency duties.

Access to PII is only conducted when the information is needed to conduct Agency official duties and should only be utilized for official purposes. Agency members will not create duplicate copies of documents that contain PII and will destroy the documents when no longer needed. When PII is extracted from a document Agency members may only target the PII that is required for the task. PII that is extracted shall not be retained beyond the records retention rules for the data and the system it was accessed from. PII shall not be stored or transmitted via personally owned devices. PII may not be taken home by any Agency member.

POLICY VIOLATION: Any user who violates any portion of this policy will be subject to the standard disciplinary processes in place with the Agency. Sanctions against staff that violate information systems and or security policies may include formal disciplinary action up to and including termination based on offense severity.