

# TRAVIS AIR FORCE BASE Privacy Visual AID Reference AFI 33-332

## Defining PII and Need-to-know

### Personally Identifiable Information (PII)

--**Sensitive PII** – PII, which if lost, compromised, or disclosed without authorization, could result in harm; i.e., SSN, Passport, Financial info, etc. (para 1.1.2.2.1.1.)

--**Non-sensitive PII** – PII, which if lost, compromised, or disclosed without authorization would NOT result in harm; i.e., Name, business or home phone, address, e-mail (para 1.1.2.2.1.2.)

**NOTE:** *Non-PII may become PII if it is associated with an identifier or other information which then relates the information to a specific individual (para 1.1.2.2.1.3.)*

**Need-to-know** is the authorized, official need based on assigned duties and responsibilities, to access information that is protected under the Privacy Act. There are three cases when a need-to-know may be established: Official business; Statutory; and Information sharing.

## Safeguarding PII

- When handling Sensitive PII, ensure e-mails are digitally signed, encrypted or attachments are password protected, and all recipients have an official need to receive the information (para 1.1.2.2.2.)
- PII accessible through SharePoint or similar web-based applications must be properly safeguarded so that only individuals who have an official need-to-know to conduct daily operations may gain access to information (para 1.1.2.2.3.)
- Remove PII on SharePoint or similar web-based applications, when no longer needed for daily operations and properly file IAW AF RDS (para 1.1.2.2.3.1.)
- AF Form 3227, *Privacy Act Cover Sheet*, or DD Form 2923, *Privacy Act Data Cover Sheet*, is mandatory and used to protect PII from being viewed by unauthorized personnel when Privacy Act materials are removed from its approved storage area (para 1.1.3.)
- AFVA33-276, *Air Force Privacy Act Label*, is mandatory and used for all electronic media (external hard drives, CD's, gov't laptops, etc.) containing PII information (para 1.1.4.)
- Documents/media containing personal information must be destroyed in a manner to prevent theft or compromise during and after destruction, destroying so that PII is both not readable and is beyond reconstruction (para 6.4.1.)
- Do NOT leave personal information in unsecured vehicles, unattended workspaces, unsecured file drawers, or in checked baggage (para 2.2.2.8.)
- Promote privacy awareness throughout the organization and reinforce the protection of PII (para 4.8.2)

## POINTS OF CONTACT

1. Unit Privacy Monitor	PHONE
2. Base Privacy Officer Ms. Linda Morris	PHONE 424-2228
3. After Hours Contact Comm Focal Point	PHONE 424-2666

## Reporting lost, stolen, or compromised PII

All incidents of lost, stolen, or "possible" compromised PII must be immediately reported by anyone discovering the breach (para 1.1.2.4.2.)

**Step 1:** Immediately notify your supervisor and unit privacy monitor

**Step 2:** Immediately notify the Base Privacy Officer

## Transmitting PII via e-mail

To protect e-mails containing PII information:

1. Add "FOUO" at the beginning of the subject line
2. Apply the following statement at the beginning of the e-mail:  
*"This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (5 U.S.C 552) and/or the Privacy Act of 1974 (5 U.S.C. 552a). Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties. Further distribution is prohibited without the approval of the author of this message unless the recipient has a need-to-know in the performance of official duties. If you have received this message in error, please notify the sender and delete all copies of this message."*
3. Digitally sign and encrypt e-mail (para 2.5.7.)

**\*\* NOTE: Do not e-mail PII to non .mil addresses \*\***

## Rosters

Paper/electronic documents that contain PII such as recall rosters, personnel rosters, lists or spreadsheets shall be marked in the header or top "FOR OFFICIAL USE ONLY" with the following banner in the footer or bottom:

*"The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties"*

(para 2.5.3.)

## AMRDEC SAFE

The Army Missile Research Development and Engineering Center Safe Access File Exchange (AMRDEC SAFE) is an alternate means to transmit PII and protect the data

Use AMRDEC SAFE to send PII when e-mail encryption can't be used. The application can be accessed via:  
<https://safe.amrdec.army.mil/safe/> (para 2.2.1.11.)