The U.S. Department of Housing and Urban Development

Personally Identifiable Information (PII) Protection At Workstations Policy

DATE OF PUBLICATION

04 August 2020

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
Original	11/15/2019	All	Initial Draft Version 1.0
Original	08/04/2020	All	Final Version

TABLE OF CONTENTS

1. Introduction

This Personally Identifiable Information (PII) Protection at Workstations Policy covers the responsibilities of personnel regarding the protection of information assets when unattended in the personal workspace. Protections are needed to prevent unauthorized access and disclosure of Personally Identifiable Information (PII), in accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a), and HUD's implementing regulations at 24 CFR Part 0 (Standards of Conduct) and Part 16 (Implementation of the Privacy Act of 1974), and 5 CFR Part 2635 (Standards of Ethical Conduct for Employees of the Executive Branch).

2. Definition

Personally Identifiable Information (PII)
PII means 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. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual. See 2 CFR 200.79.

3. Purpose

The purpose of this policy is to establish minimum requirements for protecting PII material when not in use. This policy ensures that PII is locked away, properly secured or protected, when the items are not in use and/or individuals leave their workstation.

4. Applicability

This policy applies to all HUD employees and contractor employees within a HUD building or facility.

5. Effective Implementation Date

This policy is effective as of August 5, 2020.

6. Policy

a. The following is a non-exhaustive list of items that cannot be left out on an unattended workstation or in an unlocked private/inside office when

employees are away from their desks: Files or other material, such as reports, letters, and/or bills containing PII.

b. Employees are required to ensure that all PII in hardcopy or electronic form are secured (locked) in their work area. This applies to inside offices and meeting/project rooms (unless the door is locked).

    - Computer workstations must be password locked when workspace is unoccupied. Personal Identity Verification (PIV) cards must be removed when the computer workstation is not in use.
    - File drawers/cabinets containing PII materials must be kept secured when unattended when not in use or when unattended. Keys for such drawers/cabinets must not be left out at an unattended workstation.
    - Managers shall ensure that employees have the appropriate amount of space to store files. *See* HUD/AFGE CBA, 57.04 (11). If HUD personnel do not have appropriate space to store files, they must contact their supervisor and or program manager.
    - Managers must ensure that employees have access to keys they need to lock their offices and file cabinets.

c. PII must not be left unattended or unsecured for a colleague at their work area, if the colleague is not present to receive it.

    - Documents and files containing PII should be marked with the PII Coversheet before being handed to other personnel, especially when in transit.
    - The intention of this policy directive is to prohibit employees from leaving PII materials exposed and/or unattended and unsecured. If the intended recipient is unavailable, leaving the package on the recipient's chair is not permitted. However, leaving the package with a co-worker (administrative assistant, supervisor, etc.) who is able to secure the package and subsequently deliver it to the recipient is permitted. Employees should use their best judgment when deciding if it is appropriate to leave PII materials with anyone other than the intended recipient.

d. Passwords, Personal Identification Numbers (PINs), and/or other login credentials must not be left on sticky notes posted on or under a computer, nor may they be left written down in an openly visible location.

e. Employees must remove their PIV card from HUD laptops/computer workstations when leaving workstations unattended. Employees assigned to private/inside offices must also follow this directive and shall not leave their PIV card unattended, even if their office is locked. An employee's PIV card should remain on their person or in their direct control at all times.

f. Employees shall use HUD "Secure Printing" to print documents containing PII. All community printers and faxes must be cleared of papers containing PII as soon as they are printed to ensure that sensitive documents are not left

in trays for the wrong person to pick up. Employees who have a private printer within their assigned workstation or private office must take proper action to ensure documents containing PII are not left unattended and are secured in a locked area or locked office.

- Instructions for "Secure Printing" (on most HUD computers):
  - Select printer
  - Select "properties"
  - Select "secure print"
  - Enter passcode
  - Print the document
  - When at printer (could be same day, or when returning from telework on a later day):
    - Select "job status"
    - Select second tab, "My secure jobs"
    - Click on your H Number to select your secure jobs, enter the passcode you chose, and your secure jobs will print

g. Materials needing disposal that contain PII must be shredded. No documents should be disposed of, deleted, shredded, or destroyed in violation of the Freedom of Information Act (FOIA), litigation hold, and record retention requirements. Employees should contact their supervisor or Program Office's Privacy Liaison Officer (PLO) if they have questions about whether documents fall under the FOIA, the Privacy Act, litigation hold or record retention requirements. Questions can also be directed to the Privacy Office at privacy@hud.gov.

h. Do not write PII on whiteboards.

i. Mass storage devices, such as Compact Discs (CDs), Universal Serial Buses (USBs), etc., containing PII should be treated as sensitive and secured in a locked office or drawer when not in use. Mass storage devices should also be encrypted in accordance with HUD Information Technology Security Policy, 2400.25 REV 5 (2020). Employees may seek assistance from the IT Helpdesk for instructions on encrypting or decrypting devices.

j. This policy also applies to the tops of cabinets, under desks, and windowsills.

7. Roles and Responsibilities

All employees and contractors are responsible for adhering to the Personally Identifiable Information Protection at Workstations Policy.

a. Management will ensure that reminder signage is posted in key areas of the office and/or posting copies of this policy at individual workspaces to remind employees of the policy

b. Managers should oversee adherence to the Personally Identifiable Information Protection at Workstations Policy by periodically conducting an office walkthrough, checking workstations for policy violations.

    - Managers may conduct or delegate a non-bargaining unit employee to conduct an office walkthrough to check workstations for policy violations.
    - Managers must ensure that, when applicable, they provide reasonable accommodations to employees with disabilities to carry out the requirements of this Personally Identifiable Information Protection at Workstations Policy.

c. Employees should contact their supervisor or their program office's Privacy Act liaison if they have questions about whether documents contain PII or fall under the FOIA, the Privacy Act, litigation hold or record retention requirements or if they otherwise have questions about how to comply with this Policy.

d. The Department will be responsible for:

    a. Establishing and overseeing the department-wide Information Security Program and providing security consulting assistance to all HUD Program Offices for their individual programs.
    b. Communicating the policy to employees, via e-mail and written documentation
    c. Ensuring the policy is enforced and documenting infractions.
    d. Providing and updating annual privacy and security awareness training.

8. Glossary - Abbreviations and Acronyms

CD – Compact Disc
OCIO – Office of the Chief Information Officer
PII – Personally Identifiable Information
PIN – Personal Identification Number
PIV – Personal Identification Verification
PLO – Privacy Liaison Officer (Privacy POC for individual offices)
USB – Universal Serial Bus