The U.S. Department of Housing and Urban Development

CLEAN DESK POLICY

[DATE OF PUBLICATION]
DD MMMMM YYYY

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
Original	11/15/2019	All	Initial Draft Version 1.0

TABLE OF CONTENTS

Introduction

This Clean Desk 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), Controlled Unclassified Information (CUI), and confidential medical information, 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, Part 16, and 5 CFR part 2635.

Definitions

Controlled Unclassified Information (CUI)

CUI is information that requires safeguarding or circulation controls pursuant to and consistent with law, regulations, and government-wide policies. Executive Order 13556 "Controlled Unclassified Information", which establishes a program for managing CUI across the Executive branch.

Personally Identifiable Information (PII)

PII is information which can be used to distinguish or trace a data subject's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Purpose

The purpose of this policy is to establish minimum requirements for maintaining a clean desk where confidential data (including PII) material is secured in locked areas or out of sight. This policy ensures that confidential data (including PII) is removed from individuals' workspace and locked away when the items are not in use and/or individuals leave their workspace.

Applicability

This policy applies to all HUD employees and contractors.

Effective Implementation Date

This policy is effective as of MMDDYYYY.

Policy

a. The following is a non-exhaustive list of items cannot be left out in an unlocked office when employees are away from their desks

b. Files or other material, such as reports, letters, and/or bills containing PII, CUI and confidential medical information.

c. Employees are required to ensure that all PII and CUI 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, CUI, and confidential medical information 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.
- Program managers to 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.
- Program managers must ensure that employees have access to keys they need to lock their offices and file cabinets.

d. PII, CUI, and confidential medical information must not be left for a colleague at their work area, if they are not present to receive it.

   - Documents and files containing PII, CUI, and confidential medical information should be marked with the PII Coversheet before being handed to other personnel, especially when in transit.

e. 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.

f. Employees must remove their PIV card from HUD laptops/computer workstations when leaving workstations unattended.

g. Use HUD "Secure Printing" to print documents containing PII, CUI, and confidential medical information. All printers and faxes must be cleared of papers containing confidential data (including PII) as soon as they are printed to ensure that sensitive documents are not left in trays for the wrong person to pick up.

   - 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

h. Materials needing disposal that contain PII, CUI, and confidential medical

information 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.

i. Do not write PII, CUI, or confidential medical information on whiteboards.

j. Mass storage devices, such as Compact Discs (CDs), Universal Serial Buses (USBs), etc., containing confidential data (including 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 Security Policy.

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

Roles and Responsibilities

All employees and contractors are responsible for adhering to the Clean Desk Policy.

Each office is responsible for:

a. Posting reminder signage 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 Clean Desk Policy by periodically conducting an office walkthrough; checking workstations for policy violations.

- Managers should conduct or assign personnel to conduct a daily office walkthrough at the end of the day to check workstations for policy violations.
- Managers should ensure that, when necessary, they provide reasonable accommodations to employees with disabilities to carry out the requirements of this Clean Desk Policy.

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

d. The OCIO 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 policy training and refresher training.

Glossary - Abbreviations and Acronyms

CD – Compact Disc
CUI – Controlled Unclassified Information
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

Policy Background

Policy Name: Clean Desk Policy

Point of Contact Name: LaDonne White

Author: LaDonne White

Subject Matter Expert: LaDonne White

Primary Organization: ADMIN/ExecSec/Privacy

Secondary Organization: OCIO

	Description of Information
Rationale for the policy change or policy development	*To remediate the FISMA-2018-XXX audit finding, which recommends that HUD* *a. issue a clean desk policy prohibiting unattended and unsecured sensitive data in workplaces* *b. Implement procedures to enforce a clean desk policy*
Areas of Change	This is a new policy statement. It reinforces HUD policy with respect to securing personal identifiable information and overall security in handling documents or electronic storage devices with such information.
Date Submitted	