American Federation of Government Employees
National Council of HUD Locals 222

Affiliated with AFL-CIO

451 7th Street, SW, Suite 3142
Washington, DC 20410

Ashaki Robinson Johns, PhD
President

Phone: 202-402-3077
E-mail: Ashaki.Robinson-Johns@hud.gov

July 10, 2020

Bobby Allen
Human Resources Specialist
Employee & Labor Relations Division
Office of the Chief Human Capital Officer
Department of Housing and Urban Development

RE: Demand to Bargain – Proposed Clean Desk Policy

This is in response to the Department of Housing and Urban Development's (the Department's or HUD's) Article 49 Notice of July 6, 2020, regarding a proposal to implement a new Clean Desk policy. Council 222 (the Union) supports the development of a policy to protect sensitive and controlled information. Council 222 demands to bargain over the proposed Clean Desk policy and provides the following as preliminary proposals.

1. Status Quo: The status quo will remain, and the Department shall not implement any changes associated with the new policy until all bargaining is completed in accordance with the Agreement.

2. Written Responses: Management shall provide written responses to each of the Union's proposals provided here no later than the first day of bargaining.

3. Bargaining Meetings: Management shall work with the Union to set a mutually agreeable meeting time to begin negotiating within 10 days of receipt of this demand to bargain. All bargaining shall be conducted by telephone due to the COVID-19 pandemic; the Union does not waive its right to demand in-person negotiations in the future.

4. Ground Rules: The parties shall abide by the mid-term negotiation ground rules provided by Section 49.06, other than those related to physical facilities and materials (Sections 49.06 (b) and (c)). The Department shall provide a call-in number for conference calls to be used by the negotiating teams for the duration of bargaining.

5. No Waiver of Rights: Neither the proposed policy nor any supplement or other agreement resulting from bargaining over this matter shall diminish or waive any rights that bargaining unit employees have under the parties' collective bargaining agreement, law, rule, or regulation.

6. Incorporation into Successor Agreement: All of the terms upon which the parties have agreed as a result of bargaining over this matter, and any resulting supplement or other agreement shall be incorporated as a new article into the successor collective bargaining agreement that follows the existing 2015 HUD-AFGE national collective bargaining agreement.

7. Supplement/Agreement Prevail: Where there is a conflict between the proposed policy and the collective bargaining agreement, including any supplement related to the proposed policy, the collective bargaining agreement and supplement will prevail, provided that there is no conflict with law, statute, or government-wide regulations. If there are any conflicts between the language of the collective bargaining agreement (either the 2015 or subsequent one) and any resulting supplement on this matter, the terms of the supplement shall prevail.

8. Prior Agreements: Nothing in the proposed policy shall contradict, negate, or conflict with any prior agreements related to the use of PIV cards.

9. Compliance with ADA: The Department shall ensure that all aspects and requirements of the proposed policy comply with the Americans with Disabilities Act and the Rehabilitation Act of 1973, as amended in 1998, including Section 508.

10. Reasonable Accommodations: The Department shall provide reasonable accommodations that enable disabled employees to comply with the proposed policy.

11. Training: Management is responsible for providing training to all employees on the proposed policy. No employee shall be required to comply with the proposed policy until they have received training on the policy.

12. No Adverse Action: Employees shall not be subject to adverse or disciplinary action as a result of implementing the proposed policy or for failing to comply with the proposed policy.

13. Not Applicable to Private Offices: The proposed policy shall clearly state that it does not apply to employees with private offices that are locked when the employee is not in the room. The Department shall modify the proposed policy to reflect this.

14. FOIA/Privacy Act: The proposed policy shall have no impact on whether a document or file (paper or digital copy) is subject to the provisions of the Freedom of Information Act or the Privacy Act.

15. Identification of Sensitive Documents: Management shall be responsible for identifying documents that are subject to the proposed policy, either when providing a document to an employee or when assigning work that will require an employee to create such documents.

16. Cover Sheets: Management shall provide all necessary cover sheets for employees to use, in both paper and electronic format. Managers are responsible for ensuring that all employees know where to access both electronic cover sheet files and printed cover sheets.

17. Locked Drawers: Management shall ensure that all employees have working locking drawers and keys to those drawers within their personal workstations.

18. Daily Walk-Through: Bargaining unit employees shall not be required to conduct inspections or walk-throughs to check their peers' or supervisors' workstations for policy violations.

19. Conference/Meeting Rooms: Management shall be responsible for collecting and protecting all sensitive documents used in conference and meeting rooms during breaks and following the conclusion of meetings.

20. Changes Subject to Bargaining: The Department shall immediately notify the Union any time that changes in law, statute, or government-wide regulations require a modification of the Clean Desk policy. All changes are subject to bargaining.

21. Handbook Number: The Department shall advise Council 222 of the handbook number assigned to the proposed policy. The Department shall post the finalized policy on the HUDCLIPS/Handbooks website and shall advise the Union when and where the handbook is posted.

22. Recommended Modifications: The Department shall consider making the changes to the written policy recommended by Council 222 in the attached draft and as described and explained below. The Department shall make all changes to the proposed policy necessitated by the result of bargaining and shall provide the Union with a copy of the final policy. The Union recognizes that the Department is not obligated to adopt the following suggestions but offers them as a way to help achieve the Department's goals of protecting sensitive data.

    a. Change title of policy to Sensitive Information Protection Policy for clarity. "Clean Desk" policies generally refer to business policies that mandate clearing a desk of *all* material at the end of the workday. This policy only addresses the protection of sensitive information such as Personally Identifiable Information. Changing the title will emphasize the purpose of the policy and encourage conformance.

    b. Include "Definitions" in the Table of Contents.

    c. Number each section in the Table of Contents and the body of the policy for ease of reference.

    d. Include a definition of sensitive data such as "As used in this policy, sensitive information or data includes all personally identifiable information (PII), controlled unclassified information (CUI), and confidential medical information."

    e. Include a definition of confidential medical data, which is broader than many people realize, i.e., it is more than simply medical records. A suggested definition would be: "In addition to medical records and statements from a medical professional, confidential medical information includes any information related to an individual's medical history, mental or physical condition, or treatment, including information in relation to a request for reasonable accommodation."

f. The definition of CUI has what appears to be a nonfunctioning link to the relevant Executive Order.

g. The definition of PII should distinguish between having a person's name on a letter/email when it is routine, such as emails between co-workers (because a name distinguishes an individual's identity), and when it is PII.

h. In the Purpose section, recommend replacing the word "confidential" with 'sensitive." When "confidential" is used other than as a modifier in "confidential medical information" it can be confused with the official classification level of Confidential (as in Confidential, Secret, or Top Secret).

i. The Policy section should clearly state that none of the following sections (at least a–e or f) applies to personnel with private offices that are locked when unattended.

j. Policy section a refers to a list of items that cannot be left out on a desk, but only section b identifies such items. Recommend combining sections a and b. Section b should also include informal material such as emails that need to be protected (e.g., an email requesting a reasonable accommodation or sick leave).

k. Policy section c refers to PII and CUI, but does not mention confidential medical information, which should also be locked up when not in use and the employee is not present. The section should mention the use of cover sheets for all hardcopy material not placed in files but not actively being used at any given time.

l. Policy section c should clarify that confidential medical information should be retained separately from other files. Recommend referring to other agency policy/handbooks (such as the Reasonable Accommodation Handbook) about the proper handling of such material.

m. Policy section c refers to program managers. Not all managers are "program" managers; recommend just using the term managers.

n. In the third bullet in Policy section c, suggest replacing "to" with "shall" for clarity.

o. Policy section d does not make it clear whether it is improper to leave sensitive information with a third party such as a supervisor or other employee if the intended recipient is unavailable, or whether it is simply improper to leave the material unattended.

p. Policy section d appears to hyperlink the term PII Coversheet but the link does not work. Suggest identifying where the coversheet is, or including it in an appendix.

q. Policy section f does not clarify whether the requirement also applies to an unattended but locked private office. If it does, suggest spelling out the hazards of leaving the PIV card in the computer aside from physical access to the computer or theft of the card.

r. In Policy sections g and j, suggest replacing "confidential" with the word "sensitive" for the reason given above.

s. Suggest clarifying in Policy section h that materials that require shredding may be placed in special locked shredding bins placed around the building.

t. Policy section j should specify the handbook number of the HUD Security Policy. Does this refer to the Information Technology Security Policy, HUD Handbook 2400.25 REV4.2 (2018)?

u. Roles and Responsibilities should specify to the manager of each office, not each office in general, which fails to assign responsibility to any specific individual/group.

v. Roles and Responsibilities section b, second bullet, should replace the word "necessary" with "applicable" to avoid improper determinations of what reasonable accommodations are necessary.

These are preliminary proposals only, and the Union reserves the right to amend or add proposals in accordance with Article 49 of the collective bargaining agreement. I will serve as the Chief Negotiator for this matter.

Jerry Gross
Steward
AFGE Council 222
jerry.gross@hud.gov

Encl: Annotated Clean Desk Policy draft

The U.S. Department of Housing and Urban Development

~~Clean Desk~~ Policy

Sensitive Information Protection 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

Suggest numbering each section for ease of reference.

Confidential Medical Information: In addition to medical records and statements from a medical professional, any information related to an individual's medical history, mental or physical condition, or treatment, including information in relation to a request for reasonable accommodation.

Suggest numbering each section for ease of reference.

Introduction

Sensitive Information Protection

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

Include a definition of Sensitive Information/Data: As used in this policy, sensitive information or data includes all PII, CUI, and confidential medical information.

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 (link?) 13556 "Controlled Unclassified Information", ~~,~~ which establishes a program for managing CUI across the Executive branch.

Define confidential medical information: (see above)

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.

Differentiate between simply having a name on an email (e.g., to one's co-worker or supervisor) and when it's a concern.

Purpose

The purpose of this policy is to establish minimum requirements for ~~maintaining a~~ ensuring all sensitive ~~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 sensitive 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

Clarify that none of the following applies to private offices that are locked when unattended.

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:

(Note: Only "b" identifies items that cannot be left out.)

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

what about medical info?

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 when not in use. and when the employee is not present.

The policy should clarify that medical information needs to be stored separately from other files.

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~~ 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.
- ~~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. Unclear if this means not left on an empty desk or not given to a 3rd party (supv, admin, co-worker)

- 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. Where is that cover sheet?

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. What about in a locked office?

Personnel shall

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~~ sensitive 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

deposited in special shredding containers?

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~~ sensitive 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. Provide Handbook # IT?

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~~ Sensitive Information Protection Policy.

The manager of 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~~ Sensitive Information Protection 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~~ applicable, they provide reasonable accommodations to employees with disabilities to carry out the requirements of this ~~Clean Desk~~ Sensitive Information Protection 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	