



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 20, 2020

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

RE: Union Proposals – Proposed Clean Desk Policy

Dear Ms. Allen:

On July 10, 2020, the Union provided its preliminary bargaining proposals 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) reiterates our support for the development of a policy to protect sensitive and controlled information. On July 15, 2020, the Union provided additional proposals, which we subsequently withdrew for reasons related to scheduling negotiations.

Council 222 submits the following bargaining proposals regarding the Department's Clean Desk policy. In accordance with Article 49, Section 49.06(j), the Union reserves its right to "submit new proposals based on new or modified information provided by the other party" and to "submit new proposals at any time by mutual agreement in the interest of reaching an agreement."

1. 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 Union 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.
2. **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.
 3. **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)). In lieu of providing physical facilities, the Department shall provide a call-in number for conference calls to be used by the negotiating teams for the duration of bargaining.
 4. **Status Quo:** The status quo will remain, and the Department shall not implement any the new policy until all bargaining is completed in accordance with the Agreement.
 5. **Written Responses:** Management shall provide written responses to each of the Union’s proposals indicating either agreement or providing a reason or justification for objecting to the proposal.

6. Policy Changes: 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. Prior Agreements: Nothing in the proposed policy shall contradict, negate, or conflict with any prior agreements related to the use of PIV cards.
13. 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.
14. Encrypting/Decrypting Devices: Management shall provide training and written guidance on how to encrypt and decrypt documents and mass storage devices. (See Policy section j.)
15. 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.

16. 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.
17. 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.
18. 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.
19. Practicality: Management shall ensure that all means of protecting digital and hard copy sensitive data shall be practical and feasible for employees to use.
20. 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.
21. Locked Drawers: Management shall ensure that all employees have within their personal workstations working locking drawers that are of sufficient size and depth to accommodate sensitive documents that employees handle and keys to those drawers.
22. Lockboxes: Management shall provide secure lockboxes or the equivalent to enable employees to deliver sensitive documents to colleagues in the same or different offices when the recipient is not present to receive the file. Management shall distribute the keys to all personnel and offices that may need to access such lockboxes.
23. Key Holders: To ensure that employees are able to carry keys to locking drawers and cabinets, or to shared lockboxes, management shall provide keychain wristlets to employees upon request.
24. 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 adherence or violations.
25. 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.
26. Mailroom Access: Management shall provide guidance for mailroom personnel who are required to open mail and determine the appropriate receiving office, and for other personnel who receive documents in transit that may contain sensitive information. The presence of sensitive information such as PII may not be immediately apparent (or recognized as such) by the initial recipient(s). (See Policy section d, first bullet.)

27. IT Support Access: Management shall clarify its policy on protecting sensitive data contained in HUD computers and data collection devices when IT support needs access to the computer to identify and resolve a software or other functional problem.
28. New Software Testing: Employees shall not be held responsible for adhering to this policy when collaboration with external personnel (e.g., IT support, representatives of HUD-held properties) requires shared access to electronic files during the testing of new software or electronic procedures.
29. Data Protection During Travel: Management shall be responsible for providing personnel with all necessary means to protect sensitive information, whether digital or hard copy, that personnel need to access, use, or carry while on official travel or while conducting field work. This applies to local travel as well as overnight travel.
30. Support for Remote Employees: Management shall ensure that sufficient IT support is provided to employees who work in remote areas, such as REAC Quality Assurance personnel, to prevent the loss or compromising of sensitive data.
31. 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.
32. Reasonable Accommodations: Implementation of this policy shall not have any effect on any existing reasonable accommodations. The Department shall provide reasonable accommodations that enable disabled employees to comply with the proposed policy. Management shall provide reasonable accommodations for any employee who is unable to lift or carry the hard copy documents to the necessary storage container.
33. Safety: For safety purposes, no employee shall be required to lift large hardcopy files from or to a location above shoulder height or to place them or lift from storage that is below knee level, unless such requirements were identified in the job application and position description before the employee was hired. Large files are those that weigh 5 pounds or more or are more than 2 inches thick.


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

Encl: Annotated Proposed Clean Desk Policy