

NATIONAL SUPPLEMENT
Between
U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
And
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES
NATIONAL COUNCIL OF HUD LOCALS 222

SUBJECT: HUD Handbook 2400.25, Rev-2 - Information Technology Security Policy

SCOPE: This supplement encompasses the implementation of HUD Handbook 2400.25, Rev-2, and the impact on bargaining unit employees

1. **Continued Access:** HUD's intent is to allow employees access to systems that are necessary for performing their job responsibilities. Appropriate Program Offices/System Owners shall approve individual access privileges for personnel who require access for their job responsibilities
2. **Minimum Security Requirements:** The security requirements for systems will not be contrary to government-wide regulations.
3. **Procedural Details:** The Policy is intended to provide a set of basic protection goals and standards; the procedural details normally found in operational and technical documentation are not within the scope of this document.
4. **Access to Physical Security issues:** The IT Security Policy addresses the requirement for HUD facilities group or security officers to maintain overall physical access points to facilitate housing IT systems.
5. **Uniform Security:** The Program Offices or System Owners are responsible for implementing management, operational, and technical controls to ensure that they are effective in protecting the information and information systems under their purview. This protection includes all HUD systems that maintain employee personally identifiable information (PII) data and Health Insurance Portability and Accountability Act (HIPAA) data in accordance with the Privacy Act of 1974, Public Law 93-579.
6. **PC Time out time Frames:** Management will be coordinating with the OIG to revise the timeout sessions from 10 minutes to accommodate security risk. If the request is approved it will be changed in six months or less. Until that time, waivers can be made to the Chief Information Security Officer (CISO) through the Authorizing Official (AO) and must include the operational justification, risk acceptance, what the risk are, what information is at risk, and risk migration measures.

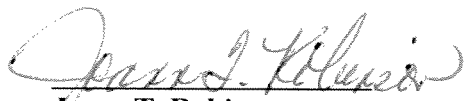
7. **Periodic Reports:** If a report is created on an employee regarding a potential or security violation, the report shall be provided to the Union in accordance with applicable laws and regulations.
8. **Sensitive Information:** Information systems that provide sensitive data are identified as being in low, moderate and high sensitivity categories. Each category may have a separate security level and protective requirements applied to the category. Employees are only required to meet the minimum security requirements.
9. **Employee Responsibility:** Management agrees that nothing in this Policy has an adverse affect regarding employees' ability to perform their duties.
10. **Updating Training:** Employees who access HUD data are required to take Security Awareness Training within required timeframes. When training cannot be completed for a justifiable reason, employees' supervisor may approve an extension of the timeframe with the approval of the CISO.
11. **Sensitive Information:** Sensitive information is defined by the program office/systems owners, and also includes information to which access must be controlled to protect the privacy of employees and their personally identifiable information.
12. **Policy Basis:** The IT Security Policy Handbook is based on federal laws, regulations and guidance on information security (e.g. National Institute of Standards and Technology (NIST) Special Publications on information security). In areas where federal guidelines are lacking, the policy reflects established best security practices within the security community.
13. **Potential Security Violations:** Potential employee IT security violations may be investigated by appropriate HUD management and in accordance with applicable procedures and may be used to improve IT security.
14. **Remote Access:** Management agrees that remote access for employees may be for compelling operational needs and during emergencies for efficient and effective program delivery.
15. **Management Protocols:** HUD Management, not contractors, is responsible for enforcing the IT Security Policy.
16. **Employee Rights:** The implementation of this handbook will not affect any statutory, regulatory or contractual rights of employees, including the Privacy Act requirements.
17. **Subsequent Negotiations:** The provisions of this Supplement will be considered in any future agreement relating to the subject of IT Security.

18. **Multifunctional devices (MFD)**: MFDs are classified as hardware that can generate documents containing sensitive data.
19. **Policy Clarification**: Management agrees that the narrative text above each of the tables titled as "HUD Policy" in Sections 3, 4, and 5 of the Information Technology (IT) Security Policy Handbook are for informational purposes and should not be interpreted as HUD policy.
20. **Existing Policies**: HUD Handbook 2400.25, Rev 2, is replacing HUD Handbook 2400.25, Rev 1 and Supplement 72.
21. **Security Incidents**: Whenever a HUD employee fails to comply with HUD security policies, the employee may be subject to corrective actions. Management recognizes that security incidents may result from intentional and unintentional actions. Management agrees that an unintentional action does not necessarily mean disciplinary action and, at Management's discretion, remedial training may be more appropriate.
22. **Privacy Rights**: HUD is committed to protecting the privacy rights of all employees. Employees should have an expectation for privacy protection as provided in the Privacy Act of 1974, as amended, 5 U.S.C. 552a, and in accordance with any laws, rules, regulations, or negotiated agreements.
23. **Information Request**: Information, as permitted by applicable laws, may be shared with the Union for representational purposes.
24. **Local Facilities**: Management agrees that changes to the IT Security Policy affecting local facilities may be negotiated at the local level.
25. **Equitable Treatment**: Employees shall be treated in a fair, impartial and equitable manner under the requirements of the Information Security Policy Handbook.
26. **New Employee Orientation**: HUD employees will receive annual IT Security Awareness Information. The Union may participate in the new employee orientations.
27. **Sanctions**: If a violation of the IT Security Policy occurs, Management agrees to comply with section 20.01(3) of the HUD/AFGE Agreement.
28. **Employee Encryption**: Management agrees that Union officials may use privately owned encrypted media only if it meets HUD standards.
29. **Union Access**: Management agrees to provide the Union with access to and use of Information Technology as allowed by law and the HUD/AFGE Agreement.

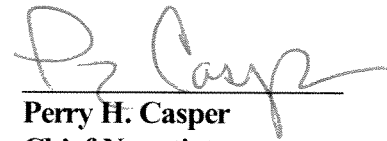
- 30. **Exceptions:** Management agrees that the Union may request an exception through the Labor and Employee Relations Division. The request must include the operational justification, risk acceptance, and risk mitigation measures. The Labor and Employee Relations Division will provide a written status to the Union. The Union may grieve any negative decision.
- 31. **Effective Date:** This supplement will become effective no more than 30 days upon approval of both parties.

MANAGEMENT

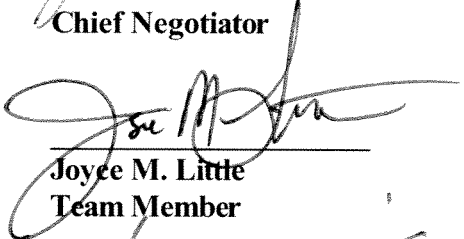
AFGE



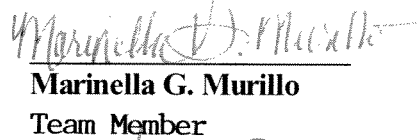
Joann T. Robinson
Chief Negotiator



Perry H. Casper
Chief Negotiator



Joyce M. Little
Team Member



Marinella G. Murillo
Team Member

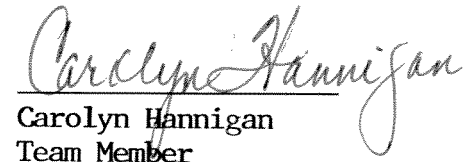


Harold E. Williams
Team Member



William L. Biggs
Team Member


John W. Smith
Team Member



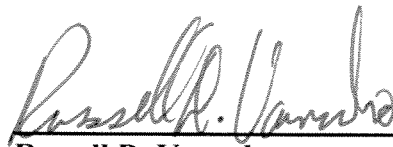
Carolyn Hannigan
Team Member

APPROVED:

APPROVED:



Sharman R. Lancefield
Deputy Assistant Secretary
for Human Resources Management



Russell D. Varnado
President, National Council
of HUD Locals 222

Date Approved 10.1.08