USER ACCOUNT ACCESS POLICY

Name: _____
(Print Name Legibly)

As an employee or as an authorized user of the IT computer systems of GSA, I will be given access privileges to Federal data and computer systems/software, especially computer systems within or accessible by GSA staff, to perform the duties of my job.

I understand the following policies apply to these data and computer systems:

1. I agree to safeguard all passwords and personal identification numbers (PINs), e.g., access and verify codes, electronic signature codes) assigned to me and I am strictly prohibited from disclosing these codes to anyone, regardless of his/her position in or outside GSA for any reason. However, I may be required to reveal these codes to the Information System Security Officer (ISSO) or IT staff if Facility Management so directs me to make such an exception.
2. I understand that I will be held accountable for all entries and changes made to any GSA computer system using my passwords and PINs. It is in my best interest not to permit others to use my personal passwords or PINs, and not use another person's account.
3. If I think any of my passwords or PIN has been compromised, I will change it and contact the ISSO or local Help Desk immediately.
4. I agree to safeguard my Personal Identity Verification (PIV) Card and wear it at all times while on GSA premises. I understand it is to be used for identification purposes only.
5. I understand that my PIV Card is to be used at all time for access into any GSA IT computer system and when entering government facilities.
6. I will never share my PIV Card or allow anyone but myself past a security point or access any IT computer system of GSA.
7. I will lock my computer anytime that I leave it unattended using <Ctrl><Alt><Del> and selecting the lock computer button, and/or removing my PIV Card.
8. I understand that if I leave my PIV Card at home I will have to contact the PIV Card Administrator to request a temporary access card.
9. If my PIV Card is damaged I will need to contact the ISSO or local Help Desk.
10. I understand that any lost or stolen PIV Card must be immediately reported to the ISSO or local Help Desk. I will report any security exposure, of which I am aware, as quickly as possible and fully cooperate in order to mitigate associated risks.
11. I am aware of GSA regulations and security policies designed to ensure the confidentiality of all sensitive information. I understand that all data to which I may obtain access to is and will remain the property of GSA. I understand that, as an employee, I have an obligation to protect data and information which the loss, misuse, or unauthorized modification of or unauthorized access to could adversely affect the conduct of GSA or other Federal programs. I am aware that information about any employees is confidential and protected from unauthorized disclosure by law. I understand that I may not access my own records or records of other employees for personal reasons through the GSA computer system. Improper disclosure of information to anyone not authorized to receive it may result in substantial fines and penalties under the Privacy Act of 1974.
12. I agree to not access, research, or change any account, file, record, or application not required in performing my official duties. If asked by another person to access an account or

other sensitive or private information, verify that the request has been authorized. I understand I will be held responsible if the access is not authorized.

13. I understand that GSA electronic mail is to be used for official government business only. I will exercise common sense and good judgment in the use of electronic mail, and I must not use it for any activity or purpose involving classified data. I understand that electronic mail is not inherently confidential and I have no expectation of privacy in using it.
14. I understand that use of any unlicensed personal software, whether installed on personal or GSA microcomputers, is illegal. I agree to contact the system ISSO to register any personally owned software that I plan to use at my workstation.
15. If granted Internet access, I agree that use of such access will be limited to tasks pertaining to my function at this office and must not interfere with official system use or access.
16. If granted access to a PC workstation, I understand that I am not to add any hardware to the workstation without prior consent from the Network Information Technology Section and that use of the workstation is strictly limited to official government business.
17. If granted access to work at home for a period of time, I understand that I will be responsible for any GSA software to which I am granted license as an employee and that such software will be removed from my personal PC if and when I either return to full duties at GSA or I should terminate my employment with GSA.
18. I understand that any lost or stolen GSA IT assets must be immediately reported to the ISSO or local Help Desk. I will report any security exposure, of which I am aware, as quickly as possible and fully cooperate in order to mitigate associated risks.
19. I understand that any violation of this notice constitutes disregard of a direct supervisory order and/or GSA policy and/or software copyright laws and will result in appropriate disciplinary action as well as suspension or termination of access privileges and may result in criminal charges.
20. I affirm with my signature that I have read, understand, and agree to fulfill the provisions and intent of this policy and recognize the importance of protecting access to any GSA computer system and confidential information with which I have been entrusted.
21. I hereby certify receipt with my signature that I have been provided and read the written GSA General Rules of Behavior, CIO 2104.1. Failure to non-compliance may incur disciplinary action and/or criminal prosecution.

Written guidance cannot cover every contingency, therefore employees are asked to go beyond the stated rules, using their best judgment and highest ethical standards to guide their actions. Employees must understand that these rules are based on Federal laws and regulations, GSA, and administrations' directives. As such, there are consequences for non-compliance with rules of behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand, suspension, demotion, removal, and criminal and civil penalties. I understand that when using GSA IT resources I will be held accountable for my actions related to the information resources entrusted to me.

Your Signature: _____ Date: _____

Your Computer Access Coordinator: _____

Your Information System Security Officer: _____

RETURN THIS FORM TO THE INFORMATION SYSTEM SECURITY OFFICER (ISSO)