



## **51V21 INFORMATION SYSTEM ACCESS AUTHORIZATION AND BRIEFING FORM**

Printed Name: \_\_\_\_\_ Phone: \_\_\_\_\_

I have the necessary clearance to obtain access on the PIA/Collaborative Environment information system assets. As a system user, I understand that it is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification, or destruction of information. I am responsible for all actions taken under my account. I will not attempt to “hack” the system or any connected systems, or gain access to data to which I do not have authorized access. I have read or will read all portions of the system security authorization package pertaining to my level of responsibilities and agree to the following:

1. Protect and safeguard all information in accordance with the security authorization package.
2. Fulfill the responsibilities detailed in the DSS Assessment and Authorization Process Manual (General User – Section 3.10).
3. Protect all media used and generated on the system by properly classifying, labeling, controlling, transmitting and destroying it in accordance with security requirements and security classification guide.
4. Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.
5. Process only data that pertains to official business and is authorized to be processed on the system.
6. Use the system for performing assigned duties, never personal business.
7. Report all security incidents or suspected incidents to the Information System Security Manager (ISSM) or designee. This includes any indication of intrusion, unexplained degradation or interruption of services, or the actual or possible compromise of data or file access controls.
8. Discontinue use of any system resources that show signs of being infected by a virus or other malware and report the suspected incident.
9. Challenge unauthorized personnel that appear in work area.
10. Ensure that access is assigned based on ISSM and ISO approval.
11. Notify the ISSM if access to system resources is beyond that which is required to perform your job.
12. Attend user security and awareness training annually and/or as required by the ISSM.
13. Coordinate user access requirements, and user access parameters, with ISSM and ISO.
14. Safeguard resources against waste, loss, abuse, unauthorized users, and misappropriation.
15. Sign all logs, forms and receipts as required.
16. Obtain permission from the ISSM or designee prior to adding/removing/reconfiguring/ or modifying any system hardware or software.
17. Comply with all software copyright laws and licensing agreements.
18. Ensure all files and media are checked for viruses and malicious logic using a current virus detection tool prior to, or at the time of introduction to a system.



19. Prevent non-authorized personnel from accessing the system and/or data.
20. Notify the ISSM or designee when access the system is no longer needed (i.e., transfer, termination, leave of absence, or for any period of extended non-use).
21. Only perform data transfers if authorized by the ISSM. If authorized, Data Transfer Agent (DTA) appointment letter and training will be executed. In addition, all data transfers will be performed in accordance with authorized procedures.
22. Follow guidelines regarding the explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
23. Comply with the following password requirements:
  - a. Protect system passwords commensurate with the level of information processed on the system and never disclose to any unauthorized persons.
  - b. Report suspected misuse or compromise of a password to the ISSM or designee.
  - c. Report discovery of unauthorized use, possession, or downloading of a password-cracking tool to the ISSM or designee.
  - d. Select a password that is a minimum of 14 non-blank characters. The password will contain a string of characters that does not include the user's account name or full name. The password includes one or more characters from at least 3 of the following 4 classes: Uppercase, lowercase, numerical, and special characters.
  - e. Passwords are not to be written down at any time without consent of the ISSO/ISSM. Same passwords should not be used with multiple systems to enhance security.

I understand that all of my activities on the system are subject to monitoring and/or audit. Failure to comply with the above requirement will be reported and may result in revocation of system access, counseling, disciplinary action, discharge or loss of employment, and/or revocation of security clearance.

User Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**FOR SECURITY AND ADMINISTRATOR USE ONLY**

☐ Employee ☐ Visitor / Company: \_\_\_\_\_  
Visit request expires on: \_\_\_\_\_  
Clearance/ Special Briefings: \_\_\_\_\_  
Verified By: \_\_\_\_\_  
Account Name: Date Added: \_\_\_\_\_  
Other, Access/Privileges, or Comments: \_\_\_\_\_

ISSM or designee Signature: \_\_\_\_\_ Date: \_\_\_\_\_