**SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)**

**TYPE OF REQUEST**

INITIAL___ MODIFICATION_____ DEACTIVATION_____ USER ID_____ DATE_____

**PART 1** (To be completed by the Requester)

1.FIRST NAME: _____2. LAST NAME_____ 3. PHONE_____

4.EMAIL ADDRESS_____ 5.JOB TITLE_____ 6. CITIZENSHIP _US_OTHER

7. DIVISION: ____ 8. IA Training and Awareness Certification Requirement (Complete as required for user)

☐ I have completed Annual Information Awareness Training Date_____

9. PL-4 RULES OF BEHAVIOR:

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 Delphinus Engineering Corporate Computing Environment system and agree to the following:

1. Protect and safeguard all information in accordance with the security authorization package.
2. Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.
3. Process only data that pertains to official business and is authorized to be processed on the system.
4. Use the system for performing assigned duties, never personal business.
5. Report all security incidents or suspected incidents to the Information System Security Manager (ISSM). This includes any indication of intrusion, unexplained degradation or interruption of services, or the actual or possible compromise of data or file access controls.
6. Discontinue use of any system resources that show signs of being infected by a virus or other malware and report the suspected incident.
7. Challenge unauthorized personnel that appear in work area.
8. Ensure that access is assigned based on ISSM, ISO and CIO approval.
9. Notify the ISSM if access to system resources is beyond that which is required to perform your job.
10. Attend user security and awareness training annually and/or as required by the FSO/ISSM.
11. Coordinate user access requirements, and user access parameters, with ISSM, ISO and CIO.
12. Safeguard resources against waste, loss, abuse, unauthorized users, and misappropriation.
13. Obtain permission from the ISSM prior to adding/removing/reconfiguring/ or modifying any system hardware or software.
14. Comply with all software copyright laws and licensing agreements.
15. 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.
16. Prevent non-authorized personnel from accessing the system and/or data.
17. Notify the Program Manager when access the system is no longer needed (i.e., transfer, termination, leave of absence, or for any period of extended non-use).
18. Follow guidelines regarding the explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
19. 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 FSO.
    c. Report discovery of unauthorized use, possession, or downloading of a password-cracking tool to the ISSM or Helpdesk.

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.

10. User Signature_____ Date_____

**PART II**- ENDORSEMENT OF ACCESS BY INFORMATION OWNER/SUPERVISOR/PM

11. TYPE OF ACCESS REQUIRED

**General User** ◯ **Privileged User** ◯

System Access: (Note: Program Manager/Supervisor selects the level of Access for the New Hire):

1. **Network Access:**
2. **Unanet Access:**
3. **Deltek Access:**
4. **Paychex**:

12. VERIFICATION FOR NEED TO KNOW: I certify that this user requires access as requested _____

13. ACCESS EXPIRATION DATE: _____

14. SUPERVISOR'S NAME_____15. SUPERVISOR'S SIGNATURE _____ 16. DATE _____

17. CIO SIGNATURE _____ 17. DATE _____