IS Access Authorization and Briefing Acknowledgement Form

I have the necessary clearance for access to the classified system. 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 which I do not have authorized access. I have read or will read all portions of the security plan pertaining to my level of responsibilities and agree to the following:

1. Protect and safeguard all information in accordance with the Authorization to Operator (ATO) and applicable STIG(s).
2. Fulfill the responsibilities detailed in the Information System Access Authorization Briefing which is derived from Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual (DAAPM) General User Requirements.
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 (SCG).
4. Obtain program approval before using any Infrastructure printers to process print jobs from the IS. The Print Job Record Form is required only for Infrastructure printers.
5. Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.
6. Process only data that pertains to official business and is authorized to be processed on the system.
7. Use the system for performing assigned duties, never personal business.
8. Every Infrastructure classified system (excludes tactical) must be logged off by the end of the work week. It is recommended that users logout daily. Unattended extended weekend processing will require coordination with security and the system administration teams.
9. 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.
10. Discontinue use of any system resources that show signs of being infected by a virus or other malware and report the suspected incident.
11. Challenge unauthorized personnel that appear in work area.
12. Ensure that access is assigned based on ISSM and Information System Owner (ISO) approval.
13. Notify the ISSM if access to system resources is beyond that which is required to perform your job.
14. Attend user security and awareness training annually and/or as required by the ISSM.
15. Coordinate user access requirements, and user access parameters, with ISSM and ISO.
16. Safeguard resources against waste, loss, abuse, unauthorized users, and misappropriation.
17. Sign all logs, forms and receipts as required. Submit Maintenance logs for any security relevant updates and maintenance-related changes (excluding tactical systems) to the baseline (reboots, shutdowns, software updates, OS configuration changes, etc.)
18. Obtain permission from the ISSM or designee prior to adding/removing/reconfiguring/ or modifying any system hardware or software.
19. Comply with all software copyright laws and licensing agreements.

20. 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.
21. Prevent non-authorized personnel from accessing the system and/or data.
22. 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).
23. Only perform data transfers if authorized by the ISSM. If authorized, Data Transfer Agent (DTA) authorization/appointment letter and training will be executed. In addition, all data transfers will be performed in accordance with authorized procedures, including Assured File Transfers.
24. Follow guidelines regarding the explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
25. Escort non- authorized personnel in such a manner as to prevent their access to data (physical or visual), which they are not entitled to view.
26. All electronic media downloaded from the IS shall be marked at the highest classification on the IS.
27. 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) If access is granted to a Generic/Group account, document actions in a manual log (or other approved method) to ensure individual user accountability.
    e) Users cannot use the same password for different systems with domains of differing classification levels.
    f) Select a password that is a minimum of 15 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.

I understand that all 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.

Tactical Users:

As a Tactical User with privileged access to the environment, I acknowledge that I have read, understand, and will comply with the requirements and responsibilities outlined below.

1. Authorization and Approval
    a) I understand that approval is given only when ALL signatures below have been supplied, indicating that I have been properly authorized to access the system with privileged credentials.
    b) https://docs.us.lmco.com/x/dL4XQgI recognize that ALL tactical passwords are highly sensitive and should only be disclosed to users who have been properly briefed - Briefings Status Verification
2. Access and Information Protection

   a) I will only access information on the computer system when necessary, in the course of my duties, and will ensure that such access is minimal and justified.
   b) I will maintain and protect the secrecy of the information to which I may have access, regardless of the method by which I acquire the information, and will not disclose such information to unauthorized parties.
   c) I will respect the privacy of other users and will not attempt to access or modify their files, data, or accounts without proper authorization.

3. Privileged Access Responsibilities
   a) I will receive approval and/or specific guidance prior to allowing other users to access the system, ensuring that they have the necessary clearance and authorization.
   b) I will use the special access or privileges granted to me ONLY to perform authorized tasks or mission-related functions, and will not use such access for personal gain or to bypass security controls.
   c) I will not share my privileged account credentials with others or allow them to use my account and I will ensure that all access is properly authorized.
   d) I will keep my privileged account credentials confidential and will not write them down or store them in an insecure manner.
   e) I will report any security incidents, including suspected unauthorized access or disclosure of sensitive information, to the ISSM/ISSO or system/network administrator immediately.
4. Additional Responsibilities
   a) I will comply with all applicable security policies, procedures, and guidelines, including those related to password management, account creation, and access control.
   b) I will participate in regular security awareness training and will stay up-to-date with the latest security threats and best practices.
   c) I will cooperate with security audits and investigations, providing access to systems and information as required.

LOCKHEED MARTIN

GENERAL USER INFORMATION SYSTEM ACCESS AUTHORIZATION AND BRIEFING ACKNOWLEDGMENT FORM

By signing this request, I acknowledge my understanding of the potential increased risk to the IS security and integrity and agree to the requirements stated in IS briefing. I understand that all my activities on the IS are subject to monitoring and/or audit. Failure to comply with the above requirement will be reported and may result in revocation of IS access, counseling, disciplinary action, discharge or loss of employment, and/or revocation of security clearance.

NOTE: All forms **NOT** completed in the entirely or filled out incorrectly will be **REJECTED**.

NOTE: If access to a classified machine is not needed, this form is **NOT** required.

Requester Information

Name:	Date:
Email:	Company:

Request Type (Select all that apply):

Briefing Renewal	New Account	**AND/OR** Tactical User
NOTE: **By checking "Tactical User" you acknowledge that you have reviewed the <u>Tactical Privileged User Briefing Section</u> of this form. ALL TACTICAL USERS are considered Privileged users**		
Signature:		

Clearance Verification:

To be completed by Security or other designated Personnel

Clearance:	Secret	Interim Secret	Top Secret	Interim TS
Special Access	NATO	:______________		
LM Employee:	_ Yes	No	Val Exp:	
Verifier Name (If different from Security Approver):			Date:	

Security Approver:

By authorizing the individual named above to have system access, you have **verified** appropriate user briefing have been duly executed and are still effective.

Approver Name:	Date:
Signature:	