LOCKHEED MARTIN

INFORMATION SYSTEM ACCESS AUTHORIZATION AND BRIEFING ACKNOWLEDGMENT FORM

References Documents:	
Directive (Compliance)	Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual (DAAPM), Version 2.2 dated 8/31/2020
Directive (Compliance)	National Industrial Security Program Operating Manual (NISPOM) Incorporating Change 2 dated May 18, 2016
Purpose:	
The Information System Access Authorization and Briefing Acknowledgment Forms are to provide ***ALL*** Information System users with the understanding of the responsibilities associated with their general user role.	
Applicability:	
The Information System Access Authorization and Briefing Acknowledgment Forms are applicable to ***ANY*** user who has been delegated extra levels of control on a computer system.	

Information System Access Overview

The National Industrial Security Program Operating Manual (NISPOM) and the Defense Security Service Assessment and Authorization Process Manual (DAAPM) requires that all persons accessing an Information System (IS) that processes classified information receive initial security briefing and take part in an annual security training and awareness; thereafter, detailing the safeguarding requirements for classified information. The NISPOM is a Department of Defense (DoD) publication that describes the security requirements to which we must adhere as defense contractors performing classified work. A Lockheed Martin Manassas IS System Security Plan (SSP) applies to each approved system and describes how we meet these requirements. The Defense Counterintelligence and Security Agency (DCSA) inspects us periodically to ensure we are complying with these requirements and are capable of continuing to safeguard the classified information the government has entrusted to us. For the purposes of this briefing, IS describes any system that processes classified information inside the closed area.

It is important that you know and understand the security guidelines you are required to follow when processing information on any IS inside the closed area. This briefing is designed to give you an overview of the guidelines. Further details may be found in the appropriate SSPs, Security Bulletins or by contacting IS Security.

Future requirements that may impact existing security policy and procedures must be coordinated and approved by the Information System Security Manager (ISSM) in sufficient time so that approvals can be obtained, or procedures be put into place.

Recognition / Identification of Classified System / Asset

Systems approved to process classified information can be identified by the ***classification labels*** affixed to the devices, or signs posted on the equipment. It is a serious violation to perform classified processing on

any system that is not approved to process classified information. Should this occur, IS Security must be notified immediately.

Password Guidelines

Passwords shall be protected at the highest classification level and most restrictive classification category of information to which they permit access. User passwords will be generated by the user. Passwords shall contain a minimum of fifteen non-blank characters and shall be valid for no longer than 60 days and changed when compromised. Passwords shall not be displayed to the screen when input and users shall be attentive to persons attempting to view their password while being entered.

Password guidelines for selecting user generated passwords, when authorized, or when the operating system cannot automatically generate passwords:

1. Passwords must contain at least 1 number, 1 upper case letter, 1 special character, and 1 lower case letter.
2. Passwords must be at least 8 characters different from the old password
3. Passwords must not contain more than 3 consecutive repeating characters.
4. Passwords must contain a minimum of fifteen non-blank characters.
5. Shall not be shared.
6. Shall not be any part of your name, or the names of family members or pets.
7. Shall not include other personal information; (i.e., name of the street you live on, the model of your automobile, or your favorite sports team).
8. Shall not use phone numbers or special dates (e.g., birthday, anniversary), license plate numbers etc.
9. Choose a password that is both difficult to guess but is easy for you to remember. Passwords must not be written down.
10. Password shall not contain 4 characters of the same class consecutively.

Media Handling:

This section is a high-level overview of media handling / control and data transfer requirements. For individuals, who are required to burn and transfer media, a separate live training, briefing and acknowledgement are required. If you require this privilege, contact your ISSO to schedule the required training.

All media (including unclassified media) inside the closed area must be marked to indicate its classification. Media that is still in its original shrink-wrapped container or is unmodified vendor media is considered unclassified does not need to be marked. Except for media being processed by a DTA for burning, all unclassified media must remain in “write-protect” mode, when residing in a classified area

- It is the user's responsibility to determine the classification of any data they process during a session, as well as ensuring all softcopy or hardcopy, including unclassified, is properly marked and protected to indicate the level of information it contains.
- When the IS has network access to facilities outside of the closed area, or Manassas campus, it is the user's responsibility to access only authorized sites identified in the Interconnection Security Agreement (ISA) and/or Memorandum of Agreement (MOA). Any access to sites other than those specified will be handled as a security violation. All access is logged in the system's automated audit logs.
- All output from a classified system must be handled and safeguarded as the highest classification level of the accredited IS until reviewed to determine appropriate classification.

Creating unclassified media off of a classified system Assured File Transfer (AFT) is authorized using a separate Data Transfer Agent (DTA) Briefing and Acknowledgement. Since ZIP disks do not have any method of write protection method available, they may only be used for backup purposes as long as the media is marked at the highest level of the system the information came from.

- **Unclassified - For Maintenance Use Only media** is media that is dedicated for use on an approved IS. This media is write-protected during use or reviewed after each use, however, it is always handled and stored as though classified and may only be used by cleared personnel (usually a SYS ADMIN function).
- **Classified media** is media intentionally loaded with classified information or mounted on a classified system and not write-protected during or reviewed after use. Secret media must be brought into formal accountability through Classified Document Control as soon as possible after creation and stored in an appropriate container.

Note: Any person performing a data transfer /media must attend a live training, briefing and sign an acknowledge to perform this function.

Classified Processing Procedures

It is the user's responsibility to protect the information they are processing. Never grant Uncleared and/or unauthorized personnel visual or keyboard access to classified information. Any individual requiring visual or keyboard access to a system is required to complete this briefing and sign the briefing acknowledgement AND complete any additional briefings required such as Data Transfer Briefing, Privileged User Access. This includes all Lockheed employees, visitors, partners, sub-contractors, and the Government. Do not leave classified information unattended. If you must leave your workstation or terminal, and it is not possible to log out due to the lengthy nature of the task you are performing, you must place a "Test in Progress" sign or screen saver on the screen and ensure that no classified information will be displayed. A "Test in Progress" sign may not be used just as an alternative to logging off.

Every classified system must be logged off at the end of the work shift. Overnight unattended batch processing (with an Unattended Processing in Progress sign) is approved only for systems running processes, compiling data, conducting backups, etc. It is not to be used as an alternative to logging off.

Classification of Information

It is the user's responsibility to determine the classification of any data they process during a session, as well as ensuring any softcopy or hardcopy is properly marked to indicate the level of information it contains. The determination of classification will be based on the appropriate classification guidance, which is available in Classified Document Control (CDC). Special briefing information can never be introduced onto a system without prior coordination and approval from the IS Security Manager (ISSM) and/or DCSA.

Classified Output - Marking and Handling

All hardcopy output, including unclassified, must be marked to indicate the highest classification level of information contained.

Secret - must be portion marked and then taken to CDC to either be put into accountability or entered into the working paper log. All output from a classified system must be handled and safeguarded at the highest classification level until reviewed to determine appropriate classification. This review must be completed within 24 hours of generation. Should the review determine that the output is classified, it must be immediately marked and brought into accountability. All output, which has not been reviewed, must be stored in an approved classified container. All output from a classified printer must be picked up immediately. All media markings shall include:

- Highest level of classification.
- Program Nickname (if applicable)
- Title (unclassified)
- Date Originated
- Derived From:
- Declassify On:
- Document Control Number: (if applicable)
- Program Name and Contract Number
- Name and Address of Originating Agency
    - Lockheed Martin – Manassas
    - 9500 Godwin Drive
    - Manassas, Virginia 20110-4166

Marking of Electronic Classified Files

All classified files created or stored on an IS will be marked according to the following guidelines:

- **Text Files** will be portions marked in a similar fashion to hardcopy requirements.
- **Code and database structures** will have a header and footer that completely spell out the security classification of the file's contents.
- **Raw and binary data** will not be marked but will be controlled by the protection of the media that will be marked and handled at the highest level of the contents. This includes all files that contain imagery data.

Audit Trails

Any event regarding access or maintenance must be tracked via audit trail records on all classified systems.

Access

All individuals accessing the classified system must use the assigned unique User ID. You are authorized access only to the specific user account created for your use. Unauthorized access to other system accounts will be considered a security violation. If you are unsure of the type of user login for a system on which you are working, contact the Information System Security Officer (ISSO) or system administrator.

Your password is considered classified, cannot be written down, and is against the NISPOM and company policy to disclose it.

Risk Management Framework (RMF) Configuration Management (CM) Process:

To ensure compliance with RMF all information systems (IS: classified networks) now require additional controls regarding the addition and removal of hardware (HW) and/or software (SW). New controls are being applied to operations on the IS due to new DCSA requirements and to renew our Authority to Operate (ATO) for classified systems. As processes are defined by the RMF Integrated Product Team (IPT), they will be posted to Confluence: Manassas Classified Cybersecurity - Confluence

All HW/SW is applicable to these processes. All HW/SW must go through the CM HW/SW SharePoint before being added to a classified system if directed to do so by an approved process. Work with the MC AT (Manassas Classified Asset Tracking) Team to process any HW/SW into the lab.

LOCKHEED MARTIN

INFORMATION SYSTEM ACCESS AUTHORIZATION AND BRIEFING ACKNOWLEDGMENT FORM

If you encounter a situation that you do not believe is covered by a process, please let the program RMF Point of Contact (POC) know so that it can be addressed. Our direction is to continue with "business as usual" until a process is defined and approved. IPT Leads/ISSO RMF POCs: https://docs.us.lmco.com/display/MANCC/RMF+Procedures

Manassas Classified Asset Tracking Process

The MCAT process must be followed in all labs utilizing the Tracker Database. Manassas Security Rev K – March 25, 2011. The purpose of the MCAT Process is to ensure positive control is maintained at all times of all classified hardware and media. The following is an overview of the MCAT process:

Authorized DoD Closed Area users shall notify a Manassas Lab tracking team member via the Tracking Team mailbox (see below) when the following occurs:

1. Initial creation or setup of classified hardware
2. Movement of all classified hardware or media (internal, incoming to a DoD Closed Area or materials to be shipped)
3. Replacement of failed classified media or hardware
4. Movement of classified media or hardware between drawers of a General Service Agency (GSA) approved container (i.e. a safe)
5. Movement of classified workstations including monitors, printers, laptop computers, routers, switches, and cryptographic equipment.

The following movement does not require any notification:

1. Movement of media and hardware within the same location code
2. Movement of cables, keyboards and mice
3. For the ASW ONLY, Movement of Confidential documents
4. Movement of classified media and hardware which is returned to its original location prior to the end of the responsible individual's work day

Notification to the Lab Tracker team member of movement of classified media and hardware shall occur as soon as possible, and no longer than within eight (8) business hours via e-mail. E-mail notification shall be sent to:

Lab-TrackerTeam.Fc-Man@lmco.com. Lab Tracker Team personnel who perform their own classified media and hardware movements shall document the change within eight (8) business hours. Lab Tracker Team persons are responsible for the following:

1. Documenting the change using the required methodology (i.e. Tracker update) within three (3) business days of notification.
2. Classified Ownership responsibilities: Custodianship is assigned to the person who created the asset, is the subject matter expert, or is currently utilizing the asset. Custodianship is assigned at time of creation, transfer of responsibilities or when checked out of CDC. It is the custodian's responsibility to ensure proper storage of the classified asset. Tracker will be the record of classified ownership in all labs that use Tracker to inventory classified assets.

LOCKHEED MARTIN

INFORMATION SYSTEM ACCESS AUTHORIZATION AND BRIEFING ACKNOWLEDGMENT FORM

IS User Account/Home Data Retention Policy

All personnel user home data on the classified systems that are disabled will be moved into an archive area – data will be deleted after 180 days utilizing the below procedure. This is an effort to reduce existing and future storage.

1. User account is requested to be Disabled by Security for the following reasons:
   - Due to inactivity – current policy is 90 days of account not being used.
   - Leaving the company
   - No longer requires an account
2. SA team will Disable the account and note in the description the reason it is disabled.
3. SA team will place the user's home in the Archive area for a minimum 180 days
4. SA team will archive user data after 6 months

When an individual leaves the company, it is the individuals responsibility to ensure all data is shared with the appropriate people, teams and management. The Security team and/or the SA team will not make a determination of what data is or is not mission critical / relevant.

Information System Access General User Definition

A general user is an individual who can receive information from, input information to, or modify information on a system. A general user does not have access to system controls, monitoring, and/or administrative functions. Responsibilities of general users include, but are not limited to:

a. Complying with the system security program requirements as part of their responsibilities for the protection of systems and classified information.
b. Complying with all policies and procedures issued by the Information Owner (IO) (e.g., AFT procedures, media protection procedures, SCG, etc.).
c. Completing, at a minimum, annual General User Training.
d. Accessing only the data, system information, software, hardware, and firmware for which they have authorized access and a NTK, and assuming only those roles and privileges for which they are authorized.
e. Being accountable for all their actions on a system.
f. Protecting the system and associated peripherals from unauthorized access.
g. Protecting authentication mechanisms at the highest classification level and most restrictive classification category for information to which the mechanisms permit access.

Information System Access Requirements

As a system user, 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.

1. Protect and safeguard all information in accordance with the Authorization to Operate (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. 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 Information System Owner (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, including Assured File Transfers.
22. Follow guidelines regarding the explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
23. 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.
24. All electronic media downloaded from the IS shall be marked at the highest classification on the IS.
25. 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. As applicable, 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.