Enterprise Information Technology (eIT) Project Management Office (PMO)
Acceptable Use Policy

1. PURPOSE

The purpose of this document is to establish an understanding that the non-DoD external user has the primary responsibility to safeguard the Information Systems (ISs) managed by the Enterprise Information Technology Project Management Office (eIT PMO). The eIT PMO manages a suite of IT capabilities connected to the Unclassified but Sensitive Non-Classified Internet Protocol Router Network (NIPRNET), including the Electronic Document Management System (EDMS), the Serious Adverse Event (SAE) system, the Electronic Data Capture (EDC) system, the electronic Common Technical Document (eCTD), FDA Study Data Validator (SDV), and Laboratory Information Management (LIM) system / products. Army Regulation (AR) 25-2 mandates the requirement for an Acceptable Use Policy (AUP), detailing the responsibilities of each Government Information System (IS) user. Federal Government information and communication systems include, but are not limited to: government owned hardware (e.g. computers, telephones, printers, facsimile machines, scanners); government software applications (e.g. office automation, electronic mail); intranet and internet; and commercial systems, when use is paid for by the Federal Government.

2. SCOPE

All non-DoD users accessing an eIT PMO product are required to read this AUP and sign in acknowledgement, stating that they have read, understand, and accept their responsibilities regarding use of the eIT PMO's suite of IT products, as well as the information stored within the products.

3. REFERENCES AND RELATED DOCUMENTS

- AR 25-2, Information Assurance
- AR 25-4-14, Personnel and Access Security Requirements
- AR25-55, Information Assurance, Section 4-200
- AR 380-53, Information Systems Security Monitoring
- Application Security and Development checklist
- DODI 8500.2, Information Assurance (IA) Implementation
- DODI 8500.3, Identity Authentication for Information Systems (ISs)
- USAMRMC Local Memorandum 25-2-1
- Web Application Security Technical Implementation Guide (STIG) 3320 v 6130

4. POINTS OF CONTACT

Questions or comments regarding this document should be sent to the eIT PMO Mailbox at usarmy.detrick.medcom-usamrmc.mbx.eit-pmo-help-desk@health.mil.

5. MINIMUM SECURITY RULES AND REQUIREMENTS

As a Government Information System (IS) user, the following minimum security rules and requirements apply:

a. The acceptable requirements for accessing an eIT PMO Information System include:

(1) Obtain a DoD Common Access Card (CAC) or DoD-approved Personal Identity Verification (PIV) certificate. Note: Non-DoD external users must have a Government Sponsor who will approve creation of the account, verify the user meets the "need to know" requirement, and provide signature on the **eIT PMO Account Request** form.

(2) Employ virus-checking procedures before uploading or accessing information from any system, attachment, diskette, compact disk (CD), digital videodisk (DVD), or removable storage device.

(3) Will not attempt to process or store classified data in any eIT PMO IT product.

(4) Will not introduce executable code (i.e, .exe, .com, .vbs, or .bat files) without authorization, nor write malicious code.

(5) Only the organizational Government Sponsor has the authority to decide, from a business perspective, whether to store **Personally Identifiable Information (PII)** in an eIT PMO product. PII data must have a **For Official Use Only (FOUO)** label on the document, and in EDMS, will also have an EDMS PII label**.** All users posting FOUO data in an eIT PMO product must adhere to the following requirements:

- It is appropriate to access FOUO data only over an approved VPN connection. Do not access eIT Information Systems via a public computer (e.g. library, hotel lobby).

- Safeguard and mark the appropriate classification level on all information created, copied, stored, or disseminated from eIT Information Systems (e.g. FOUO).

- **NOTE**: Non-DoD collaborators should not have access to FOUO documentation unless granted access by the Government Sponsor. Users will not disseminate FOUO documents to anyone without a specific need to know, in order to prevent unauthorized public disclosure.

- Regulations require printing of documents that contain FOUO information to be marked with a **For Official Use Only** label at the top and bottom of each page when non-DoD collaborators have access.

(6) Use screen locks when away from the workstation, even for a brief time. If the workstation is not in line of sight, log off workstation when departing the area.

(7) Immediately report any suspicious output, files, shortcuts, or system problems to the Army's Global Service Center Help Desk via https://gsc.health.mil or the eIT PMO helpdesk usarmy.detrick.medcom-usamrmc.mbx.eit-pmo-help-desk@health.mil and cease all activities on the system.

(8) Understand that monitoring of the eIT PMO IS is conducted for various purposes. Information captured during monitoring may be used for administrative, disciplinary actions, or for criminal prosecution.

(9) Understand that any activity that occurs using my account is my responsibility.

(10) Understand that storage or transmission of personal medical data or Public Health Information (PHI) is prohibited within the eIT PMO's suite of IT products.

b. Unacceptable use of an eIT PMO IS includes, but is not limited to:

(1) Introducing malicious code or conducting other hacking behavior on an eIT PMO IS.

(2) Using the system to store personal files that are not used to conduct business, such a photos, videos, and/or music files.

(3) Conducting a commercial business on an eIT PMO IS.

(4) Unethical uses (e.g. profanity, sexual content, gambling, soliciting funds).

(5) Sharing of accounts.

(6) Attempting to access or transmit data exceeding the authorized IS classification level (eIT PMO's level is unclassified, sensitive).

6. ENFORCEMENT

Users that do not comply with this document will have their access suspended and possibly deleted from any and all eIT PMO ISs.

7. ACKNOWLEDGEMENT

By signing this document, you acknowledge and consent to the following conditions when accessing an eIT PMO IS:

a. The US Government routinely intercepts and monitors communications on the eIT PMO ISs for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

b. Communications using, or data stored on, the eIT PMO ISs are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

c. eIT ISs include security measures (e.g. authentication and access controls) to protect US Government interests, not for personal benefit or privacy.

d. Notwithstanding the above, using an eIT PMO IS does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work products are private and confidential, as further explained below:

(1) Nothing in this document shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any US Government action for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(2) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personal misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personal misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(3) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy.

(4) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(5) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the US Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(6) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the US Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(7) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the US Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the US Government's otherwise authorized use or disclosure of such information.

(8) All of the above conditions apply regardless of whether the access or use of an IS includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this document, regardless of whether the banner describes these conditions in full detail, or provides a summary of such conditions, and regardless of whether the banner expressly references this document.

8. ACCOUNT APPROVALS INSTRUCTIONS:

a FILL OUT AND SIGN "REQUESTOR" SECTION.

b. NON-DoD MUST OBTAIN SIGNATURE OF GOV'T SPONSOR ON eIT PMO ACCOUNT REQUEST FORM (GOV'T SPONSOR IS THE SUPERVISOR OR APPROVAL AUTHORITY OF THE BRANCH/DIVISION SPONSORING THE EXTERNAL COLLABORATION, OR HAS CONTRACT/AGREEMENT OVERSIGHT; GRADE 04 OR ABOVE, OR GS-13 OR ABOVE).

c. ATTACH AUP SIGNATURE PAGE, DoD IA TRAINING CERTIFICATE, and eIT PMO ACCOUNT REQUEST FORM and send email to the eIT PMO MAILBOX (usarmy.detrick.medcom-usamrmc.mbx.eit-pmo-help-desk@health.mil).

d. QUESTIONS, CONTACT eIT PMO AT THE ABOVE EMAIL ADDRESS.

REQUESTOR: I have read the above requirements regarding use of eIT PMO Information Systems. I understand all terms and conditions in this Acceptable Use Policy (AUP) and accept my responsibilities and accountability regarding these systems and the information contained in them.

_____ _____
Date: **Requestor Last Name, First, MI *(Print)***

_____ _____
Name of Business / Organization

_____ _____
Requestor Email Address **Requestor Phone Number**

Signature or Electronic Signature of User Requesting an Account **X** _____