Family and Morale Welfare Recreation

Mission Information Systems and Personally Identifiable Information Acceptable Use Policy

1. **Information System Acceptable Use Policy (AUP):**

   a. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in all Family and Morale Welfare Recreation (FMWR) Mission Information Systems (MIS) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

   b. **Access.** Access to each FMWR MIS is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

   c. **Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

      i. Failure to comply/violations to this AUP will result in revocation of account privileges.

      ii. Restoration of privileges for 1st offense requires endorsement from the Director of FMWR and Garrison Commander (GC). 2nd offense requires endorsement from GC and ID Director. 3rd offenses will be revoked indefinitely however, may be reinstated by the Commanding General (CG) of IMCOM.

   d. **Classified Information Processing.** No FMWR MIS is authorized to process classified information or material.

   e. **Unclassified Information Processing.** FMWR MIS are the primary unclassified automated administration tools for the IMCOM G9 and FMWR Directorates and are US-only systems.

      i. FMWR MIS is considered Public and are unrestricted. Material produced using FMWR MIS are only authorized to contain information that can be distributed to the Public and the information is unrestricted.

      ii. FMWR MIS provide unclassified communication to external DoD and other United States Government organizations. Primarily this is done via electronic mail and internet networking protocols.

      iii. FMWR MIS are approved to process UNCLASSIFIED, in accordance with AR215-1, AR25-1, AR25-2, and OMB M-17-06.

f. **Minimum Security Rules and Requirements.** As a FMWR MIS system user, the following minimum security rules and requirements apply:

i. Personnel are not permitted access to FMWR MIS unless in complete compliance with the IMCOM G9 and Directorates of FMWR personnel security requirement for operating in an UNCLASSIFIED environment.

ii. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

iii. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 14 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.

iv. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

v. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

vi. I will not attempt to access or process data exceeding the authorized Information Security (IS) classification level.

vii. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

viii. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

ix. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

x. I will not utilize Army and/or DoD provided MIS for commercial financial gain or illegal activities.

xi. Maintenance will be performed by the System Administrator (SA) only.

xii. I will use screen locks and log off the workstation when departing the area.

xiii. I will immediately report any suspicious output, files, shortcuts, or system problems to the IMCOM G9 or Directorate of FMWR System Administrator (SA) and/or Information Assurance Security Offices (IASO) and cease all activities on the system.

xiv. I will address any questions regarding policy, responsibilities, and duties to IMCOM G9 or Directorate of FMWR SA and/or IASO.

xv. I understand that each FMWR MIS is the property of the Army and is provided to me for official and authorized uses. I further understand that each FMWR MIS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the FMWR MIS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

xvi. I understand that monitoring of the FMWR MIS will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

xvii. I understand that I am responsible for ensuring that use of DoD imagery, and any alterations of Official DoD imagery, meet DoD regulations (including but not limited to: DoD instruction 855001).

xviii. I will not add JavaScript on any page.

2. Personally Identifiable Information (PII) AUP:

a. Understanding.

i. I understand that only the FMWR MIS is authorized to gather PII from patrons.

ii. I will not provide PII, or enable PII to be provided, to any un-approved tool or System as a Service (SaaS) platform.

iii. I understand that I have the primary responsibility to safeguard the PII contained in the FMWR MIS. In the case of a breach or compromise of PII information I understand the procedures and responsibility of reporting.

1. Within 1 hour, report all incidents involving the actual or suspected disclosure of PII to the US-CERT at http://www.us-cert.gov/. If computer access is not available, incidents can be reported 24/7 to 1-866-606-9580 (OAA SEC) or 1-703-235-5110 (US-CERT).

2. Immediately after reporting, send an email with the US-CERT reporting number, a brief synopsis, and POC information for the incident to: usarmy.jbsa.imcom-hq.mbx.records-management@mail.mil, usarmy.jbsa.imcom-hq.list.cyber-security@mail.mil and usarmy.jbsa.imcom-hq.mbx.operations-center@mail.mil

3. Within 24 hours, the system owner must submit a PII incident report to the Army Freedom of Information act and Privacy office at https://www.privacy.army.mil/PATS/

4. Continue to follow existing command and/or local procedures to notify the IMCOM Command Privacy and PII Officers.

iv. I understand that all PII electronic records shall be evaluated for impact of loss or unauthorized disclosure and protected accordingly.

v. I understand that all PII electronic records shall be assigned a High or Moderate PII Impact Category and protected at a Confidentiality Level of Sensitive or higher, unless specifically cleared for public release.

b. **PII on Mobile Computing Devices.**

i. I understand that electronic PII records assigned a High Impact Category shall NOT be routinely processed or stored on mobile computing devices or removable electronic media without the express approval of the DA.

ii. I understand that, except for compelling operational needs, any mobile computing device or removable electronic media that processes or stores High Impact electronic records shall be restricted to protected workplaces (workplaces that minimally satisfy Physical and Environmental Controls for Confidentiality Level Sensitive or higher as established in DoDI 8500.2).

iii. I will adhere to established logging and tracking procedures for High Impact PII electronic records on mobile computing devices or portable media when they are removed from protected workplaces.

iv. I understand that any mobile computing device containing High Impact PII electronic records removed from protected workplaces, including those approved for routine processing shall be signed in and out with a supervising official designated in writing by the organization security official (IASO, IAM).

v. I understand that any mobile computing device containing High Impact PII electronic records removed from protected workplaces, including those approved for routine processing, shall require certificate based authentication using a DoD or DoD- approved PKI certificate on an approved hardware token to access the device.

vi. I understand that any mobile computing device containing High Impact PII electronic records removed from protected workplaces, including those approved for routine processing, shall implement IA Control PESL-1 (Screen Lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended).

vii. I understand that any mobile computing device containing High Impact electronic records removed from protected workplaces, including those approved for routine processing, shall encrypt all data at rest. This includes all hard drives or other storage media within the device as well as all removable media created by or written from the device while outside a protected workplace. Minimally, the cryptography shall be NIST-certified (i.e., FIPS 140-2 or current). Refer to DoDI 8500.2 IA Control ECCR for further details.

c. **Remote Access to PII.**

i. I understand that remote access to High Impact PII electronic records is discouraged, and is permitted only for compelling operational needs.

ii. I understand that only DoD authorized devices shall be used for remote access to PII electronic records. Any remote access, whether for user or privileged functions, must conform to both DoDI 8500.2 IA Control EBRU-1 and EBPR-1.

iii. I understand that remote access to High Impact PII electronic records shall employ certificate based authentication using a DoD or DoD-approved PKI certificate on an approved hardware token.

iv. I understand that for remote access to High Impact PII electronic records, the remote device gaining access shall conform to IA Control PESL-1 (Screen Lock) from DoDI 8500.2, with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended).

v. I understand that or remote access to High Impact PII electronic records, the remote device gaining access shall conform to DoDI 8500.2 IA Control ECRC-1(Resource Control).

vi. I understand that for remote access to High Impact PII electronic records, downloading and local/remote storing of PII records is prohibited unless expressly approved by the DAA.

vii. I understand that any High Impact electronic PII records stored on removable electronic media taken outside protected workplaces shall be signed in and out with a supervising official and shall be encrypted. Minimally, the cryptography shall be NIST-certified. Refer to DoDI 8500.2 IA Control ECCR for further details.

d. **Reporting the Loss (Or Suspected Loss) of PII.**

i. I understand that loss or suspected loss of PII shall be reported to the United States Computer Emergency Readiness Team (US-CERT) within one hour. Guidance regarding such instances is published at www.us-cert.gov.

ii. I understand that the loss or suspected loss of PII must report all incidents to the Army Freedom of Information/Privacy Act Office within 24 hours. Guidance is located at www.rmda.army.mil/organization/pa-guidance.shtl. I also understand I have to notify local command officials within 24 hours which may include serious incident reports, contacting Army or RCERT, Credit Card Company, local law enforcement or public affairs office.

iii. I understand that the underlying incident that led to the loss or suspected loss of PII (e.g., computer incident, theft, loss of material, etc.) shall continue to be reported in accordance with established procedures (e.g., to designated Computer Network Defense (CND) Service Provider, law enforcement, chain of command, etc.)

e. **PII Training.**

i. I have received initial/annual refresher training on my privacy and security responsibilities. I understand that I will enroll and complete a PII privacy and security refresher training course annually.

ii. I understand that I am subject to disciplinary action for failure to properly safeguard PII, for improperly using or disclosing such information, and for failure to report any known or suspected loss or the unauthorized disclosure of such information. If I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations. I have read the above requirements regarding the use and reporting of PII for the IMCOM ASP and IMCOM CASP. I understand my responsibilities regarding PII on these systems and the information contained in them.

iii. Failure to comply/violations to this mandate will result in revocation of account privileges. Restoration of privileges for 1st offense requires endorsement from the DFMWR and GC. 2nd offense requires endorsement from GC and ID Director. 3rd offenses will be revoked indefinitely however, may be reinstated by the CG of IMCOM.

3. **Accounts Required.** Please check each system you require access to.

   □ Rectrac
   □ CYMS

4. **Acknowledgement.** I have read the above requirements regarding use of FMWR MIS. I understand my responsibilities regarding these systems and the information contained in them.

5. **Signatures.**

   a. **Requestor:**

   b. **Supervisor:**