Installation Management Command Application Service Provider (IMCOM ASP) and Installation Management Command Commercial Application Service Provider (IMCOM CASP)

Personally Identifiable Information (PII)

Acceptable Use Policy (AUP)

As a user of an Information System that processes, stores and/or transmits Personally Identifiable Information (PII), I understand and will adhere to the following PII policy:

1 PII SECURITY AND IMPACT CODES

a. I understand that I have the primary responsibility to safeguard the Personally Identifiable Information contained in the IMCOM ASP and IMCOM CASP. In the case of a breach or compromise of PII information I understand the procedures and responsibility of reporting.

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

c. 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.

2 MOBILE COMPUTING DEVICES

a. 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 DAA.

b. 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).

c. 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.

d. 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).

e. 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.

f. 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).

g. 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.

3 REMOTE ACCESS TO PII

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

b. 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.

c. 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.

d. 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).

e. 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).

f. 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.

g. 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.

4 REPORTING THE LOSS (OR SUSPECTED LOSS) OF PII

a. 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.

b. 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.

c. 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.)

5 PII TRAINING

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.

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.

User Name: _____

User Signature: _____

Rank/Grade: _____

Date: _____

Supervisor Name: _____

Supervisor Signature: _____