DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE SPACE COMMAND

Authorized Use of Flash/Removable Media User Agreement

1. My signature below indicates I understand all flash/removable media is prohibited from use on all DoD computer networks unless approved by appropriate authorities and with proper security measures in place. I further understand all write privileges to removable media from systems up to the Secret classification level are prohibited unless specifically authorized by the Air Force Designated Accrediting Authority (AF DAA) or an Alternate Approving Authority. I must obtain authorization prior to using removable media or writing from SIPRNet or Secret-level systems. The use of removable media is limited to the system/s approved by the AF DAA or Alternate Approving Authority. In addition, I have read the related AF DAA *Combined Implementation Guidance for United States Cyber Command (USCYBERCOM) Communications Tasking Orders (CTO) 10-084 and 10-133*, dated 6 July 2011, and I have had the opportunity to request clarification of any provisions which I do not understand.

2. I agree to all terms, actions, and conditions contained in the AF DAA Combined Implementation Guidance, CTO 10-084, and CTO 10-133 to include but not limited to the following:

Flash Media

a. Approval for use of flash media is specific to me and I am prohibited from allowing another person to use it in my stead. I will only use flash media in the manner specifically authorized and on the system specifically approved in the authorization request.
b. I am responsible to ensure the NSA File Sanitization Tool (FiST) and Magik Eraser (ME) are used to scan all higher-risk data transfers.
c. I am responsible to ensure flash media devices are maintained and secured at a level commensurate with the classification of the data authorized to be transferred.
d. I am responsible to ensure all flash media devices are approved through the Information Assurance Manager (IAM) prior to use and that devices are clearly labeled and traceable by an approved unique bar code or serial number.

All Other Removable Media

a. I may only use the particular removable media device specifically identified in the authorization request. I may not use any other device not specifically approved for use.
b. I will comply with published guidance for conducting data transfers between classification levels. I understand the transferring of data between classification levels normally requires implementation of a DoD-approved cross-domain solution.
c. I must ensure proper classification markings, storing, transportation, and destruction of all removable media approved for use.
d. I will provide physical protection and accountability of removable media.
e. I will follow infected removable media detection procedures IAW CTO 10-084.

f. I will maintain a log of all data transfers to include as a minimum: date/time of transfer, file types, subject, name of requestor, and any additional/pertinent information. I will provide a monthly report to the IAM.

g. I am responsible for the accountability of flash/removable media device and will immediately report the loss, theft, destruction, or malfunction to the IAM. I acknowledge and agree I must immediately report any deviations of authorized data transfers and any violations of the AF DAA Combined Implementation Guidance and related CTOs to the unit security manager and IAM.

3. For military personnel: I understand the AF DAA Combined Implementation Guidance, CTO 10-084, and CTO 10-133 constitute a lawful regulation and a proper order from my chain of command within the meaning of UCMJ Article 92. It is my duty to comply with the specific processes and provisions and that I may be punished for each failure to comply.

4. For civilian government employees: I understand the requirements in the AF DAA Combined Implementation Guidance, CTO 10-084, and CTO 10-133 constitute a lawful regulation and a proper order from my chain of command. The failure to comply with the specific processes and provisions would negatively impact the efficiency of the Air Force in the most egregious sense. Each failure to comply would immediately constitute grounds for the most severe disciplinary and adverse actions provided in AFI 36-704.

5. For contractor personnel: I understand I am prohibited from using removable media on Air Force networks/systems and from writing from SIPRNet to flash/removable media, unless I am required to do so in the course of performing duties, where such duties are pursuant to the terms of the contract under which I am authorized access to Air Force networks/systems. If contract performance requires use of removable media or write capability from SIPRNet to flash/removable media, I understand I must comply with AF DAA *Combined Implementation Guidance for United States Cyber Command (USCYBERCOM) Communications Tasking Orders (CTO) 10-084 and 10-133*, dated 6 July 2011. Each violation of the processes and provisions could affect the terms of the contract and the standing of my company with the U.S. government.

User Printed Name:

Rank and organization/employer:

User Signature: Date:

IAM Printed Name: Paul L. Ray, GS-11, DAF

IAM Signature: Date: