



REPLY TO  
ATTENTION OF:

CJ-6I/JCISA

1 July 2004

MEMORANDUM FOR RECORD

SUBJECT: GCCS-K Removable Media Policy

1. The capability to write data to removable media on a classified system presents a significant challenge to ensuring that the data is properly protected once stored in persistent form. This is especially true regarding media with large storage capacities such as Compact Disc (CDR/CD-RW), ZIP disk and USB memory sticks. The possibility to store particularly large documents or compilations of classified information represents a greater potential hazard than a standard 1.44 megabyte floppy disk.
2. It is CJ-6I/JCISA policy to not include CDR/CD-RW or ZIP drives as standard hardware, or to allow USB Memory Sticks with GCCS-K client machines. Users are allocated ample storage space on the network in the form of personal folders and public storage space that should facilitate most data storage or transfer requirements. Once stored, this data will be accessible from any client machine on the network using the appropriate credentials. In addition to the protection afforded by network storage, the data is also backed up at regular intervals. For instructions on how to store data or access stored data from the network, contact your Information Assurance Security Officer (IASO) or the CJ-6I/JCISA Help Desk (DSN 315-723-8827/8828).
3. Recognizing that there may be extenuating circumstances that do require the use of removable mass-storage media, we will evaluate each request for CDR/CD-RW, ZIP drives or USB memory sticks on a case-by-case basis. If there are no other data transfer means to meet a valid operational requirement we will evaluate requests for exception to this policy based on an organization meeting all of the requirements outlined in Attachment 1.
4. Point of contact for this memorandum is Billy E. Martin, Jr., CJ-6I/JCISA Security Division, DSN (315) 723-6684, E-mail: [martinbi@usfk.korea.army.mil](mailto:martinbi@usfk.korea.army.mil).

RICHARD J. PETRASSI  
Colonel, USAF  
GCCS-K Designated Approval Authority

## ATTACHMENT 1

### To GCCS-K Removable Media Policy

#### EXCEPTION TO POLICY REQUIREMENTS

The following requirements must be completed in full prior to CJ-6I/JCISA processing a request for an exception to policy to install and/or utilize removable media devices on GCCS-K.

1. Submit an RCR requesting an exception to policy for removable media. RCRs may be submitted by going to: [http://j6ircr.korea.army.mil/RCR/RCR\\_Frame.cfm](http://j6ircr.korea.army.mil/RCR/RCR_Frame.cfm). (NOTE: only .gov or .mil clients within the K-WAN are allowed to connect. If your unit is unable to connect via the NIPRNET call the CJ-6I/JCISA Requirements Branch at DSN 315-725-3279 for further assistance in submitting an RCR.) RCR must be validated by an O-6 (or GS-15) in your organization's chain of command.

2. As an attachment to the RCR, the following questions must be answered in memorandum format, and signed by an O-6 (or GS-15) in your organization's chain of command:

(a) Why is removable media needed?

(b) What is the mission impact if removable media is not installed or authorized for use?

(c) Why are the current network storage and data transport mechanisms insufficient to meet your organization's mission needs?

(d) Provide a Concept of Operations (CONOPS) that includes:

- How your organization will ensure there is no data "spillage"? (i.e. the unauthorized/inadvertent transfer of data to a network that is lower in classification than the data being transferred. Applies only if transferring data from a higher classification to GCCS-K)

- The tools that will be used to sanitize removable media blank space, and the types of files to be transferred. (Applies only if transferring data from a higher classification to GCCS-K)

- The steps that will be used to protect the GCCS-K network from receiving data containing malicious code? (i.e., what anti-virus steps will be taken before transferring data to the GCCS-K network?)

For assistance with developing a sound CONOPS, the Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (Chapter 18), or <https://aiaweb.lackland.af.mil/homepages/690iss/pi/toolbox/procedures.html> may be referenced as examples.

(e) Provide a complete list of the GCCS-K client hostnames on which the organization proposes to install/utilize removable media. Also provide justification for why the organization's mission requires removable media devices on multiple workstations.

3. All approved removable media hardware and disks (to specifically include USB memory sticks) must be properly labeled with the highest classification of data processed. (i.e, SF-707 SECRET Label, SF-710 UNCLASSIFIED label etc. or their equivalents). If requesting the use of USB memory sticks provide model numbers of the devices to be used. Only USB memory sticks that are capable of being write-protected will be considered for use.

4. When transferring SECRET RELROK/ROKUS data from GCCS-K network to a system of a higher classification all ZIP disks and USB memory sticks must be write protected prior to insertion in the higher-classified device if the ZIP disk or USB memory stick will be attached to the GCCS-K network again.