



HEADQUARTERS, UNITED STATES FORCES, KOREA
UNIT #15237
APO AP 96205-0010

REPLY TO
ATTENTION OF:

JCISA

30 July 2003

MEMORANDUM FOR GCCS/GCCS-K and SABRE Users

SUBJECT: Workgroup Manager Policy

1. REFERENCES:

- a. AR 380-19, *Information Systems Security*, 27 February 1998.
- b. AR 25-1, *Army Information Management*, 31 May 2002.
- c. CJCSI 673101, *Global Command and Control System Policy*, 31 December 1998.
- d. DODD 8500.1, *Information Assurance (IA)*, 24 October 2002.

2. PURPOSE. Due to the proliferation of GCCS-K workstations in the Korean theater, JCISA recognizes the need for workgroup managers at local sites. This policy will outline workgroup manager responsibilities and consequences for failure to comply with this policy.

3. APPLICABILITY. This policy is applicable to all DOD military and civilian personnel and contractors, to include Korean Nationals, using the GCCS-K network.

4. RESPONSIBILITIES. Workgroup Managers (WM) will not attempt to access files or data, or use operating systems programs, except as specifically designed or authorized. WM will not permit anyone else to use another account except his or her assigned user account. WM will not reveal passwords to anyone. WM are responsible for maintaining passwords in accordance with governing DOD regulations. WM will not leave their computer terminals unattended while logged in without the screen locked. WM will promptly report any system security abuses, abnormalities, discrepancies, incidents, vulnerabilities to the site ISSO (JCISA Security, DSN 725-5719).

5. VIOLATIONS. The following activities are considered violations of this policy:

- a. Installation of software.
- b. Installation of any hardware, without submission and approval of a RCR.
- c. Removal of screensavers.

JCISA
SUBJECT: Workgroup Manager Policy

- d. Modification of local accounts database (creating users, modifying groups)
- e. Clearing event logs (System, Security, Application).
- f. Deleting or modifying Operating System and/or Application files.
- g. Modifying permissions of Operating System and/or Application files.

6. **CONSEQUENCES.** Failure to adhere to this policy will result in immediate loss of privileges.

7. **PROCEDURES.** For an organization to request Workgroup Manager accounts on GCCS-K workstations, the forms included in the enclosure must be filled out.

a. Enclosure 1 is a sample memorandum the requesting organization may use to initiate the Workgroup Manager account requests. Each organization's justification for WM accounts will be evaluated on a case-by-case basis.

b. Enclosure 2 is the Memorandum of Agreement between the requesting organization and JCISA. Organization's commander will fill this out in entirety, to include the names of the proposed WM and the workstations which will be managed.

c. Enclosure 3 is the generic Account Request form used by JCISA. Use this form for each of the WM accounts requested.

(1) Do not fill in the "GCCS" and "GCCS-K" "Applications Requested" blocks.

(2) In the block titled "Duty Title", write "Local Administrator".

(3) The organization's Terminal Area Security Officer (TASO) must verify security clearances of each proposed WM. (An Interim Secret clearance is minimum required.)

d. Enclosure 4 is a statement of understanding that must be signed by each proposed WM.

7. **EFFECTIVE DATE.** This policy is effective immediately and remains in effect until rescinded or superseded.

8. POC for this memo is LTJG Webster, 725-5719.

4 Encls
as



RICHARD J. PETRASSI
Colonel, USAF
Chief, Joint Command Information
Systems Activity

HEADQUARTERS, UNITED STATES FORCES, KOREA
--- Appropriate Letterhead ---



REPLY TO
ATTENTION OF:

<Organization>

Date

MEMORANDUM FOR Joint Command Information Systems Activity (JCISA)

SUBJECT: Workgroup Manager Request.

1. <Organization> requests Workgroup Manager accounts for <number> local administrators on <number> GCCS-K workstations.
2. The justification for this request is as follows:
 - a. <Justification Statement here>
 - b. <Continued, if necessary>
3. Enclosed is the Memorandum of Agreement between <Organization> and JCISA, account requests for the local administrators, and the statements of understanding by these local administrators.

<Commander Signature Block>

Encl (as)

Enclosure (1)

**MEMORANDUM OF AGREEMENT
BETWEEN
UNITED STATES FORCES KOREA
JOINT COMMAND INFORMATION SYSTEMS ACTIVITY
AND
<INSERT ORGANIZATION TITLE HERE>
ON
ASSIGNMENT OF LOCAL ADMINISTRATOR PRIVILEGES**

1. Scope. United States Forces Korea, Joint Command Information Systems Activity has been tasked to provide local administrator privileges on Global Command and Control System - Korea (GCCS-K) to remote commands in order to facilitate workstation troubleshooting. This document is the agreement between JCISA and *<insert organization title here>* on the rights and actions agreed upon prior to the creation of such accounts.

2. Applicability. This Memorandum of Agreement (MOA) is effective upon signature by both parties. This MOA may be amended by written agreement of both parties or may be invalidated by either party upon written announcement.

3. Responsibilities.

a. JCISA.

(1) JCISA is, and will remain, the primary Operation and Maintenance (O&M) organization that supports GCCS-K. Primary responsibility for O&M of GCCS-K will remain with JCISA.

(2) JCISA will continue to provide Help Desk support for the GCCS-K workstation located in *<insert organization title here>* area of operation.

(3) JCISA will monitor the use of local administrator accounts and will provide internal reports of activity.

(4) JCISA will create local administrators for *<insert organization title here>* for the individuals listed in subparagraph 3.b.(2) on the machines listed in subparagraph 3.b.(3).

b. *<Insert organization title here>*

(1) *<insert organization title here>* will ensure that the individuals identified in subparagraph 3.b.(2) have the necessary knowledge, skills and abilities to effectively manage the GCCS-K clients listed in subparagraph 3.b.(3).

(2) *<insert organization title here>* has identified the following individuals as local administrators:

Name:
Rank:
DSN Phone:
DEROS/PRD/ETS/EAOS:
Unclassified Email Address:
GCCS-K Email Address:
.. .. . *repeated as necessary*

(3) *<insert organization title here>* has identified the following workstations to be administered by the individuals listed in 3.b.(2).

Workstation ID 1:
.. .. . *repeated as necessary*

(4) <insert organization title here> agrees that the following activity is cause for immediate termination of local administrator account:

- (a) Installation of software.
- (b) Installation of hardware, to include printers and Zip Drives.
- (c) Removal of screensavers.
- (d) Modification of local accounts database (creating users, modifying groups)
- (e) Clearing event logs (System, Security, Application).
- (f) Deleting or modifying Operating System and/or Application files.
- (g) Modifying permissions of Operating System and/or Application files.

(5) <insert organization title here> acknowledges that activity identified in subparagraphs 3.b.(4)(a) through 3.b.(4)(c) are changes to the GCCS-K baseline and must be documented through the Requirements Change Request (RCR) process. JCISA may allow these activities by the local administrators upon approval of an RCR submitted by <insert organization title here>.

4. **Implementation.** The terms of this agreement will become effective on the latter date of signatures in Paragraph 8 of this MOA. The local administrator accounts will be created by JCISA upon signature and password transmitted to those personnel listed in subparagraph 3.b.(2) via GCCS-K mail.

5. **Effective Dates.** This MOA shall remain in effect until the DEROS/PRD/ETS/EAOS of personnel listed in subparagraph 3.b.(2) unless specifically terminated by JCISA or <insert organization title here>, but not to exceed one year. Termination will be accomplished by written notification to the other party 30 days in advance of the proposed termination date unless both parties agree to terminate sooner, however, local accounts may be disabled at an earlier date if activity specifically listed in subparagraph 3.b.(4) is detected.

7. **Review And Update.** This MOA will be reviewed annually and as required.

8. **Signatures.**

RICHARD J. PETRASSI
Colonel, USAF
Chief, Joint Command Information
Systems Activity

<name>
<rank>
<title>

Date:

Date:

Enclosure (2)



**HEADQUARTERS, UNITED STATES FORCES, KOREA
JOINT COMMAND INFORMATION SYSTEMS ACTIVITY
UNIT #15237
APO AP 96205-0010**

JCISA

MEMORANDUM FOR JCISA Information System Security Officer

SUBJECT: Statement of Understanding For Local System Administrator Privileges

1. References:

- a. CSC-STD-002-85 (DOD Password Guideline)
- b. DODI 8500.1 (Information Assurance)
- c. CJCSI 6731.01 (GCCS Security Policy)
- d. AR 380-19 (Information Systems Security)
- e. AR 25-IA (Information Assurance Implementation Guide)

2. The following guidelines apply to all systems maintained by JCISA:

- a. I understand that DOD computer systems are for authorized, official purposes only and I will brief users on this matter.
- b. I am responsible for ensuring all users operations follow the above guidelines for my assigned area.
- c. I will not permit anyone else to use another account except his or her assigned user account.
- d. I will not reveal passwords to anyone.
- e. I am responsible for maintaining passwords in approved manner.
- f. I will not leave my computer terminal unattended while logged in without the screen locked, and will brief users to do the same.
- g. I will promptly report any system security abuses, abnormalities, discrepancies, incidents, vulnerabilities, or any other inadequate security situation, to the JCISA ISSO (DSN: 725-5719).
- h. I will not attempt to access files or data, or use operating systems programs, except as specifically designed or authorized and will brief users to do the same.

3. I understand that that the following activity is cause for immediate termination of local administrator account:

- a. Installation of software.
- b. Installation of any hardware, without submission and approval of a RCR.
- c. Removal of screensavers.
- d. Modification of local accounts database (creating users, modifying groups)
- e. Clearing event logs (System, Security, Application).
- f. Deleting or modifying Operating System and/or Application files.
- g. Modifying permissions of Operating System and/or Application files.

I hereby acknowledge receipt of my user-id and password. I further acknowledge that I have read the above guidance and will adhere to the policies to the fullest extent. I understand that failure to observe these procedures may result in a loss of access, adverse administrative action, and/or other actions as provided for in the references noted in paragraph 1.

SIGNED: _____

DATE: _____

Print Name: _____

Enclosure (4)