

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

TABLE OF CONTENTS

	<u>Page Number</u>
A. Introduction	2
B. Top Secret Security	
1. Adding a User	3
2. ID Number and Password	3
3. Suspended/Deleted ID Numbers	4
4. Deleting a User	4
C. CPPS/EMPL Application Security	5
D. COFRS Application Security	
1. Adding a User	6
2. Types of COFRS Access	6
3. Security Models	7
4. Changing a User's Security Model	8
5. Changing a User's Authorized Agencies	8
6. Deleting a User's Access	8
E. Notification Letter	9
F. Telephone and Fax Numbers Contacts	10
G. Forms	11

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

A. Introduction

These procedures address establishment of the security necessary to access specific statewide computer applications operated on the mainframe computers at the Colorado Information Technology Services (CITS)/General Government Computer Center (GGCC). The specific applications are those related to the state's personnel/payroll process, (specifically CPPS, TAPS, and ADS) and those related to the state's accounting system, COFRS. Both of these applications operate in an interactive mode, referred to by CITS/GGCC as "CICS", access to which is controlled by a security product called Top Secret Security. These procedures explain how to secure Top Secret CICS access and application access.

Establishment of Top Secret CICS access is generally performed by an agency's Top Secret Security Administrator. Prior to the implementation of COFRS, the State Controller's Office (SCO), then the Division of Accounts and Control (DOAC), performed this function for higher education institutions. With the advent of COFRS, the SCO decided it would no longer perform this function and announced its decentralization to each campus. Parallely, the Higher Education COFRS Implementation Task Force was weighing assignment of responsibility for COFRS application security for higher education feeder agencies to one central person versus to someone at each campus. Because of concerns about driving additional campus workload and the difficulty of retaining current knowledge on campus about statewide applications, it was decided that the Higher Education Fiscal Coordinator (HEFC) would be the Top Secret and the COFRS Security Administrator for the higher education feeder agencies. This decision was implemented July 1990. All security requests or issues should be addressed to the HEFC.

These procedures apply to all campus and Governing Board personnel.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

B. Top Secret Security

1. Adding a User

To turn CICS access on, the Top Secret Security Access Request Form CITS/CSS and Statement of Compliance must be processed. The form is available on the FAC web page at <http://www.sco.state.co.us/fac/Security/Security.htm> or you may contact the CITS/GGCC Help Desk. To process the form, follow the steps listed below. Telephone and fax numbers for all the parties involved in this process are listed in Section F.

- a) Complete the form.
- b) The approval section of the form must be signed by the controller of the institution to which access is requested or by the system controller if access is requested to more than one institution. The Controller may delegate approval authority to another person at the institution in writing to the HEFC. No user may approve security for his/herself.
- c) Fax or e-mail the completed form to the HEFC.
- d) The HEFC will send the form to the CITS/GGCC Help Desk.
- e) The CITS/GGCC Help Desk will assign the Top Secret code and notify the HEFC.
- f) If the request is for COFRS application security, the HEFC will work with the COFRS Helpline to set up that security and notify via e-mail the user the access code. See Section D for more information.
- g) If the request is for CPPS or ADS security, the HEFC will notify via e-mail the user of the access code. See Section C for more information.

2. ID Number and Password

CICS access to CITS/GGCC is controlled by ID number and password. CITS/GGCC assigns each user an individual ID number. When the State Controller's Office was higher education's Top Secret Security Administrator, all those ID numbers began with "DF\$". When the HEFC became higher education's Top Secret Security Administrator, the ID numbering system was changed to begin each number with a two-digit alpha code unique to each institution or system, i.e. JI or ZA. This system is still being used.

When adding a new user, CITS/GGCC assigns a password of "FROG". The first time the user uses their ID number they must change the password from FROG to a self-assigned password that must then be changed every 30 days. The sign-on screens will tell the user when it is time to change their password and will provide prompts for making the change. If a user forgets the password they assigned themselves, they may call the CITS/GGCC Help Desk to get the password reset to FROG.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

B. Top Secret Security (continued)

3. System Suspended/Deleted ID Numbers

If a password is not changed within thirty days of being assigned, it will be suspended and the user will not be able to access the CITS/GGCC computers. To unsuspend their password, the user must call the CITS/GGCC Help Desk. Users whose security was established after May 2000 will be required to provide the Help Desk with the instdata information (two passwords) that was on the Security Access Form requesting their Top Secret security.

If a password is not used, and therefore not changed, within 90 days, it will be deleted by CITS/GGCC and the user will not be able to access the CITS/GGCC computers. In that case, CITS/GGCC will not reestablish the purged security. Rather, new security must be established by following the steps listed in Section B.1.

4. Deleting a User

To turn CICS access off, the Top Secret Security Access Request Form found in Section E, CITS/CSS Security Request Form must be processed. To process the form, follow the first three steps listed in Section B.1. It is important to put the ID number of the user whose access is being deleted on the form.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

C. CPPS/ADS Application Security

The HEFC is not the security administrator for CPPS or ADS application security. The Human Resources Division of the Department of Personnel/General Support Services performs that role. However, that application security cannot be established until Top Secret security has been assigned using the process described in Section B of these procedures.

If the CPPS/ADS box on the Top Secret Security Access Request Form CITS/CSS Security Request Form and Statement of Compliance is checked, upon receiving the Top Secret ID number from CITS/GGCC the HEFC will notify via e-mail the user who signed the Request Form. With this ID number, the agency is able to complete a CPPS Security Access Authorization Request Form and/or the ADS Security Access Authorization Request Form that must be submitted to the DOP/GSS Human Resources Division, where the application security will be established.

Telephone, fax numbers and a web address for the DOP/GSS Human Resources Division, CPPS and ADS can be found in Section F of these procedures.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

D. COFRS Application Security

1. Adding a User

COFRS application security will be established if the COFRS box on the Top Secret Security Access Request Form CITS/CSS Security Request Form and Statement of Compliance is checked and a model number is indicated. Upon receipt of the Top Secret ID number from the CITS/GGCC Help Desk, the HEFC will work with the COFRS Helpline to make COFRS table entries to establish the type of access requested for that user (see Sections D.2 and D.3) and will request the COFRS Help Desk to authorize that access for the agency codes identified on the Request Form. If no agency codes are indicated on the form, only the user's home agency will be authorized for access.

When the COFRS application security has been set up, the HEFC will send notification via e-mail (see Section E) to the user who signed the Request Form and instructions to help the user sign-on.

2. Types of COFRS Access

COFRS will allow a user to add, change, delete, approve and/or read data. The Higher Education Financial Advisory Committee (FAC) determined the following combinations of access will be made available to feeder agency personnel:

- a) add/change/delete/read,
- b) approve/delete/read, or
- c) read only.

(Under unique circumstances and/or with individual approval from the system controller and/or the Deputy State Controller, other combinations of a) and b) may be allowed.)

COFRS allows these capabilities to be made available to a user for specific groups of transactions and/or tables. Those groups required by a feeder agency user are significantly fewer than those needed by a user from an agency whose original accounting or purchasing system is COFRS.

The combinations of capabilities and groups available to feeder agency users have been established as COFRS Security Models. Establishing COFRS application security consists of assigning one of these models to each individual user. The COFRS Security Models are explained in Section D.3.

Only the HEFC is authorized to establish and/or change COFRS application security. This will be done with the approval of the institution controller.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

COFRS Application Security (continued)

3. Security Models

The Higher Education Financial Advisory Committee established ten COFRS Security Models explained below.

- Model 1: Data entry, change, and/or delete all document types except MW, correct and delete MW; add records to VEND; some table capabilities; no approval capability; view all tables and records.
- Model 2: Approve and/or delete all document types except MW; no data entry, change, or table maintenance capabilities; view all tables and records.
- Model 3: Data entry, change and/or delete budget document types only; no approval capabilities; no run immediate capability; view all tables and records.
- Model 4: Approve and/or delete budget document types only; no data entry, change, or table maintenance capabilities; view all tables and records.
- Model 5: View only all documents and tables.
- Model 6: Approve and/or delete all document types except MW; no data entry, change, or table maintenance capabilities; immediate processing capability except for PB; view all tables and records.
- Model 7: Approve and/or delete budget documents; no data entry, change, or table maintenance capabilities; immediate processing capability for all budget documents; view all tables and records.
- Model 8: Data entry, change, and/or delete, and approve all document types except IT and PV; data entry, change and delete PV; approve and delete IT; some table records maintenance; immediate processing capability for all documents except PV and IT documents; view all tables and records.
- Model 9: Approve, change and/or delete all document types except PV and IT; no data entry or change for PV or IT, or table maintenance capabilities; immediate processing capability for all documents except PV and IT documents; view all tables and records.
- Model 10: Add records to the Vendor Table; view all vendor-related tables.
- Model 11: Data entry, change, and/or delete all document types **including** MW, correct and delete MW; add records to VEND; some table capabilities; no approval capability; view all tables and records. **This model is provided on a temporary basis, and only when corrections to MW documents are required.**

One - and only one - of these models must be identified on the Top Secret Security Access Request Form when it is submitted to the FAST for processing.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

D. COFRS Application Security (continued)

4. Changing a User's Security Model

Requests to change a user's COFRS Security Model must be made in writing or via e-mail to the HEFC. Requests must be made by the agency controller or his/her delagee. No user may request changes to their own security. A new Request Form does not need to be submitted.

5. Changing a User's Authorized Agencies

Requests to change a user's authorized agency(ies) must be made in writing or via e-mail to the HEFC. Requests must be made by the agency controller or his/her delagee. Requests for access to multiple agencies must be submitted by system office personnel. No user may request changes to their own security. A new Request Form does not need to be submitted.

6. Deleting a User's Access

Requests to delete a user's COFRS application security must be made in writing or via e-mail to the HEFC. Requests must be made by the agency controller or his/her delagee. All requests must be followed by a Request Form for deletion of Top Security access per Section B.4.

If the deletion must happen immediately and the HEFC is not available, requests may be made to the COFRS Help Desk. Alternately, a Request Form for deletion of Top Security access, completed per Section B.4, may be faxed to the CITS/GGCC Help Desk.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

E. Notification Letter

TO:

FROM: Vicki Nichol, Higher Education Fiscal Coordinator

DATE: November 20, 2008

SUBJECT: COFRS Security

Recently, your institution authorized you to have access to GGCC/COFRS/CPPS. Your assigned User ID number is XXXXX. This code is private. Please do not share this code with anyone and take care not to record it where someone else might see it.

The first time you sign on to COFRS, your **password** will be the word **FROG**. Type in FROG on the first password line and then tab down to the second password line. Type in your own personally chosen password and press <ENTER>. Your personally chosen password is valid for thirty days. The system will prompt you when it is necessary to choose a new password. If you do not sign on to COFRS within any 30-day period, your password will be suspended. Should that occur, please call the CITS help line at 303.239.4357 option 5, to get your password re-activated. If you do not sign on to COFRS during any three-month period, your COFRS ID number will be deleted. You will need to contact your institution controller and resubmit original paperwork to get a new COFRS ID number created.

The COFRS Help Line phone number is 303.239.4357 option 2, and their e-mail is cofrs.helpdesk@state.co.us. This number and e-mail address is also on the COFRS General Message Screen. Please contact them if you experience any problems using COFRS. They will also contact you when your Document Direct and or Financial Data Warehouse access is established if applicable. That should occur within the next few days. Please contact the Helpline if you are not contacted shortly regarding that access.

If you are having communication problems with the system, please check with your ADP people before calling either the CITS or COFRS help lines.

Feel free also to contact me with any questions

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

F. Contacts

Vicki Nichol
Higher Education Fiscal Coordinator
Campus Box 436 UCA
1800 Grant St. Suite 600
Denver, CO 80237
PHONE: 303/837-2150
FAX: 303/837-2162
e-mail: Vicki.Nichol@cu.edu
Forms and instructions available at:
<http://www.colorado.gov/dpa/dfp/sco/fac/Security/Security.htm>

Coleene Smith
Human Resources Division, CPPS
Department of Personnel/General Support Services
1313 Sherman, Room 319
Denver, CO 80202
PHONE: 303/866-3810
FAX: 303/866-4138
Forms and instructions available at:
<http://www.colorado.gov/dpa/dfp/sco/payroll.htm>.

Chandra Williams
ADS
PHONE: 303-866-4642
FAX: 303/866-2122
e-mail: HR.support@state.co.us
Forms and Instructions available an:
<http://www.colorado.gov/dpa/dfp/sco/payroll.htm>.

DoIt
CITS/GGCC Help Desk
PHONE: 303/239-4357 option 4
FAX: 303-239-4609

Sue Schiffmacher
COFRS Help Desk
PHONE: 303/239-4357 option 2
FAX: 303/239-5888
e-mail: cofrs.helpdesk@state.co.us.

DEPARTMENT OF HIGHER EDUCATION FEEDER AGENCIES
SECURITY PROCEDURES FOR CICS ACCESS TO CITS/GGCC

Issued 1/15/97; Revised 11/20/08

G. Forms

Because the revised Security Procedures are available on the FAC web page, the forms are not included in this document.

- A. The CITS/CSS Security Request Form and Statement of Compliance are available at: <http://www.colorado.gov/dpa/dfp/sco/fac/Security/Security.htm>.
- B. The CPPS Advance Data Security Access Authorization Request Form is available at: <http://www.colorado.gov/dpa/dfp/sco/payroll.htm>.
- C. The ADS/EMPL Security Access Authorization Request Form is available at: <http://www.colorado.gov/dpa/dfp/sco/payroll.htm>.

<p>COFRS TOP Secret Security ID (CITS/CCSS)</p> <p>Use form: Department of Higher Education Feeder Agency Security Request and Statement of Compliance</p> <p>A Top Secret Security ID is required before access will be granted to any of these systems:</p>		
<p>COFRS Production (Financial – CITS/CSS) Security Access</p> <p>Use form: Department of Higher Education Feeder Agency Security Request and Statement of Compliance</p>	<p>CPPS Security Access</p> <p>Use form: CITS/CSS Security Request Form and Statement of Compliance</p>	<p>ADS/EMPL Security Access</p> <p>Use form: ADS/EMPL Security Access Authorization Request Form and Statement of Compliance</p>