Agency Request for
OITS-Administered Mainframe RACF Access or UserID

Check with YOUR agency's IT Security to learn your agency's procedure for obtaining mainframe access.

Many agencies have their own form or procedure for obtaining access. IF THIS IS THE CORRECT FORM, read page 2, then complete Applicant Information (Part I) and Mainframe Access Requirements (Part II) below. Direct questions to the number below, or 1-800-722-3946. Send the completed form to:

Mainframe RACF Administration Telephone: 919-754-6169
Department of Information Technology / Service Support / Hosting
P.O. Box 17209
Raleigh, NC 27619-7209

Part I - Applicant Information

To be completed / signed by agency representative who is approved to request changes or additions to mainframe access:
. Signature: _____ Printed name: _____ Date: _____

Person to receive access:

Legal Name (First, Middle, Last name): _____ Nickname: _____

Organization / Division / Unit, etc.: _____

Phone number(s) to contact user: _____ _____ FAX: _____
E-Mail
Address: _____ _____

==========

Employment Status: (Check one)
State Employee: _____

Contractor: _____ Firm: _____ Contract Expires: _____

Vendor: _____ Firm: _____ Contract Expires: _____

Other (Explain) _____Until what date: _____

==========

Supervisor Signature: _____ Supervisor name printed: _____ Date: _____
Higher-Mgt Signature: _____ Manager/Director printed: _____ Date: _____
Note: Both the Supervisor and Higher Management signatures are required.

Part II – Mainframe Access Requirements Check One: Create ID: ____ Change ID: ____ Remove User: ____
Specify ID: _____

Type of UserID (Check One): To be used by Applicant: ___ or Batch job: _____
Access to be used for transfer of file(s): Yes ___ No ___
UserID needed
For Access to: _____
(Identify at least one specific application – Examples: NCTE, NCAS, PMIS, STARS, etc.)
Special Access
Requirements: _____
Notes or (Be Specific)
Comments: _____
If there is another existing UserID that has the access needed, enter that information here.

= **Reserved for OITS Mainframe Security Use** = = = = = = = = = = = = = = = = =

Completed by: _____ Date: _____
RACF RACF
UserID: _____ Ticket: _____ Owner Group: _____

Additional Information

General UserID Information

Personal OITS **RACF (Resource Access Control Facility)** UserIDs are assigned to an individual for his/her own work use. Each individual user is personally responsible for his/her own UserID and how it is used.
Use of a personal OITS RACF UserID is **NOT** to be shared with anyone.

In some cases Part III of this form is required for approval of access. See the last two paragraphs below.

OITS RACF UserIDs assigned to contractors, vendors, or temporary employees must have a finite automatic shutdown (revoke) date associated with the UserID.

Some secure applications and resources have special access controls that allow access only to specific UserIDs that must be defined to the application **before** attempting to access it. A mainframe UserID must exist before access to other applications can be added. Once the UserID is available for use, it can be connected with proper approval to other application(s) to which it needs access. If you encounter difficulties while trying to access a specific application, contact the owner of that application or the OITS Service Desk (**1-800-722-3946 or 919-754-6000**) for guidance on how to get your UserID active in that application.

The application owner is responsible for deciding who receives access and what level of access is allowed. The OITS Security Office cannot and will not grant access to any application without the knowledge and concurrence of the application owner.

A good example of a secure application is the North Carolina Accounting System (NCAS). NCAS is owned and maintained by the Office of the State Controller (OSC) and functions as a common accounting mechanism shared by most of State government. NCAS is a large shared application that has a two tier access control structure that was purposely designed to keep State agencies away from each other. It also has a mechanism that limits what individuals within an agency are permitted to do. Your UserID must be connected to a special RACF Group before you can see the CICS logon screen for NCAS. After you get logged on, additional identities must be furnished to identify who you are and what you are allowed to do inside NCAS.

There are many applications that operate in the same fashion as NCAS. When you encounter one of them and have an actual need to get to it, contact the application owner to find out what needs to be done to set up your access. Contacting the application owner is always a wise first step.

ITS Agency Request Part III or Application Owner form

Some application security is set up in a manner that allows OITS to connect access to the userID after the application owner has approved. In this case, Part III of this request form will need to be signed. See additional page, **ITS Mainframe Access or ID – Agency Request Part III**.

In other cases, the application owner will connect the access to the new userID. In this case, the **ITS Mainframe Access or ID – Agency Request Part III** form is NOT needed; ask the application owner for whatever form the application owner needs. This is another reason to contact the application owner when needing access.