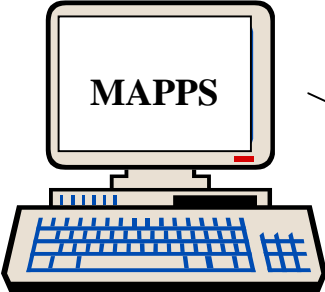


# OVERVIEW OF MAINFRAME APPLICATIONS (MAPPS)

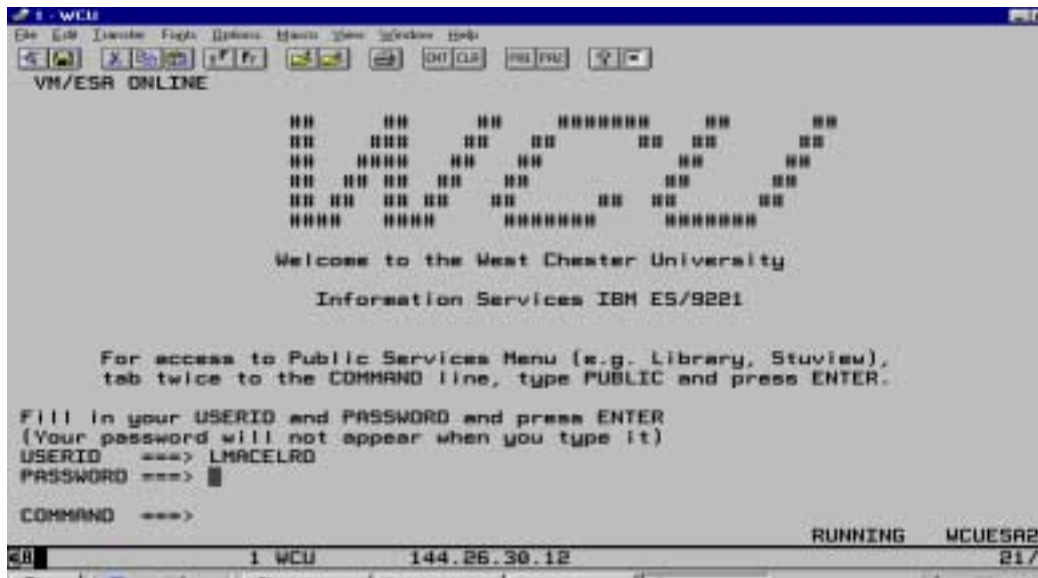


<b>Mainframe Server</b>	
Accounting	Report Req Sys
Admissions	Payroll
Advisement	Personnel
Budget	Public Safety
Career Dev.	Query Systems
CMS	Registrar
Degree Audit	Space Mgmt.
Facilities	SSI/Bookstore
Financial Aid	STUVIEW
Graduate Off.	Student Accts
Housing	FACVIEW
Inventory	

Prepared by Administrative Computing  
Revised 11/2000

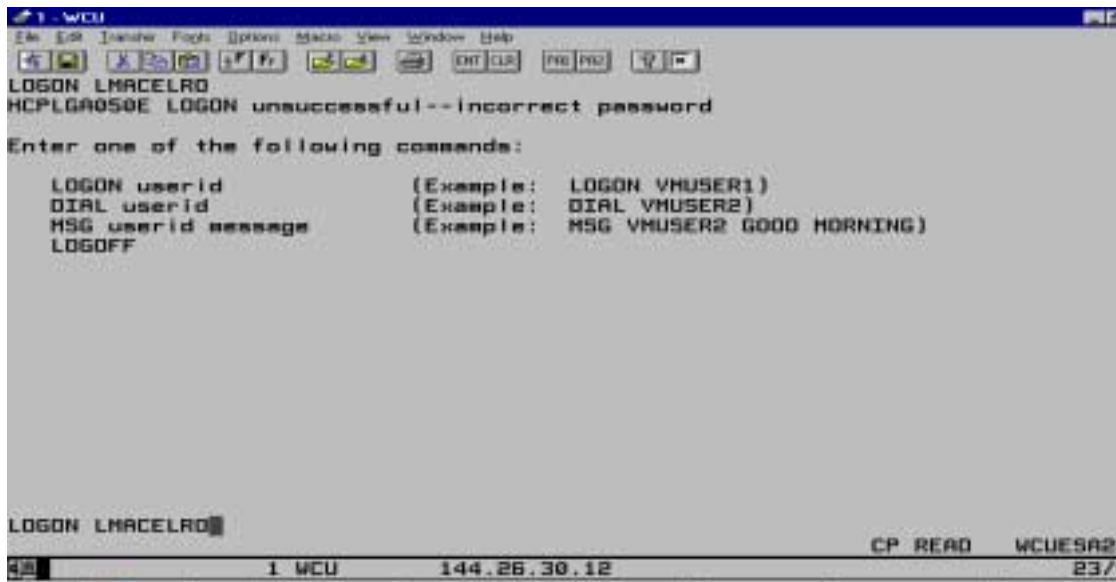
A) **Logging on to the Mainframe:** To log on to the mainframe, you must enter your user id which consists of the first initial of your first name and up to seven letters of your last name (example: John Smith JSMITH). Once your user id is properly entered, you will be prompted to enter a password. Each user creates his/her own private password which is entered at the password command line. Please note that the cursor will move; however, the password will not be visible.

It is important to remember that when creating a password, you must use at least four (4) but not more than eight (8) characters (letters and/or numbers). No spaces may be used in your password. (Hint: Try and develop a system that will make your passwords memorable to you, e.g. a pet name with the month - spot01, spot02, etc.) Do not disclose passwords.



(NOTE: If you forget your password, you should present identification to an operator in E.O. Bull Center, Room 105 in order to have your account reset.)

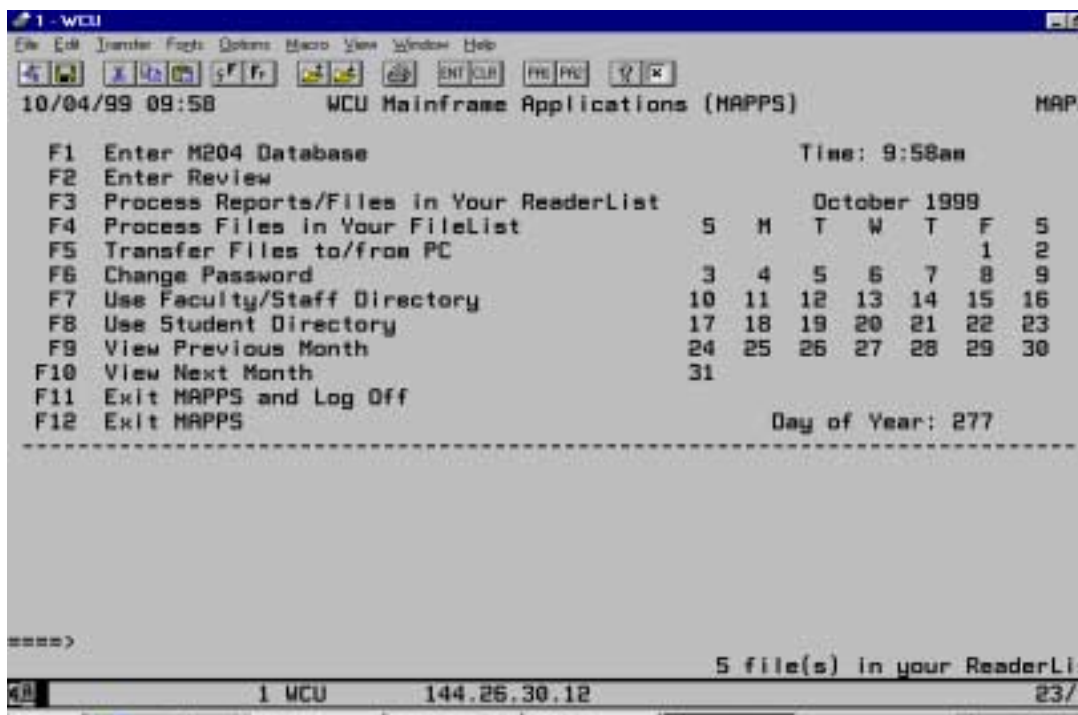
If your initial login is unsuccessful, you will see a screen like the one shown below. Simply type the following commands: LOGON<space>USERID(your id)<ENTER>



At this point, you will be prompted to enter your password. (**NOTE:** After eight unsuccessful attempts, your account is locked and an operator will need to intervene and reset your password for entry to the system. See directions on previous page for having account reset. This lockout feature is to ensure account security is not breached.)

Once your password has been accepted and your mainframe session has been established, you will see the MAPPS screen shown below. MAPPS is the "home base" for mainframe applications.

The system will prompt you to change your password(s) approximately every 30 days. The system will not allow you to use your previous two passwords. Please see "Model 204 Database Security" included in this packet.

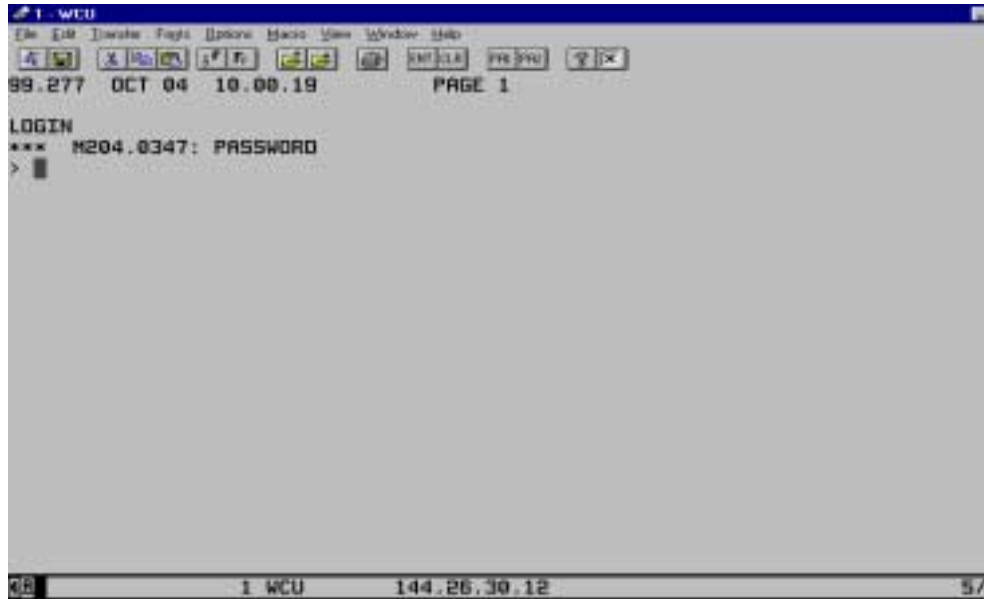


The function options located to the left of the MAPPS screen are keys to a wealth of helpful information.

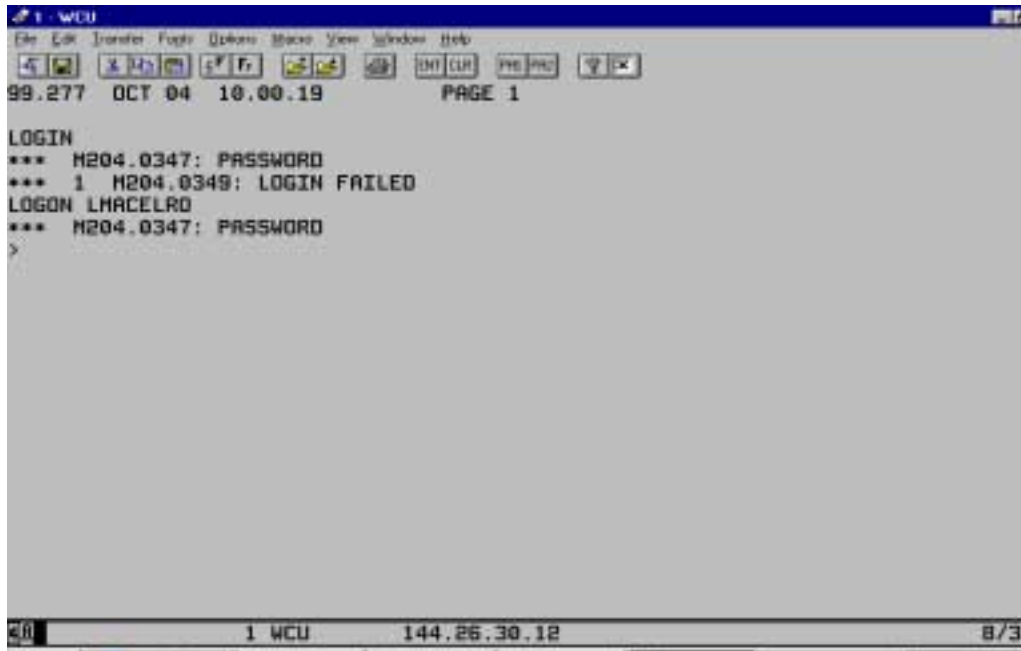
**Changing your Password:** The F6 function key gives users the option to change their password, as they feel necessary. By pressing the F6 key, users are prompted to enter their current password, then enter their new password once, then once again for confirmation.

Users are able to view the previous month to the right of the MAPPS screen by pressing the F9 function key, as well as to view the next month by pressing F10.

B) **Accessing Model 204:** Model 204 is accessed by pressing the F1 key at the MAPPS home menu, at which point you will see the screen below prompting for another password created by individual users for their private use.

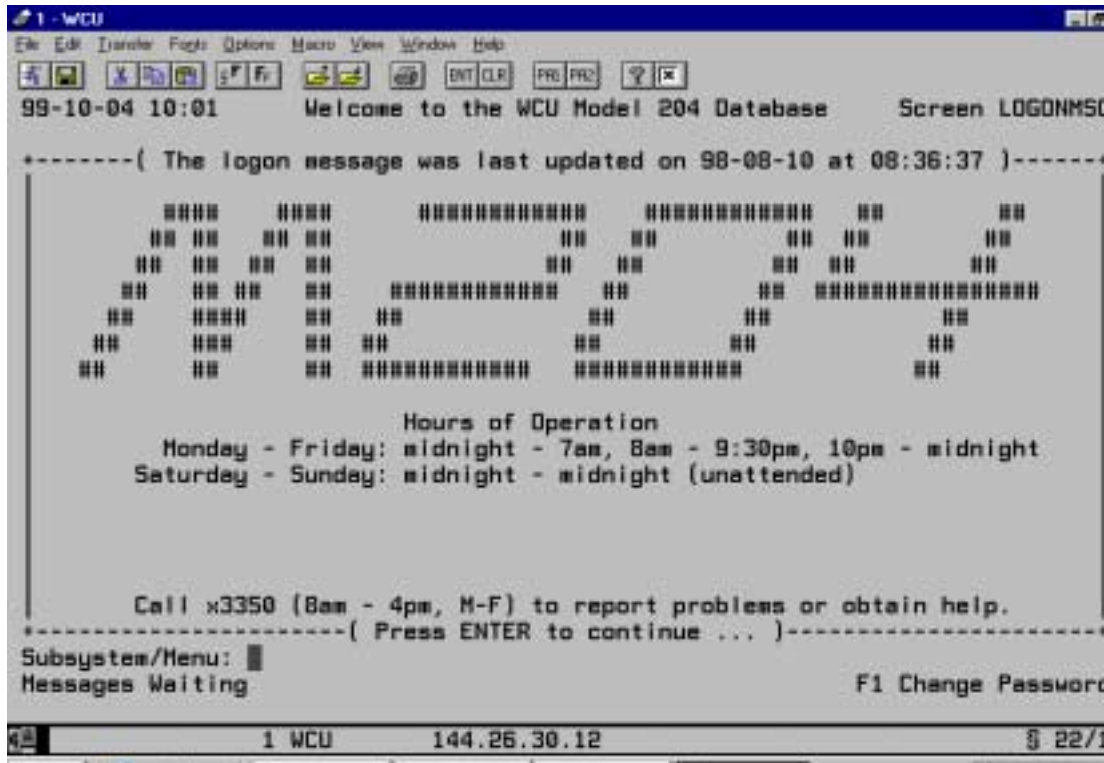


Enter your M204 private password and press the enter key. If you type the incorrect password, you will see the following screen. To successfully login to M204, you must type the following: LOGIN<one space>USERID(your id)<ENTER> (See below)



At this point, you will be prompted again to enter your password. If you are unsuccessful in your efforts, type LOGOFF <ENTER>.

Once you are successfully logged into M204, the M204 logo screen will appear. Hours of operations, special announcements, and help information will be displayed on this screen. Press ENTER to continue.



Like your "MAPPS" password, your Model 204 password will expire in approximately 30 days.

- C) **Logging Off from the Model 204 Database:** You may log off the database from any M204 menu. The last menu option on each menu screen is END (i.e. leave the subsystem and exit the 204 database). You will be returned to MAPPS.
- D) **Exiting MAPPS and Logging Off:** To exit MAPPS and log off the mainframe, press the F11key from your MAPPS menu. You will be returned to WINDOWS.

## KEYS TO REMEMBER

The Database contains information on the people, classes, facilities, etc. that make up the University.

You are given access to a subset of that data. Much of the data can only be viewed by you, while other data may be changed or added. Any data you change or add will become available immediately to others who also have access to that data.

There are just a few things you need to know to operate the system. It is reasonably easy to use because menus identify all the screens you may use. You simply select the number of the menu item you wish to use.

The chart below will show you a few special keys you will need to remember in order to use the Database.

### Useful keys:

ENTER Key	Press to enter data or to continue to the next screen. The ENTER key may be labeled RETURN on some keyboards.
F12 Key	Press to back out of a transaction or menu.
TAB Key	Press to move the cursor to the next prompt on the screen.
F1 Key	This is the HELP key. Press this whenever you want more instruction about what to enter at the current prompt.
CURSOR Keys	Press these arrow keys to move the cursor around the screen. The left and right arrows are especially useful.
BACKSPACE Key	Deletes the character preceding the cursor.
GRAY MINUS Key	Erases all characters to the right of the cursor. SHIFT/BACKSPACE may be used in the same way.
DELETE Key	Located at the bottom right of your keyboard. This key allows the user to delete the character which is positioned above the flashing cursor.
INSERT Key	Located at the bottom right of your keyboard. When this key is pressed, you are in the Insert mode. You may Insert characters at the position where your cursor is flashing. Press the Insert key to exit from this mode.
CTRL/ESCAPE	Displays the WINDOWS Task List (The list of currently running programs).
ALT/ENTER	Makes M204 a window.
ALT/TAB	Switches between running programs under WINDOWS. If one holds the ALT while tapping the TAB key, Windows displays the names of each program. One can switch to the displayed program by releasing the ALT key. This is handy when a number of programs are running.
Gray + Key	Refreshes mainframe screen when one switches back to the mainframe from a Windows application.

## TROUBLE TIPS and REMINDERS

Below are a few tips if you encounter "trouble" situations when working on the mainframe. If you try these tips and nothing seems to work, call the Help Desk at x3350.

<b>PROBLEM</b>	<b>ACTION</b>
The word <b>MORE</b> appears at the bottom right hand corner of your screen.	Press the <GRAY+> key to clear the screen.
The word <b>HOLDING</b> appears at the bottom right hand corner of your screen.	Press the <ENTER> key to clear the screen.
<b>CP READ</b> appears at the bottom right hand corner of the screen.	Type ipl cms and press the <ENTER> key twice, OR Type logoff and press the <ENTER> key twice.
After logging into the mainframe, you get a message: Reconnected at (time, day, date).	Type begin and press the <ENTER> key twice. OR Enter logoff, which resets your account and returns you to the network menu. Then double-click once again on the mainframe icon.
<b>VM READ</b> appears at the bottom right hand corner of your screen.	Press the <ENTER> key.
Inadvertently exited the MAPPS menu.	Type MAPPS and then press the <ENTER> Key.

### Reminders:

<b>User ID</b>	First initial and first seven letters of last name
<b>Passwords</b>	At least four but not more than 8 alpha, numeric or alpha-numeric characters.
	<b>DO NOT DISCLOSE</b>
	Password is required for MAPPS; password is required for M204. You may use the same one for both.
	You will be prompted to change your password every 30 days.
	Forget your password or locked out of system - Present valid ID to Operations at E.O. Bull Center, Room 105
<b>Exit</b>	F12 will exit you out of M204 screens
	F11 will exit and log you out of MAPPS
<b>Questions</b>	Call Administrative Computing at x3482

## MODEL 204 DATABASE SECURITY

There are a number of security features built into the mainframe administrative systems which protect you and which make it very difficult for unauthorized persons to gain access to data. The following briefly reviews these features and explains what responsibilities you have in protecting University data.

**Limited Access:** Information processing systems have been designed such that each user must be explicitly authorized for access to various levels of access. For example, not all users who have access to the IBM have the ability to get to the 204 database. Even when a "link" is authorized, users are limited to a series of menus, which define only the set of transactions that they require.

Many users are limited to query-only menus, which allow them to look at data but not to make any changes. Users who can update data are limited to changing only that data for which they are directly responsible.

**Individual Responsibility:** each user has been given personal logon accounts and passwords through which information systems can be accessed. A great deal of responsibility accompanies the ability to access the 204 database, and each user is responsible for processing that is done through his/her account.

Information in the database belongs to the University; it is valuable - the collection and processing costs millions of dollars annually; some of the information is confidential and/or sensitive; and information systems are integrated such that many offices depend on the accuracy of data collected in any office.

Each user is expected to maintain strict security of his logon accounts and passwords, and to provide physical security to any terminal that is logged into the database. User accounts and passwords are never to be shared or given to another user. Terminals should be logged off when not attended.

The ability to access data implies the responsibility to use the data in an appropriate manner. As a general rule, data is not to be given to an outside agency unless it is provided through MIS, and specific data relative to an individual is to be made available only to him or to his professors or various offices who need to see the data. It is a good policy to assume that any personal data is not to be made available to anyone unless they have a legitimate reason to need the data.

Many update transactions capture an individual's initials and a date in order to create an audit trail showing which person entered or changed the data. This feature is for the protection of individual users as well as for the purposes of accountability.

**Passwords:** Passwords are the primary level of security. Every user is required to provide a password in order to log into the IBM system, and a second password is required to enter the 204 database. Each user has his own password, which he is responsible for keeping secure. Passwords must be kept secret and periodically must be changed.

Passwords at the IBM system level and at the database level expire automatically every 30 days, which forces users to change their passwords.

It is imperative that passwords never be given to another person or written down where someone is likely to find them. If the security of your password is compromised, the password should be changed immediately. Remember - each person is responsible for processing done with this account. Passwords will not normally be given out over the telephone.

**Menus:** Once a user has successfully logged into 204, a monitoring system allows access to only those transactions that have been defined on a menu or series of menus for the user. The monitoring program will not allow access to any transactions that have not been explicitly authorized by the Analyst who set up the menu, and users cannot open data files directly or define code to do ad hoc processing. Users are logged out of 204 when they select the "END" option on a menu.

The object of these security measures is to protect University data. At the same time, every attempt has been made to prevent necessary security measures from being an obstacle in using the systems. Hopefully, you will find that security is adequate without being a burden.

### **The Release of Student Information:**

The Family Education Rights and Privacy Act of 1974 (FERPA) governs the release of student information.

1. Confidential student information may be released to authorized agencies or individuals only upon the student's request. Directory information, however, may be released to anyone as required to support objectives of the University.
2. Directory information includes the following: student's name, address, telephone number, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, date of attendance, degrees and awards received, and the most recent previous educational agency of institution attended by the student.
3. There are instances in which individual students may not want any directory information released without their prior written permission. In that event, all directory information is withheld from disclosure. Students may not request only selected items of directory information be withheld or request that it be withheld only in certain circumstances. This is recorded on the student's record by the following designation, <R>, which appears immediately after the social security number.
4. Access to student information, both in the computer and on paper, should only be permitted when specific duties or assignments require it.

Because of the FERPA amendment, it is not permitted to discuss a student's record without the student's approval or if the parents have declared their son/daughter as a dependent on their income tax forms and a copy is on record in the Office of the Registrar.

A student's record should not be discussed with another faculty member, unless that faculty member has an educational need to know. You will have to use your best judgment in this matter.

If you are ever in doubt, please contact the Office of the Registrar with any questions that you may have.