



SCT Banner Role Level Access Policy & Procedures

1. Authorization to Use Banner Systems

There are several levels of security associated with using Banner systems.

All users must have:

- a) An Oracle ID. (The Banner Account Request Form /Access Request Form is available in the Information Technology Department.)
- b) Authorization for each Banner form to be used. The set of forms a user needs is determined by the functions the director or department head pre-approves.

1.1. Proper Use and Banner System Information Privacy

Access to Banner systems is restricted to those who require access in order to fulfill their job responsibilities. The director (or designee) for each department makes the final determination as to what access is granted.

Users who are granted access to the Banner systems are responsible for protecting their access privileges. Violators may be subject to disciplinary action.

Information in the Banner systems is considered confidential and must be handled accordingly. Information obtained from the Banner systems should never be shared outside the workplace or used for any purpose that is not related to the users assigned job responsibilities.

1.2. Getting Authorization

1.2.1. Initial Authorization

To obtain access to any of the Banner modules, a Banner Account Request Form/ Access Request Form must be submitted to the Role Level Security Officers, Cook ADM 101. The request must be approved and signed by the director or department head or it will not be processed.

1.2.2. Updates to Existing User ID

If an existing user ID needs to be modified to grant access for additional forms, the update must be approved, in writing, by the director or department head.

Users are required to identify themselves to the Banner systems by supplying a user ID and password.

Banner sign-on enables tailored access based on the user's job function. Therefore, logged on sessions should never be left unattended.

Users should change their passwords periodically. When users forget their passwords, a "request for a password reset" must come from the appropriate director or department head.

Call 995-3963 or send e-mail to helpdesk@csu.edu with questions or comments regarding these procedures.

1.3 Choosing Passwords

Passwords must be a minimum of six characters in length and should contain at least one number. (Note: Passwords cannot begin with a number)

Choose one that is easy to remember, but hard to guess.

Never write passwords down.

1.4. Changing Passwords

For security purposes, passwords should be changed frequently. Passwords will need to be changed for each applicable database/instance (i.e. PROD).

1.4.1. How to Change the Password

1. Logon to using the current Banner Password.

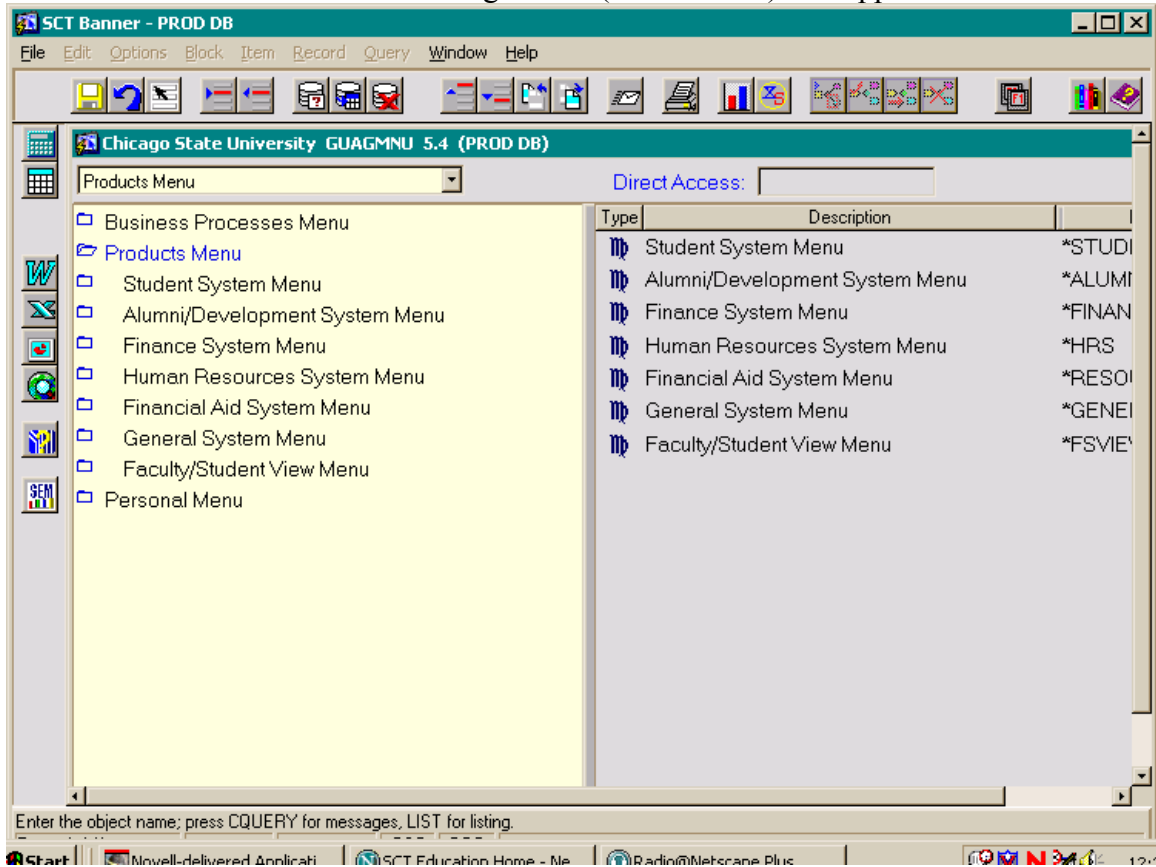


The image shows a Windows-style dialog box titled "Logon". It has a blue title bar with a close button (X) in the top right corner. The dialog box contains three input fields: "Username:" with the text "username", "Password:" with "*****", and "Database:" with "prod". At the bottom of the dialog box, there are two buttons: "Connect" and "Cancel".

Type the User ID in the Username box.
Type the current Password in the Password box.
Type instance (PROD, MIGR, or TEST) in the Database box.
Click Connect.

2. On the Banner Menu, enter GUAPSWD in the Direct Access

3. The Oracle Password Change Form (GUAPSWD) will appear.



- Type current Oracle password.
- Type new Oracle password.
- Verify new Oracle password.
- Click Save.
- Click Exit.