Security Roles and Responsibilities

Security Administration:

There are ways to change security for the end user without having to go through the rigors of security maintenance tasks. Actions that would require this type of change are:

- A new or non-employee is hired
- An employee transfers within the organization and their job function changes
- An employee leaves or terminates from the organization
- An employee job function changes without a transfer and needs to have access rights removed or added.

All of these changes can occur without any design impact to existing security objects. The security administrator would use existing roles to either add or remove from the user profile.

The security administration function will be performed by each specific institutional resource responsible for the specific duties for security. This will include the addition, update and removal of User Profiles from the system. The updates to User Profile will be restricted to the use of existing security objects (roles/permissions) as delivered with the security model.

1. **Local security administration (institutional) is assigned to one or more institutional users through the role *BOR Security Administrator*.**
2. **Local security administration functionality includes the following areas.**
    a. **Institutional User Profile Maintenance**
    b. **Institutional Role Maintenance**
    c. **Institutional Permission List Maintenance**
    d. **Department Security Maintenance**
    e. **Password Controls**
    f. **Account Lock Out**
3. **Board Of Regents security administration functionality includes the following areas:**

    a. **User Profile Maintenance (Security Model only)**
    b. **Role Maintenance**
    c. **Permission List Maintenance**
    d. **Password Controls**
    e. **Query Access Maintenance**
    f. **Single Signon**
    g. **Portal Security**
    h. **Definition Security**