Understand Security Roles

Security Roles

Security roles allow system administrators to create a grouping of permissions that can be assigned to users. These permissions determine what users can access and do within the system. Security roles are used to both grant and restrict users' access to data.

> If a user doesn't have the permission to access a specific area they will see a Restricted Area message.

Roles may be constrained to limit a user's permission to a specified area. A constraint can be general to the permission or specific to the user's Division.

> Administrators can review permissions and edit constraints at the user level by accessing the individual's User Record.

Dynamic Security Roles

A dynamic security role is one that is automatically assigned or removed when a user joins or leaves an organizational unit.

Security Roles are in a hierarchy with the System Administrator role at the root because it contains all system permissions. Other dynamic security roles are:

- **Default Role for Every User in the System** - This role is automatically assigned to every user when they are added to the system.
- **Approver** - This role is responsible for approving training and is automatically assigned to a user when they are listed as another user's approver.
- **Manager** - This role is automatically assigned to a user when they are listed as another user's manager. They are responsible for approving training for direct reports.
- **Cost Center Approver** - This role is responsible for approving training.
- **Instructor** - This role is automatically assigned to a user when they are made an instructor in the system.

Access Security Role Administration

1. Open the **Admin** tab in the menu bar and select **Security** in the dropdown menu.
2. Select the **Expand** button **.**
3. Select the **Users** button to view whom is assigned to a role.
4. Select the **Edit** button to view the Role Details.
5. Select **Next** to view the Role Permissions.
6. Select **Next** to view constraints.