

Library Security Application Security Guidelines

- ❖ All Academic Affairs customers are to be set to the NULL (Security Level) setting, when added to Shared Data. Since these customers do not use the LFOLKS web site, this setting should NOT be changed.
- ❖ All "No name/job related" customers are to be set to the NULL (Security Level) setting, when added to Shared Data. Since these customers are just for inventory tracking, this setting should NOT be changed. AN EXCEPTION: SHARED/CIRC, COPY, CPMC, MEDIA, RBR, SPCOLL logins would be used by SA's at public desks would receive the Web Only setting.
- ❖ All Library customers are to be defaulted to the Web Only setting, when added to Shared Data. Also, all Library customers will have their Initial Login record set to Web Only when added to the Library Web Apps Security module. They only need a Login record, if their access is going to be Web Only.
- ❖ All security level change requests for Library customers above Web Only will require a justification and evaluation by IDT before a change can be made.
- ❖ User Level will require the Library customer to have Maintless Level in at least one other CF/Oracle Web Application. User Level will only see the modules processing report programs (Not support program reports).
- ❖ Maintless Level will be used primarily by - Student Assistants working for a Library Customer, who has at least Maint Level in the same CF/Oracle Web Application. IDT will use this level, where multiple levels of maintenance are needed.
- ❖ Library customers whose primary responsibility is the health of the data collected will use Maint Level.
- ❖ Application administrators will use Admin Level.
- ❖ DBAdmin Level will be used for Database and System administrators.