

## PeopleSoft Access Authorization Rules

1. Access within the PeopleSoft applications will be job based. That is, each individual that is requesting access to systems will be provided with only the access needed to perform his/her job. No additional access will be granted as a “backup” to another user. If there is a need for a user to temporarily fulfill the duties of an absent user, a request for a temporary Operator ID must be submitted including the anticipated end date.
2. Access authorization will be accomplished by granting jobs one or more "operator classes", groups of menus and panels with defined privileges. Jobs will not be given access to menus and panels outside of operator classes.
3. The Security and Confidentiality Requirements Statement on the Request Form is a necessary notification of the security expectations of users. Users must acknowledge the statement each time they are given access to an operator ID or have modifications made to existing access. All active users also will receive an annual reminder of the requirements.
4. Users must be provided functional training before given access to the PeopleSoft application. This training can be administered through a formal training session or by a qualified end user who is able to provide adequate instruction and assistance. By signing the “Request for Peoplesoft Operator ID” form, the supervising authority warrants the user has received appropriate training.
5. People who are not LCTCS employees may be given access to the PeopleSoft applications for specific periods of time not to exceed one year when they are sponsored by LCTCS or one of the campuses within the LCTCS System.
6. Passwords for operator IDs will be issued to individuals and may not be shared under any circumstances. It is recommended that passwords be changed immediately when a new Operator ID is issued and **every 30 days** thereafter. Instructions will be provided for changing passwords. Problems with changing passwords should be reported immediately to the IT security office.

7. A user's access to an operator ID will be terminated when: his/her employment status terminates, he/she no longer needs it to perform job responsibilities or when his/her continued access constitutes a risk to the information technology resources of LCTCS.
  
8. Upon termination of an employee or contractor from a program (college) or agency (LCTCS systems office), the human resource officer of the employee's agency or program must notify or cause their respective agency/program Institutional Security Officer and the LCTC Security Administrator to be notified of the separation. Please refer to, *Guidelines and Timeframes to Notify Information Systems of Separated Employees*.
  
9. The IT security office must be notified when an employee changes job functions, positions and campus locations. An Operator ID Request form must be completed indicating the required modifications to the Operator ID.