



## Business Process For PeopleSoft Access Requests

The PeopleSoft Access Form must be completed and approved for each employee who needs PeopleSoft access.

**Business Process:**

1. The employee’s supervisor completes the form via the online Security Access Request System (SAS) (go to <http://www.losrios.edu/psaccess>).
  - A. Prior to completing the form:
    - i. If the employee is not a full time staff, please verify with the employee that he/she does not have access to PeopleSoft via another department.
  - B. Complete the form.

For details and instructions on using the online system, review the User Guide at <http://www.losrios.edu/~secdocs/restricted/SASRequesterGuide.pdf>.
2. The Level 1 approver reviews the form to ensure that the role(s) requested provide the employee with the data access necessary to perform their job function without permitting access to sensitive or confidential data unnecessary to their job function. Note: If Level 1 approver(s) is not available, a Level 2 can sign for a Level 1. However, Level 1 and Level 2 approvers can not be the same person.
  - i. A request for View Only access or role inactivation requires Approval Level 1 only.
3. The Level 2 approvers will review the form to ensure that District access control policy has been followed.
4. The District Office HelpDesk processes the request as approved by the college/DO.

**Note:**

- Improperly authorized forms will be returned for correction.
- Request for access will not be granted until all necessary approvals have been received.
- Access granted to employees without an active job record will be removed the next business day.

**Information Security R-8871, Section 6.1 Access Control Policy:** Data shall be captured and stored in a manner that supports employees accessing the data necessary to the job function without permitting access to sensitive or confidential data unnecessary to the job function. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and maintained.

**Information Security R-8871, Section 7.0:** All individuals employed by the District are held responsible for adhering to District procedures for system access, use and security.