

There are two basic categories of **HR USERS** at Long Beach:

1. **Departmental & Division Users** with 'read only' access to a subset of employee data that is determined by their row level security: *what node on the organizational chart as defined by the [LBCMP Dept Security tree](#).*
2. **Central Users** who have access to all employees but only certain pages and privileges as defined by their role in the organization; e.g. Benefits Coordinator, HRIS Analyst, Budget Analyst, Payroll Tech, etc.

Departmental & Division Users

Three roles are available to departmental and division users:

- ✓ **HRUSER 1**
- ✓ **HRUSER 2**
- ✓ **CSLink Reports** – [See listing of reports](#)

HRUSER 1 – *generally provided to department level employees with business reason to access employee job records without access to confidential information as defined by campus policy and the State of California Information Practices Act. A full compendium of access pages is available upon request.*

HRUSER 2 – *confidential information accessed by this group is obtained through the Search Match functionality that allows a positive identification of an individual who may have the same name as others in the database. However, Search Match also displays SSN, gender and date of birth to assure the correct person is found (assuming the operator already has access to this other information.) HR has disabled the ability for a user to drill down into the Search Match detail. HRUSER 2 group also receives the Payroll Detail by Employee report distributed each month with the CS Link reporting package. This report will display the employer paid benefits for every employee within a department or division domain. A full compendium of access pages is available upon request.*

Central Users

There are many different roles established for central users depending on their position and job duties. These are found on the bottom section of the HR Security Access form. The LB campus security setup was designed with the perspective of separation of duties and internal control so a process owner could be reasonably accountable for data integrity within their domain of responsibilities. (Meaning if data gets entered or changed it, the changes are due to actions of a single department and a subset of users.)

Actually, many of the central users have 'read only' access to a limited subset of information based on their job needs but their row level security is campus-wide. Others have the ability to create new effective dated entries but only within their areas of responsibility. Another very limited subset of central users, primarily supervisors or their designees, has the ability to correct records. If you would like additional information on the specifics of a central role, please contact Janet Parker, 5-8831.