HR/Payroll Systems Security Requirements and Process

Prepared by the Division of Human Resources, Department of Personnel & Administration, updated December 2003.

The Department of Personnel & Administration (DPA) is responsible for the administration of the two database systems used to process transactions related to employment. The Applicant Data System (ADS) is used to assist in the selection process and EMPL is the employee database. Both databases are linked. Both databases contain confidential and highly sensitive information. Access to and use of these systems is subject to the following expectations or requirements. The Systems Security Administrator will be the central point for receiving request forms for these two systems and resides in the Division of Human Resources (DHR).

- Each department, including institutions of higher education is expected to appoint a single contact for security requests and maintaining updated user security and access.
- All users are expected to strictly adhere to all confidentiality and security requirements, regardless of level of access.
- All requests to grant, modify, or delete security and access must be written and submitted to the Systems Security Administrator on the required forms (see below). No verbal requests will be accepted.
- All users must sign compliance agreements and strictly adhere to all confidentiality and security requirements, regardless of level of access.
- A user's appointing authority is responsible for explaining the required security and compliance agreements, including the potential consequences of a breach in confidentiality or abuse of system access.

  DPA reserves the right to revoke or modify security and access for fraud, a breach in confidentiality, abuse of authority, sharing of a user ID or password. The department's contact will be notified prior to such action.

- All users are expected to be properly trained and maintain updated knowledge whenever system changes occur. Training is available from DHR.
- Each department is expected to develop internal audit controls to assure proper access and use of the systems. Each department is expected to also maintain security-related forms for audit purposes. The System Security Administrator will perform periodic audits to ensure proper access and use of the systems, and departments are also encouraged to periodically conduct transaction audits.

PROCESS

1. The appointing authority completes the forms and explains requirements and policies. DPA requires the *ADS/EMPL Security Access Authorization Request Form* and the *Statement of Compliance*. These forms are available on the web at www.colorado.gov/dpa. For CPPS access, you will need to call Central Payroll at (303)866-3725 for instructions. For EMPL and ADS access, the HR Administrator must sign the form.

2. Each department's Top Secret Security (TSS) Administrator is responsible for establishing "top secret security" to allow log-on access to the state's mainframe. The department's TSS Administrator must resolve any problems with "top secret security" access.

3. Once mainframe access is established, the department's contact must fax the completed *ADS/EMPL Security Access Authorization Request Form* and *Statement of Compliance* to 303-866-2458 in order to allow access to either of the databases.

4. After system security is established, the form will be faxed back to the department's contact and also kept on file by the System Security Administrator.

   If the request involves ADS, a copy will be delivered to the Workforce and Staffing Consultants unit to update its internal table.

5. The Systems Security Administrator generates monthly reports listing those with security and access. These reports will be provided to the department contact to verify those with security and access.

6. Deletion of security and access is to occur as close as possible to the date of termination, transfer, or change in assignment that no longer requires processing transactions. The department contact initiates deletion of system access with the *ADS/EMPL Security Access Authorization Request Form* to change an employee's access. The completed form is faxed to the Systems Security Administrator at 303-866-2458. The System Security Administrator will change system security and then forward a copy of the form to appropriate staff to modify internal tables.

   To avoid discrepancies, no deletion of access on an internal table will be made before the System Security Administrator has updated the Natural systems security.