



## Position & Personnel Data Base (PPDB) and E-Recruit Security Access Request Process and Instructions

The following steps outline the general guidelines for requesting user access to PPDB. Please contact HR Systems at [Group.PPDB@state.or.us](mailto:Group.PPDB@state.or.us) for any questions.

Who	Action
Supervisor	Determines the correct level of access applicable to the required duties of the user's position then completes the User Information and Access Information Section of the Position & Personnel Data Base (PPDB) Security Access Request and Confidentiality Agreement. The Access Information section should provide a descriptive narrative outlining and justifying the request and level of access indicated.
Supervisor	Checks the information for accuracy then forwards an electronic copy of the PPDB Security Access Request and Confidentiality Agreement to the agency's security officer and prints out a manual copy for employee review and signature.
Agency Security Officer	Receives the electronic copy of the completed PPDB Security Access Request and Confidentiality Agreement and waits to receive the manual copy with signatures.
Supervisor and Employee	Review with the employee the policies and laws described in the agreement and answer any questions that the employee may have. The supervisor must verify that the employee has read and understands the agreement.
Supervisor and Employee	Sign and date the PPDB Security Access Request and Confidentiality Agreement verifying that they have read and will abide by the terms of the agreement.
Supervisor	Submit the manual form to the agency's Human Resources Manager or Appointing Authority for approval.
Agency Human Resources Manager or Appointing Authority	Verify that the level of access is correct. If the request is unapproved the form should be returned to the employee's supervisor to be corrected and the process will restart if applicable. If the request is approved then the Human Resources Manager or Appointing Authority will sign and date the request and forward to the agency's security officer.
Agency PPDB Security Officer	Review the request and verify that all sections have been completed and are applicable then sign and date verifying that they have reviewed the form and are aware of the guidelines and responsibilities.

Agency PPDB Security Officer	Compare the signed manual form with the electronic form to verify the information from both forms match. If the information does not match then the security officer will verify the information and make corrections to the electronic copy based on the information from the manual form. Retain the manual form.
Agency PPDB Security Officer	Submit the electronic form via email attachment to: <a href="mailto:Group.PPDB@state.or.us">Group.PPDB@state.or.us</a> The subject of the e-mail should read: 'Agency XXXXX Request for PPDB Access'. Where XXXXX = the agency number. If the request requires access to APPL/CERT or E-Recruit System then the security officer will also cc: <a href="mailto:applcert.info@das.state.or.us">applcert.info@das.state.or.us</a>
PPDB Security	Check the information and verify that the request for access is acceptable. If APPL/CERT access is requested then PPDB Security will wait for confirmation from DAS Statewide Recruitment before access to APPL/CERT System is granted.
DAS Statewide Recruitment	If access to APPL/CERT is granted then DAS Statewide Recruitment will forward the e-mail request to PPDB Security indicating access to APPL/CERT is approved.
PPDB Security	Add user to security table then forward information to RACF Administration.
RACF Administration	Add the user to the proper groups and send the temporary password to the user and notify PPDB Security that the user has been added and that the temporary password has been communicated to the user.
PPDB Security	Notify the agency security officer once access has been granted.
HR Systems	Perform audits on a scheduled and unscheduled basis.

**Instructions:**

Complete the form electronically and save a copy. Forward the form via e-mail to your agency security officer. Print out a hard copy of the form for signatures. The hard copy of the form must also go to your agency security officer after it has been signed. The agency security officer will sign last. All signatures are required. The security officer will forward the electronic form to PPDB Security via e-mail [group.ppdb@das.state.or.us](mailto:group.ppdb@das.state.or.us) and save the signed hard copy for documentation. The completed form must remain on file for 3 years after superseded or authorization expired.

**User Information:**

Fill out the section completely. If you do not know the User ID please contact your HR Department and ask personnel to look it up in PBED. Do not use SSN in the Employee ID field.

**Access Information:**

Make sure all access information is complete and correct. If you need assistance completing the access information section contact PPDB Security via email [group.ppdb@das.state.or.us](mailto:group.ppdb@das.state.or.us). Please do not submit the

form to PPDB Security unless you have all the required information. The Agency Master Operator designation has the ability to see sensitive data and update employee record. Only the Agency Master Operator can view or change an employee record that is designated exempt from public disclosure. Only DAS HR Systems personnel can be designated as DAS Master Operators. If Employee Record Update access is granted then the user will be able to view sensitive data for their agency. Justification is required for users with Display Only Access to view sensitive data. PPDB Security may deny requests for access to sensitive data if there is not sufficient justification showing that it is required for the duties of their job. Dataset Access is for Information Technology employees that handle PPDB data downloads. They do not look at specific records or make any updates in PPDB, only handle raw data to support agency reporting or systems. If you have a unique or non standard request for access please list that in the Misc Access area. Give a description of the duties that justifies the level of access requested, the frequency and how long access is needed. Be specific. Make sure all guidelines have been read and understood.