

Position & Personnel Data Base (PPDB) Security Access Request and Confidentiality Agreement

User Information

Name (print) Last, First M.I.		Employee ID	User ID	
Position/Title		Phone	Extension	
Agency #	Work Location and Address	City	State OR	Zip

- Update or display access to sensitive data will not be granted to temporary or non-status employees. Exceptions may be approved for special circumstances;
- Statewide display without sensitive data is only granted to HR personnel unless specifically required for the job;
- Access to sensitive data for those who have display only access will only be granted with proper justification showing a job related need;
- DAS HR Systems highly encourages agencies to limit the number of users having Agency Master Operator access to one or two people in order to maintain security integrity. Only Agency Master Operators can update or see sensitive data for employee records that are exempt from disclosure per ORS 192.445.

PPDB & Application/Certification Access Information

<u>Update Access</u>	<u>Display Access</u>		<u>Other</u>	
Employee Record Position Record	Employee Record Agency View Statewide View	Position Record Agency View	Web Reports	PPDB Datamart
Agency Master Operator DAS Master Operator	Sensitive Data (Justification Required)	Dataset Access (IT Staff Only)	<u>Misc. Access:</u>	

Describe the job duties that require access to PPDB and give justification supporting the level of access requested:

Describe frequency of use? (daily, once a week, once a month, as needed... etc.)

How long is access needed? (ongoing, special project, job rotation, backup behind leave...etc)

User Guidelines and Responsibilities:

- Access to PPDB information is for job related purposes only.
- Users will not share confidential or sensitive information or use the information for any personal reason or gain.
- User must not share their password with any person or allow another person to use their access in any way.
- PPDB data is confidential and may be used solely for the purpose of human resources, workforce development, and budget functions internal to the Agency.
- Disclosure or release of employee data and statistics for any other purpose or to any entity not a direct party to the agency's internal management functions requires express, written approval of the State Public Records Officer, who is the official custodian of the information.
- The agency's security officer must be notified immediately if the user's password or access has been compromised.
- The user will read, understand and agree to adhere to all applicable agency and statewide policies, including but not limited to the following:
 - 107-004-050 Information Asset Classification
 - 107-004-051 Controlling Portable and Removable Storage Devices
 - 107-004-052 Information Security
 - 107-004-053 Employee Security
 - 107-004-100 Transporting Information Assets
 - 107-004-110 Acceptable Use of State Information Assets

Supervisor Guidelines and Responsibilities:

- Supervisors will be cautious in their request for approval.
- Supervisors will ensure that their request for access is based on a valid need; and ensure that level of access required to perform the duties is associated with the user's position on a consistent basis.
- Supervisors must not request access until they are certain that the user understands the PPDB information security requirements.
- Supervisor and employee will review Oregon Public Records Law (ORS 192.501 to 192.505) and Oregon Administrative Rule 105-10-0011, before access to data is allowed.

Security Officer Guidelines and Responsibilities:

- Security officer is responsible for maintaining documentation of the requests for PPDB access for all users in their agency.
- Security officer will review the request for accuracy and ensure that both the user and supervisor signatures are present before submitting the request to PPDB Personnel Security.
- Security officer understands that DAS HRSD will perform audits on a regular and undetermined schedule to ensure that proper documentation is being maintained for users in their agency.
- Security officer agrees to restrict access of data to individuals in regular status (permanent or limited duration) state positions.
- Security officer agrees that access by temporary or contracted employees is not allowable.
- Security officer agrees to implement and maintain a policy to ensure that agency staff with access to data will always lock their computer screen or logoff before leaving their workstation.
- Prior approval by DAS HR Systems is required before any exceptions to this agreement are granted.

Confidentiality Agreement

I understand and agree that:

- I have read the guidelines and responsibilities set forth above. I acknowledge that it is my responsibility to maintain all employee (current and former) information in confidence.
- I have read the policies above and agree to abide by the rules as set forth.
- The Position and Personnel Data Base is categorized as Information Asset Classification Level 4 - Critical data per 107-004-050 and shall be treated as such.
- I will discuss any questions I have regarding this agreement, policy, or the Confidentiality Guidelines with my Human Resource representative or agency security officer prior to divulging, discussing, or transmitting any confidential information.
- The obligation to maintain the confidentiality of information obtained while employed by the state continues beyond separation of employment.
- Violation of this confidentiality agreement, policy, or the Confidentiality Guidelines may result in discipline up to and including termination of employment.

User Name	User Signature	Date
Supervisor	Supervisor Signature	Date
HR Manager or Appointing Authority	HR Manager or Appointing Authority Signature	Date
Agency Security Officer	Agency Security Officer Signature	Date

Agency Security Officer Use:		
Request from HR Manager received	Submitted to DAS PPDB Security	DAS PPDB Security granted access
Date	Date	Date