



United States Office of Personnel Management

Retirement Systems Modernization Coverage Determination Application

CDA USER PROFILE		
CDA Userid	Section I – Applicant Information	
	<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none; vertical-align: top;"> <input type="checkbox"/> New CDA Userid <input type="checkbox"/> Existing CDA Userid <i>(Furnish CDA Userid in CDA Userid box on left.)</i> <input type="checkbox"/> Deactivate CDA Userid Specify deactivation date: <input style="width: 100px;" type="text"/> <i>(Furnish CDA Userid in CDA Userid box on left.)</i> </td> <td style="width: 50%; border: none; vertical-align: top;"> <input type="checkbox"/> Modify existing CDA Userid Specify effective date: <input style="width: 150px;" type="text"/> <i>(Furnish CDA Userid in CDA Userid box on left.)</i> Specify what is being modified: <input style="width: 150px; height: 20px;" type="text"/> <i>(Name, type of access, etc.)</i> </td> </tr> </table>	<input type="checkbox"/> New CDA Userid <input type="checkbox"/> Existing CDA Userid <i>(Furnish CDA Userid in CDA Userid box on left.)</i> <input type="checkbox"/> Deactivate CDA Userid Specify deactivation date: <input style="width: 100px;" type="text"/> <i>(Furnish CDA Userid in CDA Userid box on left.)</i>
<input type="checkbox"/> New CDA Userid <input type="checkbox"/> Existing CDA Userid <i>(Furnish CDA Userid in CDA Userid box on left.)</i> <input type="checkbox"/> Deactivate CDA Userid Specify deactivation date: <input style="width: 100px;" type="text"/> <i>(Furnish CDA Userid in CDA Userid box on left.)</i>	<input type="checkbox"/> Modify existing CDA Userid Specify effective date: <input style="width: 150px;" type="text"/> <i>(Furnish CDA Userid in CDA Userid box on left.)</i> Specify what is being modified: <input style="width: 150px; height: 20px;" type="text"/> <i>(Name, type of access, etc.)</i>	
<input type="checkbox"/> Federal Employee <input type="checkbox"/> Permanent <input type="checkbox"/> Temporary Exp. Date: <input style="width: 100px;" type="text"/>		
Agency Name: <input style="width: 150px;" type="text"/> Department: <input style="width: 150px;" type="text"/>		
<i>(If applicant is a contractor, a Federal employee supervisor must fill out form and have contractor sign and date in blocks 7 and 8.)</i>		
<input type="checkbox"/> Contractor Company Name: <input style="width: 150px;" type="text"/> Contract Number: <input style="width: 150px;" type="text"/>		
Expiration Date of Contract: <input style="width: 100px;" type="text"/> Agency Name: <input style="width: 150px;" type="text"/> Department: <input style="width: 150px;" type="text"/>		
1. Name <i>(Last, First, Middle Initial)</i>	2. Telephone number <i>(Include Area Code and Extension)</i>	
3. Last four digits of Social Security Number	4. Title/Position	
5. Duty Location <i>(City/State/Zip Code)</i>	6. E-mail address	
Computer UserID and Password Disclosure Statement I understand that my ID and password are for my use only. I agree to protect my password from disclosure by all reasonable means, and not to willingly divulge it or allow its use by any other person(s). If I believe that another person has learned my password, I will notify my supervisor immediately. I understand that my use of government equipment, including computer systems, must comply with the policies specified in the OPM "Policy on the Use of Government Office Equipment." If I am an employee of an agency other than OPM, I must also comply with my agency's policy.		
7. Signature of applicant	8. Date of signature <i>(MM/DD/YYYY)</i>	
Section II – Federal Supervisor Information on page two (2) must be completed by your supervisor		

Section II – Applicant's Federal Supervisor Information

(Applicant's Federal Supervisor must complete this section)

9. Grant the applicant the following CDA user access

General Access Only

Yes No

Manual Override*

Yes No

* Manual Override Authorization is an additional authorization in the CDA that is generally granted to senior staff and supervisors. It is used at the time when a retirement coverage determination made by the CDA differs from the Retirement Plan of record.

10. Applicant's Federal Supervisor Name (Last, First, Middle Initial)
(The approving official must be a Federal employee supervisor.)

11. Title/Position

12. Telephone number *(Include Area Code and Extension)*

13. Duty Location *(City/State/Zip Code)*

14. E-mail address

16. Supervisor's signature

17. Date of signature *(MM/DD/YYYY)*

All information and proper signatures must be completed or this User Profile Form will be returned without processing. If you have any questions, please contact OPM at (800) 239-2492 or contact us at CDAHelp@opm.gov. After you complete this form online, print form, and sign and date blocks 7 and 8, have your supervisor complete Section II and sign and date blocks 16 and 17. Fax all pages of this form to (202) 606-2060 or (202) 606-0910. We cannot accept a completed form via email at this time.

Section III – OPM Security Officer Information

(To be completed by OPM Security Officers Only)

18. Comments

19. Signature of Designated Security Officer (DSO)

20. Date of signature *(MM/DD/YYYY)*

OPM COMPUTER USER RESPONSIBILITIES

As a user of OPM's computer systems, you are expected to understand and comply with the responsibilities outline below. You will be held accountable for your actions when using these systems. If you violate OPM policy regarding these responsibilities, you may be subject to administrative action ranging from counseling to removal from the Agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

Privacy While Using Government Equipment – You do not have the right to privacy while using any Government equipment, including Internet or email services. Furthermore, your use of Government office equipment, for whatever purpose, is not secure, private or anonymous. While using Government office equipment, your use may be monitored or recorded.

Protection of Software, Data and Hardware – You are not allowed to introduce any unauthorized software and data (including software and data protected by copyright, trademark, privacy laws, other proprietary data or material with other intellectual property rights beyond fair use), hardware or telecommunications devices or modify any configurations. In addition, you will protect all sensitive information residing in OPM computer systems, preventing unauthorized access, use, modification, disclosure or destruction of that information. This includes records about individuals requiring protection under the Privacy Act, sensitive financial information and information that cannot be released under the Freedom of Information Act. Disclosure of sensitive information, trade secrets and intellectual property to unauthorized individuals is also prohibited.

Service Restoration – The availability of the computer systems is a matter of importance to you. You are responsible for assisting in any way that you can for restoring service in the event the computer systems becomes non-operational.

System Privileges – You are given access to the computer systems based on a need to perform specific work at OPM. You are expected to work within the confines of the access allowed and are not to attempt to access systems or applications for which access is not authorized.

Telecommuting – The OPM Human Resources Handbook, Chapter 368, Telecommuting, contains the policy and procedures for authorizing telecommuting. In general, immediate supervisors approve, on a case-by-case basis, employee requests to telecommute. Telecommuters who access OPM's general support systems must adhere to all IT security policy and procedures that would apply if the individual was accessing OPM's systems in the office. Dial-in access for telecommuters or other users whose job functions may require it is authorized by the Chief, Network Management Group.

Use of Government Office Equipment – You will comply with the policies specified in the OPM Policy on Personal Use of Government Office Equipment.

Use of Passwords – You will create and use passwords as specified in the IT Security Policy. You must keep your passwords confidential and not share them with anyone. Individual applications may have more stringent password requirements than the general policy requirements.