Department of Defense Education Activity

PROCEDURAL GUIDE

NUMBER 14-PGRMD-004
DATE May 15, 2014

RESOURCE MANAGEMENT DIVISION

SUBJECT: Procedures for Granting Access to the Defense Civilian Personnel Data System

References: (a) DoD 7000.14-R, "Department of Defense Financial Management Regulation," June 2011, Volume 1-15, as amended
(b) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013

1. PURPOSE. This Procedural Guide documents the proper processes and procedures for granting user access and permissions for the Defense Civilian Personnel Data System (DCPDS) at the Department of Defense Education Activity (DoDEA).

2. APPLICABILITY. This Procedural Guide applies to the Office of the Director, DoDEA; the Director, Domestic Dependent Elementary and Secondary Schools, and Department of Defense Dependents Schools, Cuba (DDESS/DoDDS-Cuba); the Director, Department of Defense Dependents Schools, Europe (DoDDS-E); the Director, Department of Defense Dependents Schools, Pacific, and Domestic Dependent Elementary and Secondary Schools, Guam (DoDDS-P/DDESS-Guam), (hereafter collectively referred to as "DoDEA Area Directors"); and all DoDEA District Superintendents and school administrators.

3. DEFINITIONS. See Glossary.

4. GUIDANCE. This Procedural Guide defines the roles, responsibilities, and processes for granting access to DCPDS. DCPDS user access is managed according to References (a) and (b).

5. PROCEDURES. See Enclosure 1.

6. EFFECTIVE DATE. This Procedural Guide is effective immediately.

RMBRADY

Robert M. Brady
Associate Director for Financial
and Business Operations

Enclosures
1. Procedures
2. DD Form 2875, System Authorization Access Request (SAAR)
3. DCPDS User Account Request Form

Glossary

ENCLOSURE 1

PROCEDURES

1. DEFENSE CIVILIAN PERSONNEL DATA SYSTEM (DCPDS) ACCESS OVERVIEW. DCPDS is a database containing current, projected, and historical employee personnel management data, such as education level, work experience, current grade and step, awards history, projected training requirements, and completed training. While the database itself is maintained externally, the Department of Defense Education Activity (DoDEA) is responsible for ensuring that only authorized individuals are granted access to DCPDS, and that the access granted to those individuals is required in the execution of their responsibilities and duties.

2. GRANTING DCPDS SYSTEM ACCESS.

a. When requesting DCPDS access, employees must complete Part I of the DD Form 2875, System Authorization Access Request (SAAR) (Enclosure 2), and the DCPDS User Account Request Form (Enclosure 3). Once completed and signed, requesting users send both forms to their supervisor for approval.

b. The supervisor completes Part II of the DD Form 2875 and the DCPDS User Account Request Form, verifying user access and authorizing account setup with a manual or electronic signature.

c. The supervisor then proceeds as follows, depending on their location:

(1) If the supervisor is located at a school, the approved and signed documents are forwarded to the school secretary. The school secretary forwards the request documents to the Area Service Center (ASC).

(2) If the supervisor is located at a District Superintendent Office (DSO), they forward the request documents to the servicing ASC.

(3) If the supervisor is located at DoDEA Headquarters (HQ), they forward the request documents to the servicing DoDEA HQ Functional Automation and Information Management (FAIM) Branch.

d. The servicing ASC or FAIM Branch files the DCPDS User Account Request Form and forwards the DD Form 2875 to the Personnel Security Program Manager (PSPM) at the DoDEA HQ Office of Safety and Security (OSS).

e. The PSPM uses the Joint Personnel Adjudication System (JPAS) to verify if the requesting user has passed an Access National Agency Check with Inquiries (ANACI) background investigation. DLA has determined that DCPDS requires Information Technology (IT) Access Level 2, therefore requiring all DoDEA employees seeking DCPDS access to complete an ANACI background investigation.

ENCLOSURE 1

PROCEDURES

(1) Upon completion of the ANACI, the form is completed and signed by the PSPM and returned to the servicing Human Resources (HR) specialist.

(2) If the employee fails the ANACI, he/she is denied DCPDS access. The following process is used to grant interim access:

(a) The DoDEA OSS initiates an ANACI investigation and selects the Special Agreement Check (SAC) (i.e. Federal Bureau of Investigation (FBI) fingerprint check) option in the Agency Use Block (AUB) template on the Electronic Questionnaire for Investigations Processing (e-QIP).

(b) The employee completes the Standard Form (SF) 86 in e-QIP.

(c) The DoDEA security office reviews, approves, and submits the e-QIP application, including the request for a SAC, to the Office of Personnel Management (OPM) for processing.

(d) Once completed, OPM sends the FBI fingerprint check (i.e. the SAC) to DoDEA.

(e) The DoDEA security office reviews the SAC. If there are no serious issues with the SAC, the process continues; however, if the SAC uncovers unfavorable or serious issues, interim access is denied and the employee must wait until the full investigation is adjudicated to be granted access.

(f) The DoDEA security official completes the DD Form 2875, noting in Block 27 that the employee favorably completed a background investigation. The date and type of investigation submitted and the date of the completed FBI fingerprint check are also reflected on the DD Form 2875.

f. The servicing ASC or FAIM HR specialist reviews the DD Form 2875 and the DCPDS User Account Request Form to verify that the forms are complete and accurate; that forms are signed by certifying officials; and, that the employee is eligible to receive the requested type of access or access modification. The ASC HR specialist forwards all requesting documentation to the FAIM HR specialist.

g. The FAIM HR specialist reviews, verifies, and signs the documentation before forwarding them to a Defense Logistics Agency (DLA) supervisory HR specialist and submitting a copy to the DLA HR Self-Service inbox. If the forms are inaccurate, the FAIM HR specialist works with the ASC HR specialist or the supervisor to resolve the issue.

h. The DLA HR Self-Service e-mails the ASC and FAIM servicing HR specialists and the requesting user that DCPDS access has been granted.

ENCLOSURE 1

PROCEDURES

(1) If a new account has been created, the e-mail provides a user identification (ID); after the initial login, users access DCPDS using their Common Access Card (CAC).

(2) If the requester is a local national employee, the e-9999999mail includes a user ID and a password for all future logins.

i. When a formerly authorized user is no longer eligible for DCPDS access (i.e. he/she separates from DoDEA, switches jobs, and/or changes duties and responsibilities), the servicing ASC or FAIM Branch initiates an action to deactivate that employee's access within 30 days of their absence or job change.

(1) Every quarter, the ASC or FAIM Branch obtains a listing of DCPDS users within their servicing area and their access rights.

(2) The ASC or FAIM Branch reviews and compares the user list with the list of current employees and their assignments.

(3) Supervisors initiate actions to terminate inactive or ineligible employees. Supervisors are responsible for notifying ASC or FAIM Branch when an employee moves or terminates.

(4) The ASC or FAIM Branch obtains a list of the DCPDS users verified for the quarter, along with a signed and dated statement from the supervisor stating, "I have reviewed the DCPDS user list and access rights as of MM/DD/YY, and verify that these are active employees with a requirement for DCPDS access."

(5) Alternately, if action has been taken to remove inactive or ineligible employees from DCPDS access, the statement may read: "Action has been initiated to remove (identify employee and user name) from the DCPDS user database. With the completion of this action, I verify that all the remaining employees herein listed are active and have the appropriate level of access to DCPDS for the quarter ending MM/DD/YY."

(6) The statement is signed by an authorized official within the ASC or FAIM Branch. While DLA retains DCPDS request forms, DoDEA retains copies of the DCPDS User Account Request Form and the DD Form 2875 for review upon the supervisor's request.

ENCLOSURE 2

DD FORM 2975, SAAR

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST
☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID_____
DATE *(YYYYMMDD)*

SYSTEM NAME *(Platform or Applications)*
LOCATION *(Physical Location of System)*

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*
2. ORGANIZATION
3. OFFICE SYMBOL/DEPARTMENT
4. PHONE *(DSN or Commercial)*
5. OFFICIAL E-MAIL ADDRESS
6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS
8. CITIZENSHIP ☐ US ☐ FN ☐ OTHER
9. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☐ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)* _____
11. USER SIGNATURE
12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS

14. TYPE OF ACCESS REQUIRED:
☐ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☐ OTHER _____

16. VERIFICATION OF NEED TO KNOW
I certify that this user requires access as requested. ☐
16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*

17. SUPERVISOR'S NAME *(Print Name)*
18. SUPERVISOR'S SIGNATURE
19. DATE *(YYYYMMDD)*
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT
20a. SUPERVISOR'S E-MAIL ADDRESS
20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR
21a. PHONE NUMBER
21b. DATE *(YYYYMMDD)*
22. SIGNATURE OF IAO OR APPOINTEE
23. ORGANIZATION/DEPARTMENT
24. PHONE NUMBER
25. DATE *(YYYYMMDD)*

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Adobe Designer 9.0

ENCLOSURE 2

DD FORM 2875, SAAR

26. NAME *(Last, First, Middle Initial)*			
27. OPTIONAL INFORMATION *(Additional information)*			
PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION			
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☐ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION		
TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*