DCMA Manual 4201-08

Human Resources Systems and Automated Tools

Office of Primary Responsibility:	**Talent Management Capability**
Effective:	May 26, 2019
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA-INST 4201, "Civilian Personnel," July 20, 2018
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/TM/SitePages/4201-08r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64, implements policy established in DCMA Instruction 4201, assigns responsibility and prescribes general principles associated with Human Resources Systems and Automated Tools Access and Maintenance.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA activities unless higher-level regulations, policy, guidance, or agreements take precedence.

1.2. POLICY. It is DCMA policy to:

a. Implement policy and establish uniform DCMA-wide procedures and guidelines, delegate authorities and assigns responsibilities regarding Human Resources (HR) systems and automated tools access.

b. Assign responsibility for monitoring the appropriateness of accounts as well as the account holder documentation to Civilian Human Resource Agency (CHRA) and DCMA.

c. Have a documented process to ensure access and privileges are validated as well as maintained per the documented regulations.

d. The guidance within this manual is applicable to systems directly owned by or licensed to CHRA or when the account administration responsibility has been delegated to CHRA by the system owner. This includes the Defense Civilian Personnel Data System (DCPDS); electronic Official Personnel Folder (eOPF), CHRA Access Control Lists (ACL), Business Objects (BOXI), USA Staffing® (USAS), which includes Onboarding Manager (OM), and all other applications assigned to CHRA for administrative management.

e. Execute this manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBLITIES

2.1. EXECUTIVE DIRECTOR, HUMAN CAPITAL DIRECTORATE OR DESIGNEE. The Director of Human Capital (HC) or designee will:

a. Develop and implement HR System Access policy and guidance.

b. Follow all requirements of CHRA Administered Account Maintenance, Standard Operating Procedure (SOP) No. ISD-15-SOP-01 and recommend updates and corrections where required.

c. Request account termination when employees no longer require system access or leave the organization.

d. Respond timely to annual account validation reviews issued by Fort Riley Helpdesk, Information System Division (ISD).

e. Review requests for accuracy, completeness, and appropriateness of the user role and organizational access.

f. Perform quarterly reviews to identify users who have changed positions, moved organizationally, or who are no longer employed, and take appropriate steps to extend or terminate/end-date accounts.

g. Notify supervisors and users to perform annual recertification of accounts.

h. Follow all requirements of this manual and recommend updates and corrections where required.

SECTION 3: PROCEDURES

3.1. ACCOUNT REQUIREMENTS.

a. Determining Account Requirements. Supervisors must determine which HR systems are required for positions within their organization, and complete the forms (or request user completion of forms) required to establish, change, or terminate/end-date HR system accounts. The following actions should trigger a form submission to add, modify, or terminate/end-date an account:

(1) A user is new to the organization.

(2) A user leaves an organization. It is essential account terminations are processed immediately if an account holder leaves the agency.

(3) Account access rights or system roles are expanded or diminished, or new systems are required to meet work assignment changes.

(4) A user's supervisor changed, whether or not the organization was changed.

(5) A user's organization code changed, whether or not the supervisor was changed.

(6) A user legally changes his/her name.

b. Obtain Army Knowledge Online (AKO) Account. Before access is granted to HR systems and tools, the user must register and establish an AKO account. Refer to the Resource Page for AKO Account Registration Guidance under the Guidance section. This application is used by CHRA to authenticate user identity. The types of accounts:

(1) Unsponsored Accounts: Civilian Personnel.

(2) Sponsored Accounts: Contractor, Military Personnel and Local National. Require sponsorship by ISD personnel.

3.2. REQUEST PROCEDURES.

a. Initial Account Request.

(1) When requesting access, nominee must complete Part I of the DD Form 2875, "System Authorization Access Request (SAAR)," and the CHRA Employee User Account Request Form (URF). Refer to the Resource Page in the Templates section. Once completed and signed, the user will send both Forms to their supervisor for approval via encrypted email.

(2) The supervisor completes Part II of the DD Form 2875 and the CHRA URF, verifying user access and authorizing account setup with an electronic signature.

(3) The supervisor must send DD Form 2875 via encrypted email to obtain signatures from the Personnel Security Manager and a DCMA authorized Information Assurance Officer (IAO) or designee for completion of the form. The minimum Personnel Security Investigation (PSI) requirements for system access is a National Agency Check with Inquires (NACI).

(4) Once all signatures are obtained, the supervisor or designee will send an encrypted email to the Human Capital Business Division (HCB) inbox DCMA Ft Lee HQ Mailbox HCB Encrypted. (Refer to the Resource Page in the Points of Contact section for email address.)

(5) HCB reviews forms to ensure completeness and accuracy. Forms not completed appropriately will be returned to the sender for correction and resubmission.

(6) HCB will submit the request forms to ISD via encrypted email to the Fort Riley Helpdesk or submit a ticket in CHRA HR Service Portal application for processing.

(7) Once the accounts have been established, the ISD or HCB staff will notify the user that access has been granted along with login information and guidance. Refer to the Resource Page for the Access Request Process Flowchart under the Process Flowcharts section.

b. Modification Account Requests.

(1) If the system name and supervisor have not changed from the original DD Form 2875 and the Information Assurance (IA) training is dated within the last 12 months, the URF will be accepted for account modifications. Follow same guidance in paragraph 3.2.a.(1).

(2) If the ISD does not have a valid DD Form 2875 on file, the supervisor changes or the organization is not the same as what is on the initial DD Form 2875, then the user must complete a new DD Form 2875 and the CHRA Employee URF. Follow initial request guidance in paragraph 3.2.a.(1).

(3) Realignment modifications will be submitted by HCB to the ISD according to the organization's validated realignment crosswalk provided by the Business & Financial Operations Executive Directorate, Manpower and Organization Management Division (FBO).

c. Deactivating Account Requests.

(1) Supervisor must complete and sign the first page of the DD Form 2875 and submit to HCB to deactivate accounts. The supervisor will sign the form, but the following signatures are not required: Employee, IAO or Personnel Security Manager.

(2) Refer to Resource Page for guidance on form completion in the Guidance section.

(3) If the Army Servicing Team (AST) has a Separation/Loss Standard Form (SF) 50, "Notification of Personnel Action," for the user, all user accounts administered by ISD will be deactivated.

(4) Email notification and/or the SAAR from the supervisor will be accepted by HCB to deactivate the account(s) via inbox found in the Requesting HR Systems and Tools Access section on resource page.

d. Access Approval.

(1) Requests for Agency-wide access must be approved by HC Executive Director with coordination through HCB before access is granted.

(2) For all other requests, HCB has the authority to "Approve" or "Deny" access requests. Approval and level of access is based on the need to access this information to perform one's job responsibilities as provided for in the DoD Directive 5400.11, "DoD Privacy Program."

(3) Disputes to access can be adjudicated by the HC Executive Director, HC Deputy Director, or HCB Chief.

3.3. SEGREGATION OF DUTIES. HCB is responsible for ensuring sufficient separation of duties for roles with DCPDS responsibilities. Refer to the Resource Page for DCPDS Segregation of Duties Matrix in the References section.

3.4. PERIODIC ACCESS REVIEW.

a. Quarterly Review.

(1) HCB will perform reviews on a quarterly basis to identify users who have changed positions, moved organizations, or are no longer employed with the requesting office.

(a) HCB will submit a CHRA HR Service Portal ticket or send email to Fort Riley Helpdesk to terminate/end-date all accounts for users who have separated from DCMA within 10 business days of review completion.

(b) HCB will contact the User if the person has changed positions other than a career promotion or realignment. If there is no response, accounts will be terminate/end-date within 10 business days of requested return date.

b. Annual Review (Recertification).

(1) HCB will prepare a list of all active DCPDS and Civilian Personnel Online (CPOL) account holders to perform annual recertification of accounts.

(2) HCB will send account lists to the Director, Commander, Deputy, and/or Mission Support Office (MSO) Chief requesting management to identify any accounts requiring termination or change, and verify that any remaining accounts are still active and valid. Management will have 10 business days to respond in writing. If there is no response, accounts will be terminate/end-date within 10 business days of requested return date.

(3) Upon receipt of management response to the annual review, HCB will submit a request to terminate/end-date accounts as required to ISD. If account changes are requested, ensure appropriate paperwork is completed, signed, and submitted.

(4) Annual review certification paperwork will be stored for a period of three years. Records will identify the information sent to management, management's response, and action taken to resolve account issues. User paperwork and account maintenance records will be annotated to indicate actions taken.

c. Internal Controls.

(1) HCB will ensure evidence of quarterly reviews, to include identification of personnel changes impacting account records and actions taken to update records, is available.

(2) HCB will ensure evidence of annual recertification reviews, to include management responses and actions taken to update records, is available.

3.5. CHANGE MANAGEMENT. Any change request to any HR System must follow the procedures contained within the Change Management SOP. Refer to the Resource Page for guidance under the References section.

GLOSSARY

G.1. DEFINITIONS.

AKO. Provides web-based enterprise information services to the United States Army, Joint, and DoD customers. Enterprise services are provided to these customers on both classified and unclassified networks, and include portal, e-mail, directory, discovery, and single sign-on functionality.

AST. The service provider responsible for providing HR support for the agency.

CHRA. The organization within the Department of the Army responsible for providing "civilian" HR support.

CPOL Portal. A collection of tools and links to various civilian HR management applications and information, including links to DCPDS, employee SF50s, My Biz+, and other systems.

DCPDS. The database of record for civilian employees of the DoD.

Business & Financial Operations Executive Directorate (FBO). The Manpower and Organization Management Division is responsible for providing realignment crosswalks.

Fort Riley Helpdesk (ISD). ISD is responsible for providing HR systems & tools support.

HR Service Portal. A self service automated tool that allow users to submit tickets to resolve issues with CHRA systems and applications.

IAO. The IAO or appointee of the office responsible for approving access to the system being requested.

MSO. The Administrative staff that provides support to the Director and personnel within an organization.

Personnel Security Manager. Validates the background investigation or clearance information.

Supervisor. Certify that the user requires access as requested.

User. The person requesting the access.

GLOSSARY

G.2. ACRONYMS.

AKO	Army Knowledge Online
CHRA	Civilian Human Resources Agency
CPOL	Civilian Personnel Online
DCPDS	Defense Civilian Personnel Data System
DD Form 2875	System Authorization Access Request (SAAR)
DoDD	DoD Directive
HCB	Human Capital Business Division
HR	Human Resources
IAO	Information Assurance Officer
ISD	Information Systems Division
Standard Form 50	Notification of Personnel Action
SOP	Standard Operating Procedures
URF	Employee User Request Form

REFERENCES

Civilian Human Resource Agency(CHRA) No. ISD-15-SOP-01," CHRA Administered Account Maintenance SOP"; December 22, 2016
DoD Directive 5105.64,"Defense Contract Management Agency (DCMA)," January 10, 2013
DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014