



AKO / DKO PROCEDURE # AKO-PRC-0031

Non-U.S. Citizen Account Provisioning

Last Updated: 15 March 2010

Overview

5 AKO/DKO supports secure access to disparate, cross-Service capabilities and information as an enterprise collaborative environment for war fighting, business, and intelligence users. It is understood that such activities may be supported by citizens of countries other than the United States, and that such support may require some type of AKO/DKO access. This procedure describes AKO/DKO's guidelines and restrictions on assigning such personnel portal access and holds true regardless of the country in which access occurs.

10 Existing accounts are not automatically grandfathered into compliance by this procedure; however, existing account holders should not abandon their current accounts and apply for new ones. Sponsors of existing accounts are to follow the appropriate approval procedure for their situation, skipping the new account registration or sponsor change step and using the existing account user ID in the procedure. Existing accounts that are currently typed as portal access but no longer qualify in this regard must be downgraded by the sponsor or are subject to administrative downgrading by the AKO/DKO PMO with or without notice.

15 It is a violation of Army regulation 25-2, sections 4-14 and 4-15 for any full account holder with sponsorship rights to grant access to a non-U.S. Citizen outside of this procedure. Also note that AKO/DKO account holders may not share their credentials or allow access via an existing session with any person, regardless of nationality.

Non-U.S. Citizen Account Usage – Definition

25 Army Regulation 25-2 defines a foreign national as an individual who is ***not a citizen of the United States of America (U.S.A)***. In general, non-U.S. citizens are not permitted AKO/DKO accounts in the same manner by which Army Contractors, Family, DKO users and other guests of United States citizenship are assigned access rights.

30 Service Members who are not a citizens of the United States; and, are currently serving as an active, reservist or National Guard member of the United States armed forces; and, who have taken the Enlistment Oath as cited in 10 USC Sec. 502, Subtitle A, Part II, Chapter 31, are entitled to a portal access type account; however, this does not exempt the recruiter, ranking NCO or Commanding Officer from submitting the required digitally signed email notification with checklist attachment to ako.nonus.accounts@us.army.mil advising of the account usage.

35 Non-U.S. Citizens, regardless of nationality, may not have administrative rights within AKO/DKO nor may they have access to Utility or Group accounts or sponsor other individuals. Individuals whose actual position qualifies at a higher investigative level that what is applied for will be considered as having met the investigative requirement for the lesser position.

40 Family members of trusted non-U.S. citizens are not permitted access to AKO/DKO and account holders are to be instructed that the sharing of their account information or access with any other personnel will be cause for immediate account deactivation.



BEFORE YOU SEND AN EMAIL TO AKO.NONUS.ACCOUNTS

- 5 (1) Select who the account sponsor will be. The sponsor MAY BE ANY FULL ACCOUNT HOLDER with sponsorship privilege and who is a United States Citizen. Requests submitted by a sponsor who does not qualify to validate the request will be denied.
- (2) Select who the validating official will be. The validating official must be a United States citizen. The sponsor and the validating official may be the same individual IF the sponsor is of sufficient rank.
- 10 (3) Ensure the applicant has registered for the account and is using the appropriate account type declared as email only. See Appendix A, "Available Account Types" at the end of this document.
- (4) Download and complete the corresponding category checklist.
- 15 (5) ATTACH the category checklist to an email addressed to ako.nonus.accounts@us.army.mil to be sent by the qualifying person. Checklists that have been cut-and-pasted into an email are not acceptable and will be denied.
- (6) ALL CORRESPONDENCE MUST BE DIGITALLY SIGNED. Refer to the checklist definition to determine who must send the email. Unsigned correspondence will result in the application being denied.
- 20 (7) An FAQ is available on the policies and procedure portal page found here:
<https://www.us.army.mil/suite/page/278081>

QUICK NOTES

- 25
- Categories are mutually exclusive, that is, you DO NOT apply for one category with the expectation to "upgrade". Select only one Category for the duration of the account.
 - Starting the account as "email only" and selecting Category 1 are not the same. ALL ACCOUNT APPLICATIONS START AS EMAIL ONLY. Category 1 accounts REMAIN as email only. All other categories have the option to process the applicant for portal access.
 - Do not send any documentation for a Category 8 application to AKO/DKO. Send only the approval confirmation received from G6 upon process completion.
 - Read the declarations on the checklists carefully as some declarations require that additional material be attached to the email or that multiple emails be sent. Any documentation required by this procedure to substantiate a claim or certification must conform to AR 25-50 unless it is a predefined DoD form or issued by a recognized educational institution or commercial certifying body.
 - A non-U.S. citizen who wears the uniform of their country's military or is an employee or elected official of any government except the United States CANNOT be declared as a "Local National".
 - There is no "grandfathering" of accounts. Because an account existed before this procedure was published does not exempt the sponsor from conforming to this procedure for that account.
- 30
- 35
- 40
- 45



Account Application Categories

(Category 0) Classified Access

To qualify for this category, the non-US citizen must have a security clearance issued by a US Government Agency and be listed in the Joint Personnel Adjudicated System (JPAS). FOREIGN CLEARANCES DO NOT QUALIFY. **Application email returned by the sponsor.**

(Category 1) Email only accounts

Available to all applicants. **Application email returned by the sponsor.**

(Category 2) Portal access by ACU Officers

If the person is a military or governmental member of a partner country as defined by the United States Department of State and as listed in the DAMI-CDD (380-10) Memorandum of 20 January 2006. **Application email returned by validating official.**

(Category 3) Portal access by non-U.S. citizens who hold an IT-III or equivalent trust level position

Available to Level IT-III certified applicants. Requires attachment of Form DD 2875. **Application email returned by validating official.**

(Category 4) Portal access by non-U.S. citizens who hold an IT-II trust level position

Available to Level IT-II certified applicants. Requires attachment of Form DD 2875. **Application email returned by validating official.**

(Category 5) Portal access by non-U.S. citizens who hold an IT-I trust level position:

Available to Level IT-I certified applicants. Requires attachment of Form DD 2875. **Application email returned by validating official.**

(Category 6) Portal access by International Military Students (IMS)

This category applies only to those students who have been vetted and approved for U.S. Army Training and Professional Military Education (PME) and are attending resident training or enrolled in the Army Distance Education Program (DEP) at U.S. Army and Army-managed schools/training activities. **Application email returned by validating official.**



(Category 7) Portal access by non-US citizens in **non-official roles**

5 Available to local nationals and ex-patriots who are not uniformed service members or do not hold a government role. **Application email returned by validating official.**

(Category DODCE) DoD Civilian Employee (Federal Service)

10 If the individual is a civilian employee of the United States Department of Defense. **Application is submitted by validating official.**

(Category ASM) Active/Reserve/NG Military Service Member

15 If the individual is an active service member of the United States Military and not a U.S. citizen. **Application is submitted by validating official/recruiter.**

(Category 8) Portal access accounts by non-US citizens **acting in an official capacity for their home country. This includes all uniformed or government personnel who do not qualify for another category.**

5

- i. The account must be **APPLIED FOR BUT NOT APPROVED** by its sponsor **until the following steps have been completed.**
- 10 ii. Prepare the Delegation of Disclosure Authority Letter (DDL) for the individual. The DDL is explained in DoDD 5230.11 (<http://www.dtic.mil>). An example template is provided on the AKO portal page <https://www.us.army.mil/suite/page/278081>. This sample contains all known clauses and is specific to account access grants for AKO/DKO and AKO-S/DKO-S; however, all clauses may not be required. In addition, signature block(s) have not been included. The document should be edited and printed on letterhead as appropriate.
- 15 iii. **NOTE:** The exemplar DDL does not contain references to NDP-1 categories 3, 4 and 7 as access to these data categories by a non-U.S. citizen is outside the scope of this procedure.
- iv. Create a record of access granted for inclusion in the applicant's file.
- v. Create a document package containing:
 - 20 a. A commander's statement describing the need-to-know/need-to-share tied to the applicant's activity level certification.
 - b. The DDL.
 - c. A statement from the installation Information Assurance Manager (IAM) stating that proper security procedures are in place.
 - 25 d. A record of favorable security adjudication.
 - e. As issued by the local employing office, an Acceptable Use Policy (AUP) agreement signed by the applicant.
 - f. Declaration that the applicant is under the supervision of a U.S. citizen.
 - g. Declaration of the applicant's and sponsor's AKO/DKO user ID.
 - h. Declaration of the country of citizenship.
- 30 vi. Submit the created documentation package to obtain DAA approval.
- vii. Update the environment C&A documentation with the approved application.
- 35 viii. Submit the approved application package to the Regional Chief Information Office (RCIO) Information Assurance Program Manager (IAPM) (*Note: RCIO is the language used within the regulation although they no longer exist in that form. Operationally, this will be the Theater Network Operations Center (TNOSC)*).
- ix. After obtaining DAA approval, submit the application package to NETCOM/9th SC (A) Office of Information Assurance and Accreditation (OIA&C) <http://www.netcom.army.mil/docs/ContactList.pdf>.
- 40 x. After obtaining NETCOM/9th SC (A) OIA&C approval, submit the application package to Deputy Chief of Staff (DCS) G2. www.g2.hqsareur.army.mil, <http://www.usarso.army.mil/DCSG2/>

The following steps occur independently of the requestor:

- 45 xi. The IAPM shall review and process the request unless it can be rejected for cause.
- xii. The IAPM submits the package to the DAA for review and approval.
- xiii. NETCOM/9TH SC (A) shall review and process the request unless it can be rejected for cause.
- xiv. DCS G2 shall review and process the request unless it can be rejected for cause.

Upon receipt of the above approvals, the requestor shall:

- 50 xv. **The sponsor approves the account as email only.**
- xvi. Forward the documentation package with approvals to CIO / G6. The package should be sent to ciog6.foreign.policy@us.army.mil.
- xvii. CIO/G6 notifies the AKO/DKO PMO of package receipt.
- 55 xviii. Upon approval, the AKO/DKO PMO upgrades the account access to "portal access". An email is sent by the AKO/DKO PMO to the sponsor stating the action taken.



Appendix A - Available Account Types

If the individual is not a member of the United States military or a full-time, regular United States Civil Servant, the AKO/DKO portal provides two account types for the classification of non-U.S. citizens: **Foreign Officer** or **Local National**. Non-U.S. citizen members of the United States military and Civil Service use account types that are equivalent to those assigned to U.S. citizens occupying the same job positions; however, this does not exempt non-U.S. citizens from the described procedures.

Use the account type **FOREIGN OFFICER** if the individual qualifies as a member of any one of the following groups as defined by AR 25-2, Section 4-15, paragraph a:

- Foreign Liaison Officer (FLO)
- Cooperative Program Personnel (CPP)
- Engineer and Scientist Exchange Program (ESEP)
- Standardization Representative (STANREP)
- Military Personnel Exchange Program (MPEP)

AKO/DKO further restricts the following categories of job assignment to the **FOREIGN OFFICER** account type:

- Foreign Government Official (career or elected)
- Diplomat or Embassy Staff
- Member of a Law Enforcement Agency
- Member of the Intelligence Community
- Member of the Judiciary or other Legal representative
- Member of a Public Works Agency

Use the account type **LOCAL NATIONAL** if the individual qualifies as any one of the following:

- Volunteer
- Employee of the sponsoring office or of the United States Government but not a civil servant
- Contractor
- Employee of a contracted firm
- Non-appropriated funding salaried
- Any other non-U.S. citizen not categorized by any of the above

Account Access Types

The **access** determines the level of interaction that the non-U.S. citizen may have with AKO/DKO resources. An access assignment is not an account type. As described by AR 25-2, Section 4-15, paragraph (b), *"Approval to access the NIPRNET does not equate to authority to exchange data or access systems located on that network."*

- An "email only" access assignment allows just that, email only.
- A "portal access" access assignment allows use of all Knowledge Centers and Web Pages that are permitted access by their administrators, IM, Chat and Forums. A portal access qualified account may also upload and download files, use search and access the white pages listing.

Note that email-only and portal access assignments will both authenticate as an account holder's credentials when supplied via an access made by Single Sign-on or Lightweight Directory Access Protocol (LDAP). The access assignment is independent of the validity of a user ID / password combination. Validation by AKO/DKO SSO/LDAP authentication does not guarantee access to a particular resource as the resource owner may impose additional restrictions outside of AKO/DKO jurisdiction.



Appendix B - Selecting a Category - Guidelines

Required documentation and execution of procedure is the responsibility of the requesting sponsor or the authorizing official, whichever is appropriate for the category selected. All category checklists may be found on the portal policies page (<https://www.us.army.mil/suite/page/278081>).

Equivalent investigation – A non-U.S. citizen who has had a favorable background investigation equivalent to that required to obtain a SECRET clearance may be granted a portal access account with the appropriate full account holder sponsorship of that guest account. This qualifies as a **Category 0** account and also permits access to AKO-S (if authorized.) Proof of clearance must be attached to the application. A designation of *favorable security review* is available only to non-U.S. citizens who were approved by agencies within the United States or its territories or have had favorable security adjudication while within the United States or its territories. Pursuant to National Security Position Handbook 440-7, Appendix B, the documentation required to obtain a favorable security review at the SECRET level is:

- Form 9-3056 *Personnel Security Action Request*
- SF 86 *Questionnaire for National Security Positions* (optional SF 86A *Continuation Sheet*, if required)
- SF 87 *Fingerprint Chart*
- Position Designation Record
- Release to obtain a credit report

For further information, refer to the document "*Requesting OPM Personnel Investigations*", available at the website: <http://www.opm.gov/extra/investigate/IS-15.pdf>.

Reasonable Trust – A non-U.S. citizen who has established a reasonable trust relationship with the office of employment may be allowed an email only account after approval by the onsite DA Information Assurance Security Officer (IASO). To define "local security concerns" the following is taken into consideration. The arrival of such personnel must occur under some agreement acknowledge by the facility. This agreement should state the purpose and scope of activity. The assumption is that if local domain access has been granted, then a certain amount of "reasonable trust" exists. In other words, if the non-US citizen can be granted access to the local domain, then at a minimum, an email only account is warranted. On the other hand, if domain access has not been granted and the expectation is that the non-US citizen will be accessing AKO/DKO via the Internet, then a "local trust" has not been established since access from the Internet is an unregulated forum. Reasonable trust may also be established by conducting a local agency check including law enforcement or credit. When reasonable trust has been established, this qualifies as a **Category 1** account.

Grant by Country of Origin – citizens of certain partner countries may have access rights equivalent to those of US citizens. Partner countries are qualified by the State Department and as listed in the DAMI-CDD (380-10) Memorandum of 20 January 2006. A list of currently recognized partner countries can be obtained by sending a request via email to ako.nonus.accounts@us.army.mil. This qualifies as a **Category 2** account.

IT Level Designations –As used in this procedure, IT levels are equivalent to the IA IT levels described in AR 25-2, Section 4-14, § (a). Form DD 2875 is required as an attachment to a **Category 3, 4 or 5** checklist. Note that interim status applications cannot be accepted.

Local Nationals – citizens of the station country or ex-patriots holding a visa valid for work in the station country. This qualifies as a **Category 7** account.

Active Service Members – **Checklist ASM** must be used.

Civilian Employees - **Checklist DODCE** must be used.



5 **Grant by Waiver** – Is a signed statement issued by the Knowledge Management Division (KM) of CIO/G6. A waiver is not processed by a checklist or by email to ako.nonus.accounts@us.army.mil. Waiver requests sent to this address will be returned unprocessed. A waiver's issuance is preceded by the sponsor or authorizing official obtaining:

- 10
- A statement from the commanding officer (U.S.) declaring the specific mission requirement;
 - A statement from the data owner declaring acceptance of the mission requirement and granting permission to access such data; and,
 - A statement from the governing DAA accepting the risk.

15 The above three documents are submitted to ciog6.foreign.policy@us.army.mil. Upon approval, CIO/G6 will deliver a copy of the waiver to the AKO/DKO Account Action Officer.



Appendix C – Account Guidelines and Modification

- (1) Sponsors must be citizens of the United States even if they are full account holders with sponsorship privileges.
- 5 (2) If the non-U.S. citizen has not previously held an AKO/DKO account, they must apply for one using New Registration on the portal splash page. The country of citizenship must be declared by the applicant when the account is created. If an existing account is to be transferred between sponsors, the current sponsor must contact the help desk and have the sponsorship changed to the new sponsor. If the existing sponsor is not available or an existing account has
10 been deactivated, the new sponsor must send an email to ako.nonus.accounts@us.army.mil and request assistance.
- (3) To ensure that an account is not denied by AKO/DKO, delivery of the required email and attachments should be sent once the user ID is known. Sponsor indifference towards the established procedures or the assignment of account types unapproved for use by a non-U.S. citizen will result in the loss of sponsorship privileges, notification of the chain-of-command and HQDA CIO/G6, possible loss of AKO/DKO credentials; and, in egregious circumstances, legal and criminal proceedings.
15
- (4) Account authorizations are **not transferable between sponsors** in differing commands or DOIM / IAPM jurisdictions. In this situation, the new sponsor is responsible for re-validating the user within the new job assignment.
20
- (5) Sponsors are responsible for setting the proper account revocation date if the duration of activity does not coincide with a default account validity period.
25
- (6) Emails to AKO/DKO and CIO / G6 missing the required checklist for the category selected will not be honored. Applications resulting in abandonment or unanswered emails originated by AKO/DKO or CIO/G6 to the sponsor after fifteen (15) days will be denied with a deletion notification sent to the sponsor or validating official.
30
- (7) **Common Access Card (CAC) Issuance** – receipt of a CAC by personnel who are not citizens of the United States is insufficient grounds for granting a portal access type account. The requirement to use a CAC for AKO/DKO access and possession of such for justification of having an account are mutually exclusive properties.
35
- (8) **Changes to the Account** – non-U.S. citizens who hold AKO/DKO accounts may affect account changes including personal contact information, password, security questions and mail options. Only sponsors may change the FIN/SSN or Country of Citizenship. This action must be performed in coordination with the AKO/DKO Customer Support Center (CSC).
40