



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, U.S. ARMY GARRISON-YONGSAN
UNIT #15333
APO AP 96205-5333

13 FEB. 2017.

IMYN-ZA

UNITED STATES ARMY GARRISON-YONGSAN (USAG-Y) POLICY LETTER # 46

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Transition to Web-Based, Out Processing (OUTPROC) Installation Support Module (ISM) to Manage Service Members Out-Processing

1. REFERENCES:

a. Installation Management Command (IMCOM) Policy Memorandum 600-8-1, Installation Out-Processing.

b. Army Regulation (AR) 600-8-101, Personnel Processing, 19 February 2015.

2. PURPOSE: To provide guidance on accessing and maximizing the use of the web-based ISM to manage service members' in or out-processing. The ISM is an automated system that imports and exports personally identifiable information for United States Army Soldiers to and from external sources to provide the Army a capability manage administrative personnel and logistical functions at the Installation level. ISM provides Installation Commanders and Staffs with an automated information system that assists in the accomplishment of day-to-day administrative tasks in the areas of Soldiers' In/Out-processing. ISM is used to print installation clearing papers.

3. APPLICABILITY: In accordance with IMCOM Policy Memorandum 600-8-1, Garrisons will manage Soldiers' Out-Processing by utilizing web-based ISM. Soldiers and agencies spend unnecessary time and effort performing a function that can be automated.

4. POLICY:

a. All Installation activities are required to utilize ISM to make the Installation clearance process more efficient and expedient.

b. Pre-clearance and self-clearance (Soldier physically goes around) will be maximized with Soldiers visiting only those agencies that require their physical presence and cannot be accomplished through ISM.

IMYN-ZA

SUBJECT: Transition to Web-Based, OUTPROC Installation Support Module (ISM) to Manage Service Members Out-Processing

Agencies requiring Soldiers' presence will be identified when he/she reports to the MPD to receive clearance papers.

c. Commanders and Senior Mission Partners must make every effort to minimize the number of agencies requiring the service members presence.

5. Activities not currently utilizing the ISM module must request access. Commanders and Senior Mission Partners are required to do the following:

a. Identify staff (primary and secondary), in your activity, who requires access to ISM. Designated staff must complete DD Form 2875 and submit it to Installation Functional Administrator. To request access to the ISM module, log on to <https://ism.army.mil/> and click "request account."

b. Provide a roster with primary and secondary staff members who have access to the ISM module to the USAG-Y, Director, Directorate of Human Resource.

5. The point of contact for this policy is the Director, Directorate of Human Resources at DSN 738-5017.

Encl
DD Form 2875



J. SCOTT PETERSON
COL, CA
Commanding

DISTRIBUTION: A

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		DATE (YYYYMMDD)
<input checked="" type="checkbox"/> INITIAL	<input type="checkbox"/> MODIFICATION	<input type="checkbox"/> DEACTIVATE
<input type="checkbox"/> USER ID		
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	9. DESIGNATION OF PERSON
		<input type="checkbox"/> US <input type="checkbox"/> FN	<input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN
		<input type="checkbox"/> OTHER	<input type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)			
<input checked="" type="checkbox"/> 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

Requesting access as a Work Center User for the Installation Support Module (ISM) to pre-clear Soldiers

14. TYPE OF ACCESS REQUIRED:			
<input checked="" type="checkbox"/> AUTHORIZED		<input type="checkbox"/> PRIVILEGED	
15. USER REQUIRES ACCESS TO:			
<input type="checkbox"/> UNCLASSIFIED		<input type="checkbox"/> CLASSIFIED (Specify category)	
<input checked="" type="checkbox"/> OTHER <u>INSTALLATION SUPPORT MODULE (ISM)</u>			
16. VERIFICATION OF NEED TO KNOW		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)	
I certify that this user requires access as requested. <input type="checkbox"/>			
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)

26. NAME (Last, First, Middle Initial)

27. OPTIONAL INFORMATION (Additional information)

Deros or CAC card expiry date:

CAC card 10 digits:

Date of Birth:

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 <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> 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)
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

- (1) Name. The last name, first name, and middle initial of the user.
- (2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
- (3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).
- (4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
- (5) Official E-mail Address. The user's official e-mail address.
- (6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.
- (7) Official Mailing Address. The user's official mailing address.
- (8) Citizenship (US, Foreign National, or Other).
- (9) Designation of Person (Military, Civilian, Contractor).
- (10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
- (11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).
- (12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

- (13) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
- (14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)
- (15) User Requires Access To: Place an "X" in the appropriate box. Specify category.
- (16) Verification of Need to Know. To verify that the user requires access as requested.
- (16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
- (17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- (18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (19) Date. Date supervisor signs the form.
- (20) Supervisor's Organization/Department. Supervisor's organization and department.
- (20a) E-mail Address. Supervisor's e-mail address.
- (20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.