



AUG 30 2013

VETERANS' PROGRAM LETTER NO. 04-13

TO: ALL NATIONAL OFFICE STAFF
ALL REGIONAL ADMINISTRATORS
ALL DIRECTORS OF VETERANS' EMPLOYMENT AND
TRAINING SERVICE
ALL COMPETITIVE GRANTEEES

FROM: KEITH KELLY 

SUBJECT: New User Account Setup Process

I. Purpose: To streamline the new user account setup process for the Veterans' Employment and Training Service (VETS) Operation and Program Activity Report (VOPAR) system by assigning to the Regional VOPAR administrators the responsibility of creating new VETS and grantee users in VOPAR and ensuring the proper documentation associated with new user accounts are complete and accurate.

II. Reference(s): <http://labornet.dol.gov/itc/it/operations/csh-4/CSH-4-Volume-0-Information-Security-Policies.doc>; 18 U.S. Code 1030, Computer Fraud and Abuse Act of 1986; National Information Infrastructure Protection Act of 1996

III. Rescinds (or Supersedes): Not Applicable

IV. Background: New VOPAR user requests were previously made via email and the New User form and Rules of Behavior (ROB) documents were signed and retained in a central repository at the National Office. VETS must continue to ensure the VOPAR system meets all department and federal security requirements.

Employment and Training Administration (ETA), which houses VOPAR, requires that the ROB be retained indefinitely.

More information on the Rules of Behavior can be found in the US Department of Labor Computer Security Handbook, Edition 4.0, Volume 0 Information Security Policies Version 1.1, October 2011 (<http://labornet.dol.gov/itc/it/operations/csh-4/CSH-4-Volume-0-Information-Security-Policies.doc>).

V. Summary of Changes: The following describes the process for the new user account forms:

- VOPAR Grantee New User Account Authorization Form
 - VOPAR VETS Staff New User Account Authorization Form
 - VOPAR Rules of Behavior
1. The Director for Veterans' Employment and Training (DVET) or the Grant Officer's Technical Representative (GOTR) reviews and signs the VOPAR New User Account Authorization Form and the ROB.
 2. All forms must be scanned and emailed to the Regional Administrator for Veterans' Employment and Training (RAVET), where they will be assigned to the regional VOPAR administrator.
 3. The Regional VOPAR administrator is authorized to setup the new user on the VOPAR system.
 4. The Regional VOPAR administrator then has 10 business days after the New User form and the ROB have been received in the Regional Office to forward the approved forms to the National Office.
 5. The National Office VOPAR Administrator will review all forms to ensure compliance. If these forms are not completed properly or signed as required, the account will be deactivated temporarily and the National Office VOPAR Administrator will work with the appropriate Regional Office to rectify.

VI. Inquiries: Appropriate Regional POC:

Region	Contact Name	Contact Number	Contact Email
Boston	Charlotte Brindley	617-565-2080	brindley.charlotte@dol.gov
Philadelphia	Virginia Youst	215-861-5390	youst.virginia@dol.gov
Atlanta	Bernadette Walsh	404-562-2306	walsh.bernadette@dol.gov
Chicago	Alfredo Mendoza	312-353-0971	mendoza.alfredo@dol.gov
Dallas	David Vogt	972-850-4722	vogt.david@dol.gov
San Francisco	Rebecca Klein	415-625-7675	klein.rebecca@dol.gov

VII. Expiration Date: Until rescinded or superseded

VIII. Attachment(s):

- VOPAR Rules of Behavior
- VOPAR Grantee User Account Authorization Form
- VOPAR VETS User Account Authorization Form

**Veterans' Employment Training Service (VETS)
 Operations and Programs Activity Report (VOPAR)
 User Account Authorization Form**

Each VETS employee who will need access to VOPAR must complete this form when requesting a new account or a modification to an existing account. For those that provide support for more than one office, a separate account for each office is required. Submit the form to your supervisor for authorization and submission to the National Office.

For those authorizing accounts, this form and a signed ROB should be converted to Adobe PDF files and sent as email attachments to vopar-help@dol.gov using the filename standard of **last name, first name.pdf**. The subject of the email should be **VOPAR Account**.

Name: _____
First M.I. Last (include any titles, such as: "Jr.", "Sr.", etc.)

Telephone: _____ E-Mail Address: _____

This form is to request a: (check only one)

New account

Change to an existing account

Role: (check only one)

State Office (except DVET)

National Office

DVET/GOTR

TAP Administrator

Regional Office (except RAVET)

VOPAR Administrator

RAVET

Assigned Office: (check only one)

National Office

Missouri State Office

Boston Regional Office

Montana State Office

Philadelphia Regional Office

North Carolina State Office

Atlanta Regional Office

North Dakota State Office

Chicago Regional Office

Nebraska State Office

Dallas Regional Office

New Hampshire State Office

San Francisco Regional Office

New Jersey State Office

Alaska State Office

New Mexico State Office

Alabama State Office

Nevada State Office

Arkansas State Office

New York State Office

Arizona State Office

Ohio State Office

California State Office

Oklahoma State Office

Colorado State Office

Oregon State Office

Connecticut State Office

Pennsylvania State Office

District of Columbia Office
Delaware State Office
Florida State Office
Georgia State Office
Guam Office
Hawaii State Office
Iowa State Office
Idaho State Office
Illinois State Office
Indiana State Office
Kansas State Office
Kentucky State Office
Louisiana State Office
Massachusetts State Office
Maryland State Office
Maine State Office
Michigan State Office
Minnesota State Office
Mississippi State Office

Puerto Rico Office
Rhode Island State Office
South Carolina State Office
South Dakota State Office
Tennessee State Office
Texas State Office
Utah State Office
Virgin Islands Office
Virginia State Office
Vermont State Office
Washington State Office
Wisconsin State Office
West Virginia State Office
Wyoming State Office

Supervisor's Authorization

I hereby authorize the System Administrator to create or modify a user account with the specified access for the above user.

Signed: _____ Date: _____

Print Name: _____

Title, Office, and Phone: _____

**The Veterans' Employment and Training Service (VETS)
Operations and Programs Activity Report (VOPAR) System
Rules of Behavior (ROB)**

Agency Name: U.S. Department of Labor (DOL)
Veterans' Employment and Training Service (VETS)
200 Constitution Avenue, N.W.
Room S-1316
Washington, DC 20210

Application Name: VOPAR

Purpose of Rules: The ROB are established to provide guidelines regarding the usage of the VOPAR system and the consequences of non-compliance.

As a user of the VOPAR system, you are responsible for adhering to the following rules when accessing VOPAR:

- Unauthorized access or use of the system for any purpose other than official government business is punishable by a fine, imprisonment, or both. Your use of the system may be monitored (18 U.S. Code 1030).
- You are entirely responsible for any and all activities that occur under your system account while logged into the VOPAR System.
- Unauthorized attempts to upload information or change information on the VOPAR system are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996.
- Only authorized users are allowed access to VOPAR system data.
- VOPAR system data (printed or non-printed) must not be divulged to any individual not specifically authorized to receive such information.
- Sharing user login information, i.e., your username and password, is strictly prohibited. You must take the necessary steps to ensure that others do not use your account to gain unauthorized access to this system.
- VOPAR system data must not be tampered with, changed, deleted or altered unless the user is authorized to do so.
- The VOPAR system may not be used to collect personal information.
- Any fraudulent activities, including illegally using someone else's account to process VOPAR system data, posting system messages, or emailing customers for personal gain or concern is strictly prohibited.
- This system may not be used to breach the security of any system user or to gain access to another person's (internal or external) computer, software, or data.
- This system may not be used to circumvent the system authentication or security of any account, network, or host. This includes, but is not limited to: accessing data that is not intended for you, logging into a server or account to which you are not authorized to access, or probing the security of other networks, and so on.

- Using tools to compromise the security of this system, such as password-guessing programs, cracking or packet sniffing tools, or any network probing tools is strictly prohibited.
- Any attempt to disrupt or deny operation of this system is strictly prohibited.
- Transmitting viruses, via email or otherwise, to this system is forbidden.
- It is prohibited to sell any of the data or information obtained from this system.

Users shall be responsible for notifying temiquel.maria@dol.gov, epps.rhonda.l@dol.gov, or mcclain.chris@dol.gov immediately of any unauthorized use of their account or any other breach of security in regard to these policies. VETS will investigate any and all suspected violations of these policies and reserves the right to take corrective or legal action against the violator. If an investigation is warranted, user account access may be disabled. As a system user, you are responsible for ensuring that your use of the system complies with the policies stated therein. Any system user who does not agree to be bound by these policies should immediately discontinue use of this system and should notify VETS to remove their account.

All system users of the VOPAR system must follow the rules outlined here. Any abuse of these policies may be punishable by law. Questions regarding complaints or violations of this policy may be directed to your supervisor for appropriate handling and resolution.

The VETS Information Systems Security Officer (ISSO) is responsible for supporting and enforcing the established policies set forth in the ROB. The policies set forth in the ROB have been put in place to protect the VOPAR system users from the adverse impact that can result from intentional violations of the ROB. If you believe you have been the victim of activities that are in violation of the ROB, contact the VETS ISSO, and the appropriate action will be taken to investigate or attempt to resolve the alleged violation. You may report your concern or incident to temiquel.maria@dol.gov, epps.rhonda.l@dol.gov, or mcclain.chris@dol.gov. Please make sure you include the date and time of the incident, log files (if appropriate), examples or any other information that may be useful to the investigation, and verification of the incident as well as your name and phone number or e-mail address so this office can contact you directly.

VETS reserves the right to disable your account access without notice for violation of these policies.

Unauthorized use of VETS Information Technology resources by a user is a violation of Federal Law and could leave the user vulnerable to disciplinary action, administrative action, criminal action, and /or financial liability. Anyone using VETS Information Technology resources expressly consents to monitoring, and violators shall be reported to the proper authorities.

Signature _____

Date _____