U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

EMPLOYMENT AND TRAINING ADMINISTRATION
ENTERPRISE BUSINESS SUPPORT SYSTEM
RULES OF BEHAVIOR

VERSION 2.0

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
11/9/06	**Rules of Behavior/Version 2.0**	**Miranda Key**	**Modified to address DOL's rules that were released June 2006**

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
11/9/06	**2.0**	**Miranda Key**
11/9/06	**2.0**	**Joan Sullivan**
11/9/06	**2.0**	**Michael Chepkwony**
11/9/06	**2.0**	**Dave Wilson**

TABLE OF CONTENTS

1 RULES OF BEHAVIOR

As a user of the Employment and Training Administration (ETA) Enterprise Business Support System, I understand that I am personally responsible for my use and any misuse of my user account and password. I understand that by accessing a U.S. Government information system that I must comply with the following requirements:

1. Users must:

    - Safeguard the information to which you have access at all times.
    - Obtain your supervisor's written approval prior to taking any Department of Labor (DOL) sensitive information home or otherwise away from the office. The supervisor's approval must identify the business necessity for removing such information from the DOL facility.
    - Adhere to the security policies and procedures when approval is granted to take sensitive information home or away from the office.

2. The system is intended for official government use only.

3. The system may not be used for commercial purposes, for financial gain, or in support of "for profit" non-government activities.

4. The government reserves the right to monitor the activities of any user and/or any machine connected to ETA Enterprise Business Support System.

5. The ETA Enterprise Business Support System and the information contained within are the property of the federal government. DOL owns the data stored on these systems, including all messages and information, even those deemed personal.

6. No data may be transmitted on the system that is more sensitive than the level for which that system has been approved.

7. Information that was obtained via ETA Enterprise Business Support System may not be divulged outside of government channels without the express, written permission of the system owner.

8. Any activity that would discredit the Department, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material, is prohibited.

9. Any activity that violates Federal laws for information protection (e.g., hacking, phishing, spamming, etc) is prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

10. ETA Enterprise Business Support System user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism

should never be shared or stored any place easily accessible. If stored, a password may not be stored in a clear-text or readable format. Sharing of user accounts is grounds for terminating system access.

11. The information owner must approve and authorize the employee's level of access in writing via documented account management procedures.

12. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), pre-public release information such as economic indicators, proprietary data, or export controlled software or data is prohibited. All use of copyrighted software must comply with copyright laws and license agreements.

13. Remote off-site (e.g., dial-in) access to a computer system must be approved and authorized in writing by the appropriate management authority and the system owner.

14. Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.

15. Only devices that are formally certified and approved by the system owner shall be connected to the ETA Enterprise Business Support System. At no time should personally-owned equipment be connected to the system.

16. Any security problems or password compromises must be reported immediately to the senior agency information security manager.

17. I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 10 years in jail for the first offense for anyone who commits any of the following violations:
    - Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
    - Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system.
    - Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
    - Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

18. When the user no longer has a legitimate need to access the system, the Federal manager/supervisor or designee, or Contract Officer Technical Representative must submit a Enterprise Business Support System Access Request Form immediately to the system's designated Help Desk support staff so that the user's access can be terminated.

Apart from the guidelines in the DOL Policy; ETA Computer Security Handbook, "Information Technology (IT) Security Policy Manual" (January 31, 2005), and "IT User Procedures" (January 31, 2005) documents, the Rules of Behavior (ROB) delineated below pertain to all persons who utilize the Enterprise Business Support System. As a customer and/or user of the Enterprise Business Support System, you are responsible for adhering to the additional rules listed below:

1. 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).
2. You are entirely responsible for any and all activities that occur under your system account on the website.
3. Unauthorized attempts to upload information or change information on this website 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.
4. Only authorized users are allowed access to the Enterprise Business Support System data.
5. Enterprise Business Support System data (printed or non-printed) must not be divulged to any individual who is not specifically authorized to receive such information.
6. 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.
7. Enterprise Business Support System data must not be tampered with, changed, deleted, or altered unless the user is authorized to do so.
8. Enterprise Business Support System data must not be disclosed without proper authorization from the management of the ETA Office of Performance and Technology (PROTECH) or the applicable ETA Program Office in the national office.
9. This website may not be used to collect personal information, such as employer or attorney information (e.g., mass mailing) to conduct personal business without their (the employer or attorney) proper consent or the consent of the U.S. DOL. You are not allowed to use this website to send commercial messages (e.g., advertisements) or unsolicited bulk emails (e.g., informational announcements like loss of family notices).
10. Posting material or information that is unlawful, such as obscene materials, inappropriate content, or language on this site is prohibited. Users will be held solely responsible for any information posted and published to this website that is in violation of this policy. Users shall be held responsible for ensuring that any information or content posted/published is in fact appropriate for the intended recipient(s).
11. Any fraudulent activities, including illegally using someone else's account to process Enterprise Business Support System, post system messages, email customers for personal gain or concerns is prohibited.
12. This website 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, without the proper consent of the person.
13. This website may not be used in any attempt to circumvent the system authentication or security of any account, network, or host. Please note that this would include, but is not limited to, accessing data that is not intended for your information, logging into a server or account you are not authorized to gain access, or probing the security of other

networks, and so on.

14. Using tools to compromise system security of this website, such as password-guessing programs, cracking or packet sniffing tools, or any network probing tools is strictly prohibited, and, legal action may be taken against you.
15. Any attempt to disrupt or deny operation of this website is strictly prohibited.
16. Transmitting viruses, via email or otherwise, when using this system is not allowed.
17. It is prohibited to sell any of the data or information gained from this website.

Users shall be responsible for notifying the DOL, ETA immediately of any unauthorized use of your account or any other breach of security in regards to these polices. ETA 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, users' 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 polices should immediately discontinue use of this system and should notify the Help Desk to remove their account at karim.omar@dol.gov and wilson.david@dol.gov.

All system users of the Enterprise Business Support Systems Website System must follow the rules outlined here. Any abuse of these policies may be punishable by law. Questions regarding complaints, violations, or this policy may be directed to the Help Desk at karim.omar@dol.gov and wilson.david@dol.gov for appropriate handling and resolution.

The DOL, ETA, PROTECH's Security Manager is responsible for supporting and enforcing the established policies set forth in the ROBs. The policies set forth in the ROBs have been put in place to protect the Enterprise Business Support Systems (Enterprise Business Support System) website system users from the adverse impact that can result from intentional violations of the ROBs. If you believe you have been the victim of activities that are in violation of this ROBs, the PROTECH will take appropriate action to investigate and attempt to resolve the alleged violation. You may report your concern or incident to this division at ETA.IT.Security@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.

DOL reserves the right to disable your account access without notice for violation of these polices!

Penalty

Unauthorized use of ETA 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 ETA information technology resources expressly consents to monitoring, and violators shall be reported to the proper authorities.

Effective: November 9, 2006