IT System Rules of Behavior

As a user of the U.S. Department of Labor (DOL) computer network (the Employee Computer Network/Department Computer Network (ECN/DCN), I understand that I am personally responsible for my use and any misuse of my system account and password. I understand that by accessing a U.S. government information system that I must comply with the following requirements:

1. Adhere to all security policies. Policies are governed through the Computer Security Handbook (CSH) and the Department of Labor Manual Series (DLMS). Employees are responsible for reviewing these policies.
    - DLMS: http://labornet.dol.gov/workplaceresources/policies/DLMS/.
    - CSH: http://labornet.dol.gov/itc/it/esd/csh-5/
2. The network is intended for official government use only. Limited personal use that does not violate DOL policy may be authorized by a DOL federal supervisor or Contracting Officer Representative (COR). How?
3. The network may not be used for commercial purposes, financial gain, or in support of "for profit" or "non-profit" non-government activities.
4. The federal government reserves the right to monitor the activity of any computing device (e.g., desktop workstations, laptops, mobile devices), Universal Serial Bus (USB) drives, etc. connected to its infrastructure.
5. The network is the property of the federal government. DOL owns all data that is collected, used, stored, and transmitted, on its infrastructure, including business and personal email messages and information.
6. No data may be transmitted on a system that is more sensitive than the level for which that system has been approved.
7. Information that was obtained via the network may not be divulged outside of federal government channels without the express written authorization of the data owner.
8. Any activity that discredits the Department, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, racist, abusive, sexually explicit, obscene, harassing, inflammatory, unlawful, or intimidating messages or material or otherwise objectionable statements, language, or content is prohibited.
9. Any activity that violates federal or state laws for information protection (e.g., hacking, spamming, etc.) is not permitted.
10. User accounts are provided solely for the use of the individual for whom they are created.
11. Passwords or any other authentication mechanism shall not be shared with; used by; disclosed; written down; or stored in a clear-text or readable format any place accessible to others.
12. All computing devices connected to the network must be configured to comply with the

password complexity characteristics outlined below.

- Passwords must be at least eight (8) alphanumeric characters in length
- Passwords must contain a mix of characters from the following four (4) categories :
  - English upper case letter (A, B, C, etc.)
  - English lower case letter (a, b, c, etc.)
  - Special character ({,}, [,], (,), <, >,:, ', ",?, /, |, `, ~,!, @, #, $, %, ^, &, *, _, -, +, =, etc.)
  - Arabic number (0, 1, 2, 3, etc.)
- Passwords must not consist of any of the following:
  - Dictionary words or common names (Betty, Fred, Rover, etc.)
  - Portions of associated account names (user Identification (ID), login name, etc.)
  - Consecutive character strings (abcdef, 123456, etc.)
  - Simple keyboard patterns (asdfgh, qwerty, etc.)
  - Generic passwords such as a password consisting of a variation of the word "password" (e.g., P@ssword1)

13. User account passwords must be changed every 90 days. System service and other similar account (e.g., System Administrator) passwords must be changed every 90 days.
14. Reuse of the twelve (12) previously used account passwords (i.e., password history) is prohibited to prevent users from using the same password for 12 previous password changes.
15. After three (3) invalid password attempts, the user account will be locked out for a period of 15 minutes. If reactivation of a user account is required before the lockout period expires, the user must visit the Enterprise Service Desk or Regional IT Manager and present their DOL ID badge to request the service or follow the current process.
16. All computing devices must be configured to automatically time-out or engage a password protection screen saver after a period of 15 minutes of inactivity. In addition, computing devices must allow authorized users to manually disconnect or engage a password protection screen saver.
17. Federal supervisors and CORs are allowed to request a password reset for their federal or contractor employee subordinates, respectively.
18. DOL federal and contract employees in support of official government business such as telework (working from home), while on business travel (hotels, conferences, airports, etc.) or other non-government remote off-site locations may use approved Government Furnished Equipment (GFE) with an approved wireless technology for remote access.
19. Only computing devices that are DOL Government Furnished Equipment are permitted to connect to DOL IT systems.
20. DOL federal and contract employees shall not disable or circumvent security implementations installed on the GFE or wireless device used to access the network.
21. DOL federal and contract employees shall not allow the GFE device to be dual homed at any

time. Dual-homed is when the GFE has more than one active network connection and communicating on these connections. Therefore when using the GFE on a wired network connection, the wireless connection should be disconnected or removed from the GFE. The opposite also applies, when using the wireless feature; the GFE must not be connected to a wired network (i.e. home network, DOL network, or other).

22. Only approved collaborative (audio and video conferencing) computing mechanisms can be connected to DOL IT systems. Collaborative computing mechanisms must be approved by the user's management prior to connecting to a DOL IT system. Collaborative computing mechanisms must be disconnected from the IT system(s) when not in use to avoid undesired automatic activation.
23. All computing devices containing agency sensitive information (e.g., employee names, social security numbers, personal financial data, etc.) must be encrypted and password protected in accordance with DOL policies and procedures.
24. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data are prohibited. All use of copyrighted software must comply with copyright laws and license agreements.
25. Peer-to-peer file sharing (also known as P2P) is not allowed on DOL GFE. This technology allows users to download media files such as music, movies, and games using a P2P software client that searches for other connected computers.
26. Software which facilitates behaviors which are expressly prohibited under the code of ethical behavior, such as gaming, gambling, possession or distribution of pornographic materials, unauthorized transmission or sharing of copyrighted material, etc. is not permitted.
27. DOL federal employees and contractors do not have a right, nor should they have an expectation, of privacy while using any government office equipment at any time, including remote access, business and personal Internet usage.
28. Any security problems or account/password compromise must be reported immediately to your agency Information Systems Security Officer (ISSO) and security personnel.
29. Security-minded users are essential to the network's defense in combating email Phishing and SPAM. Users should verify email messages are from a trusted/known sender; should never access/click on any links from unknown or suspicious senders; should never provide account information to anyone (known or unknown); and should never open any attachments from unknown or suspicious senders. Users are required to:
    a. Not open or forward the email message,
    b. Delete suspect/suspicious email message from email "Inbox" and "Deleted Items" folders,
    c. Not click on or access web links provided in suspect/suspicious email messages, and
    d. Report receipt of any suspected/suspicious Phishing or SPAM email messages immediately to your agency ISSO or to the Enterprise Service Desk.
30. DOL federal and contract employees must ensure the security of GFE by:

a. Periodically connecting GFE to the network via the system's secure remote access capability, thus allowing the GFE to receive necessary software patches and upgrades. It is essential and required that all users connect their GFE to the network at least once every 30 calendar days in order to receive patches and updates.
b. Preventing the loss and/or theft by physically protecting the GFE as though it were your own personal equipment.
c. Not leaving the GFE laptop unattended for extended periods of time.
d. Using a laptop locking device (cable) when appropriate; i.e., when using a laptop in public areas.
e. Reporting the loss or theft of GFE devices to the Enterprise Service Desk at 1-855-Labor-It or 1-855-522-6748, within thirty minutes of noticing the loss or theft of the GFE.
f. Not allowing unauthorized individuals to access the internet or the network using the GFE.
g. All DOL users may request specially configured mobile devices, laptops and/or cell phones, when traveling to locations that the Department, the Department of Homeland Security, and/or the Department of State have been deemed to be of significant risk. All DOL users must return the devices to the Enterprise Service Desk or approved location upon their return so the devices can be inspected and reimaged for reuse.

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

32. Users are to not to use social media/networking sites nor post OTIS information on public websites.