Online Learning Center^2 (OLC^2) Rules of Behavior

In accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, the following "Rules of Behavior" for the U.S. Department of Energy System is hereby established. The Office of the Chief Human Capital Officer (HC) expects each user to observe the following rules when using Online Learning Center^2 (OLC^2).

1. **Authorized Access:** All requests for access must go through the OLC^2 Help Desk for authorization.
2. **Assignment and Limitations of System Privileges:** Unless you are a privileged user, the privileges provided to you [the User] are adequate to perform the normal functions associated with Online Learning Center^2 (OLC^2).
3. **Remote Access:** Primary access to Online Learning Center^2 (OLC^2) is from the DOE Network using Internet Explorer. Although OLC^2 can be accessed from personally owned or provided hardware and/or information systems that have an internet connection and a browser**,** never save OLC^2 information to personally owned or provided hardware and/or information systems.
4. **Disposal of Information**: Disposal of electronic and paper information shall be in accordance with federal and DOE policy and direction.
5. **Individual Accountability:** Never share your logon credentials, userID\password, with anyone. Never leave logged on workstations unattended. Workstations unattended for 30 minutes or more must be paused. Do not enter classified information or Sensitive Unclassified Information (SUI), including Personally Identifiable Information (PII), into the system. When access to these IT resources is no longer required, notify the OLC2 Help Desk and make no further attempt to access these resources.
6. **Limits on System Interconnection:** All system changes, regarding the interconnections/interfaces with other systems, are under the strict control and approval authority of the DOE Information System Owner and OPM System Owner and therefore must be coordinated and approved prior to implementation into the production system.
7. **Password Management:** If application passwords are used they must:
    a. Be between 8 and 20 characters;
    b. Contain a lower case letter, an upper case letter, a number (0…9), and a non alphanumeric special character;
    c. Be different from the previous 6 passwords;
    d. Be different from the E-Signature PIN;
    e. Recommended not to be stored in keyboard macros or .bat files, and

f. Recommended not to consist of user ID, personal data, or to be easily "guessed."

g. The password should not contain common words or proper names.

h. The password does not contain any simple pattern of letters and numbers.

i. The password employed by a user on unclassified systems is different form the password employed on classified systems.

j. Individuals must not leave clear-text passwords in a location accessible to others.

k. Individuals must not enable applications to retain passwords for subsequent reuse.

l. Passwords must be changed: at least every 6 months, as soon as possible after a password has been compromised, or after one suspects that a password was compromised, on direction from management.

8. **Information System Controls (with application logons):**

   a. The information system automatically locks after 3 consecutive invalid access attempts.

   b. The information system limits the number of concurrent sessions for any user to 1 session only.

   c. The information system automatically terminates a logon session after 20 minutes of inactivity.

9. **Security Training:** Every federal employee and contractor is required to take security awareness training upon employment and to take security refresher training annually.

10. **Reporting of IT Security Incidents:** Any unauthorized penetration attempt or unauthorized system use, or virus activity will be reported to your supervisor in accordance with DOE M 205.1-1 (IPWAR Manual). Users should also report the security incident to the DOE Enterprise Service Center at (301) 903-2500.

11. **Restoration of Service:** Restoration of service is in accordance with the MOU between DOE and OPM along with the OLC^2 vendor's Contingency Plan.

12. **Data Encryption:** Never copy or send SUI, including PII, to an external storage device or send it electronically without using a DOE approved method of encryption, such as Entrust.

13. **Consequences of Behavior Inconsistent with the Rules:** Failure to adhere to these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation and the judgment of the appropriate authority.