Attachment 1

Rules of Behavior (ROB)
For Privileged Users of Open World Leadership Center Database System

Authority

Pursuant to Open World Leadership Center (OWLC) Policy “Using the Internet, Computers and Electronic Communications Systems”, these Rules of Behavior set forth the supplementary duties and responsibilities of OWLC employees and contractors who have privileged access to the OWLC Database System.

Overview/Purpose

To manage and maintain the OWLC Database System, certain individuals are granted elevated privileges that exceed those of a typical Open World IT user. These Rules of Behavior explain the special obligations privileged users have to protect the confidentiality, integrity, and availability of the OWLC Database system and to ensure that the system is effectively managed and maintained.

Privileged Users and Accounts

Privileged users are users granted additional rights beyond those of a typical user. Privileged Accounts are IT system accounts utilized by privileged users to perform management and maintenance of the system.

System accounts and level of privileges vary dependent upon the role being fulfilled. Typical operating system level accounts are generically referred to as “administrator” or “root” level accounts. Other privileged users, such as account managers, may only have rights to create, delete, and change user accounts.

Coverage

These rules apply to all privileged users, both employees and contractors, who use the OWLC Database system. Annually, all privileged users are required to review and accept these rules and acknowledge that they understand what is expected of them.

Penalties for Non-Compliance

Compliance with these rules will be enforced through sanctions commensurate with the level of infraction. Actions may include, for example, verbal or written warnings, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation. As noted below, violation of these rule may also result in criminal sanctions under 18 U.S.C. § 1030.

Attachment 1

Rules of Behavior (ROB)
For Privileged Users of Open World Leadership Center Database System

As a privileged OWLC Database user, I agree that I will faithfully abide by the following rules:

1. I will manage and maintain the IT systems for which I have privileged access in accordance with applicable OWLC policy.

2. I have been granted privileged access to accounts on the OWLC Database system. I am the only individual who will access this account. I will not knowingly permit access by others without written approval.

3. I will use privileged accounts to access information solely and directly pertaining to the management and maintenance of the system that I am administering.

4. I will use a non-privileged account to log-in to any system for normal duties, unless performing technical support or to install authorized non-packaged software.

5. I am aware that running any computer system as an administrator makes the system extremely vulnerable and exposes it to security threats (e.g., malicious code).

6. I will not access the Internet for any reason while using my privileged account. This includes the downloading of files (including patches or updates), etc.

7. I will protect system information, including media and hard copy reports and documentation, in a manner commensurate with the sensitivity of the information.

8. I will ensure that I obtain authorization to install any non-standard software from Workstation Change Control (WCC) prior to installation.

9. I will not make any changes to the workstation configuration without prior authorization from WCC. This includes stopping and starting Operating System services while signed-in as an administrator.

10. I will not use any unauthorized system tools. I understand that the Information System Business Owner (ISBO) must grant permission to perform keystroke monitoring, utilize vulnerability scanners, or place packet capturing devices or analyzers on this system.

11. I understand that, when logged in as an administrator, I am required to use the “runas” command or its equivalent to install or execute software that requires administrative privileges, when possible.

12. I will immediately report any suspicious activities to the ISBO. My report will include the time, date and details of the event.

Attachment 1

Rules of Behavior (ROB)
For Privileged Users of Open World Leadership Center Database System

13. I understand that: Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of OWLC policy; may also be violation of 18 U.S.C. § 1030, may constitute theft, and is punishable by law. Failure to abide by these provisions may constitute grounds for termination of access privileges, disciplinary action, and/or civil or criminal prosecution. Misuse of assigned accounts and accessing others' accounts without authorization is not allowed. This system and resources are subject to monitoring and recording.

14. System. This user has been granted privileged access to the OWDB System.

As the Information System Business Owner, I approve privileged access for this user.

Name and Title of ISBO: Jane Sargus

Signature: ___________________________________ Date:

15. Privileged User. I accept these rules of behavior for privileged use of OWDB system.

Name of Contractor Employee: _________________________

Name of Contractor:___________________________________

Signature: ___________________________________ Date: