USDA United States Department of Agriculture

Classified Stand-Alone Computer User Agreement

I understand that as a classified computer system User, it is my responsibility to comply with all security measures necessary to protect classified information systems and classified information. I acknowledge that I have received the initial classified computer security awareness training and I understand that I am accountable for my actions while using a classified computer.

I further agree that I will:

- Use stand-alone classified computers for official government business only. I am aware that my actions will be monitored and that I will be held accountable for my actions on a classified computer. I understand that any misuse or inappropriate use will be investigated and prosecuted according to federal statute.
- Observe and follow the rules and regulations governing the secure operation and authorized use of the system.
- Access only the data, control information, software, hardware, and firmware that I am authorized access to and have a need-to-know, and I will assume only those roles and privileges for which I am authorized.
- Protect the user passwords at the highest level of classified information processed by the computer. I will report any compromise or suspected compromise of the password to the System Owner.
- Protect all files, media or documents containing classified data in accordance with DM 3440-001.
- Immediately report all security incidents and potential threats and vulnerabilities involving a classified stand-alone computer to the System Owner, ISSO, and PDSD.
- Participate in annual and refresher security awareness briefings and training.
- Protect classified computers and display monitors from unauthorized access or viewing.
- Ensure physical security procedures, access control procedures, and visitor access control procedures are followed.
- Ensure that access for cleared non-authorized users is approved by the System Owner before granting access to any directory, file, or data under user control.
- Ensure that system media and system output are properly classified, marked, controlled, stored, transported, and destroyed in accordance with procedures.
- Not introduce malicious code into a stand-alone computer or any of its components.

Classified Stand-Alone Computer User Agreement

- Not bypass, strain, or test security mechanisms without prior authorization from the System Owner or the ISSO. If security mechanisms must be bypassed for any reason, I will coordinate the procedure with the System Owner, and receive written permission from the ISSO for the procedure.
- Not install any hardware or software (including the importing or exporting of software) on classified stand-alone computers.
- Not relocate or change system equipment without proper authorization from the System Owner or ISSO.
- Not electronically transfer data from a classified system to a system approved to operate at a lower classification (unless I have been appointed as a Data Transfer Agent (DTA), and are properly trained and equipped to utilize the required tools and procedures.)
- Inform the System Owner when access to a particular computer is no longer required (e.g., completion of project, transfer, retirement, or resignation.)

1. Printed Name of User	**2. Signature of User**
3. Printed Name of System Owner	**4. Signature of System Owner**
5. Organization	**6. Date**
7. Printed Name of Security Official	**8. Signature of Security Official**