United States Department of Agriculture Marketing and Regulatory Programs Animal and Plant Health Inspection Service Grain Inspection, Packers and Stockyards Administration	**ACKNOWLEDGMENT OF EMPLOYEE RULES OF BEHAVIOR (ROB) FOR GOVERNMENT FURNISHED MOBILE DEVICES**

The mobile computing agreement is between the United States Department of Agriculture (USDA), (Animal and Plant Health Inspection Service (APHIS), Grain Inspection, Packers and Stockyards Administration (GIPSA), and its employees and non-employees (herein referred to as users) to approve the use of Government furnished mobile devices (e.g., smart phones, tablets, laptops, etc.) in the workplace.

USDA, APHIS, and GIPSA, hereby grant you access to utilize your Government furnished mobile device for authorized APHIS and GIPSA business. As a condition of the mobile computing approval, you are required to sign this agreement indicating that you will abide by the system security policies and protocols as set forth in this form and the documents referenced herein. Authority for compliance is through the APHIS Chief Information Security Officer (CISO).

Privacy Conditions:

Users are hereby informed that there is no right to privacy on Government furnished mobile devices.

With regard to the Government furnished mobile device, USDA reserves the right to perform the following actions:

- Install mobile management software (e.g., sandboxes, containers, Mobile Device Management (MDM) clients, etc.) and implement security controls required to protect Government applications and information by agency authorized Information Technology (IT) staff, either in person or OTA (over-the-air).
- Log, monitor, audit, and retain all device, application, and business information, including, but not limited to, files, databases, pictures, audio, video, and other media.
- Log, monitor, audit, and retain network traffic information generated by the mobile device.
- Monitor and report on Global Positioning System (GPS) location and any other sensor type of information collected through the mobile device.
- Respond to legitimate discovery requests for Government email, attachments, documents, and any other forms of information on the mobile device, arising out of administrative, civil, or criminal proceedings. In some cases, the device will be physically collected to retrieve data and be returned at a later date.

In addition, users will agree to the following conditions of use and behavioral standards:

- Comply with all USDA password policies for access to the mobile management software on their device, including use of strong passwords, password expiration, and password history. PINs (personal identification numbers) are not passwords.
- Keep the device current with security patches and updates, as released by the manufacturer and approved by USDA/APHIS and GIPSA, when prompted on the device.
- Not install software that allows users to bypass standard built-in security features and controls (e.g., jail break, root, or unlocking the device).
- Allow mobile management software (sandboxes, containers, MDM clients, etc.) to be installed on devices to segregate and protect USDA/APHIS and GIPSA applications and data, and not remove these management and security applications.
- Not install any nonUSDA, APHIS and/or GIPSA approved applications, or remove any required USDA, APHIS, and GIPSA applications without the APHIS CISO's advance approval.
- Not download or transfer sensitive, Personally Identifiable Information (PII), and/or Classified National Security Information from or to their Government furnished mobile devices, unless explicitly approved by the USDA/APHIS and GIPSA Chief Information Security Officers (CISO). Classified information is only allowed on authorized and properly secured Government Furnished Equipment (GFE) devices.
- Immediately notify the appropriate incident response group and their supervisor if devices are lost, stolen, damaged, or will be replaced, at which point USDA/APHIS and GIPSA will take steps to wipe or remove the mobile management software, including all applications (apps) and data.
- Notify local IT support staff one week prior to separation or termination of Government employment to allow for confirmation of removal of Government data from the mobile computing program.

Other Requirements:

- Access to USDA applications and data by any unauthorized persons other than yourself using your account is expressly prohibited.
- USDA/APHIS and GIPSA provided credentials are to be used solely in connection with the performance of your responsibilities as set forth in your official job duties with the USDA, APHIS, and GIPSA.
- The user is responsible and accountable for using USDA information and resources as outlined in the USDA Cyber Security policies the APHIS Electronic Mail Use, Security, and Privacy Policy.
- The acquisition and use of sensitive information can only be achieved within the sphere of the user's official duties and in accordance with these Rules of Behavior, the Annual Security Awareness Training and Rules of Behavior, and the Federal Privacy Act of 1974, 5 U.S.C. § 552a.
- All materials and information printed from your Government furnished mobile device that is considered sensitive Privacy Act Information must be secured at all times and destroyed via shredder when no longer in active use.
- Remote sessions to USDA information and resources will be terminated when not in use in accordance with APHIS, Federal Information Security Management Act (FISMA), and USDA requirements.
- Wireless transfer of USDA data and files to Government furnished devices will comply with Departmental/Agency wireless policy.
- Unauthorized or improper use of Government office equipment could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, criminal penalties, and/or employees being held financially liable for the cost of improper use.

Any questions about your responsibilities and accountability as a user of USDA information and resources should be discussed with your supervisor and/or Agency CISO.

Statement of Understanding:

It is your Agency's (APHIS or GIPSA) right to restrict or rescind computing privileges, or take other administrative or legal action due to failure to comply with the above referenced Rules of Behavior. Violation of these rules may be grounds for disciplinary action up to and including removal.

I affirm that the foregoing is true and correct in conformance with 28 U.S.C. 1746 (Declaration under Penalty of Perjury).

Printed Name:	Agency:
Signature:	Date: