DOI Information Security Rules of Behavior: For External Partners

Important Prerequisites for External Partner Access to GeoPlatform

1. The External Partner must create a **Login.gov** account at (https://secure.login.gov/sign_up/enter_email) and associate an approved **authentication method** to the Login.gov account.

2. The External Partner must create a **GeoPlatform Login.gov** account at (https://geoplatform.maps.arcgis.com/home/index.html) and complete the email verification step. This ensures a first-time log in to GeoPlatform AGOL, as well as BLM visibility of the account for purposes of role modification to BLM Partner Data Editor and visibility for group membership.

3. T*he External Partner must sign and return the Information Security Rules of Behavior User Agreement below to their BLM contact.*

Please reference the *BLM GeoPlatform SOP* (section titled Creating a GeoPlatform Account) or the *GeoPlatform Account Setup: External Partner* for additional information on account setup.

User Instructions: Retain for Future Reference

Violations of the following rules are considered information security incidents. According to the Department of the Interior Manual 375 DM 19, "all suspected, actual, or threatened incidents involving the destruction, physical abuse or loss of technological resources shall be reported to the appropriate authorities." All information system users shall report observed security incidents to their supervisors and to the BLM Field Office Information Technology Security Manager (ITSM). The BLM Field Office ITSM may recommend the removal of any individuals' access (to include User ID and password) from any BLM Information System and/or automated information resources system in the event of a security incident.

Personally Identifiable Information (PII) is defined in OMB 06-16 and OMB 06-19 as: "...information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual." The loss of PII data is considered an Information Security Incident. Note that this loss may occur as a result of a 'physical loss' (e.g., losing a laptop) or a 'logical loss' (e.g., being hacked).

Information Security Rules of Behavior:

1. No classified National Security Information will be entered into any agency Information System.

2. Data collected on behalf of the BLM are considered to be the property of the U.S. Government. BLM Information Systems are provided to be used for official Government business. No personal software, private data, unlicensed proprietary software, or otherwise non-governmental information will be used on, entered into, or stored on any Government-owned Information System or equipment.

3. Commercially developed and licensed software shall be treated as proprietary property of its developer. Title 17 of the U.S. Code states that, "It is illegal to make or distribute copies of copyrighted material without authorization." The only exception is the user's right to make a backup for archival purposes, assuming one is not provided by the manufacturer. It is illegal to make copies of software for any other purpose without the permission of the publisher. Unauthorized duplication of software is a Federal crime. Penalties include fines of up to $100,000 per infringement and jail terms of up to 5 years.

4. Individual User IDs and passwords are assigned to each person having a valid requirement to access any BLM information system and local/wide area networks. All activities accomplished under this User ID are directly attributable to the user to whom it is assigned. It is, therefore, to be used only by the individual user. Remember, each person is responsible for all activities logged under the User ID that has been assigned to them.

5. Do not attempt to access any data contained on agency Information Systems for which the user ID does not have authority to access or the user do not have a specific need-to-know. If the need to access an Information System has been established through the appropriate supervisory channel, the request to grant access shall be made by the System Owner or other designated individual.

6. Usernames, passwords or PIN numbers are not to be shared with or disclosed to anyone. If a user believes that their Username and password have been compromised, the password must immediately be changed and the BLM Field Office ITSM must be notified. Passwords should be changed at required intervals or any time a user feels the possibility exists that it may have been compromised.

7. Never use personal information (e.g. telephone numbers, names of family members, pets, etc.) as passwords. Passwords must comply with all current agency password policies.

8. Usernames, passwords or PIN numbers are not to be written down. Any required documentation of usernames, passwords or PIN numbers shall be secured in a sealed envelope and locked in a safe. Under no circumstances should User IDs and passwords be posted ANYWHERE!

9. Users must physically protect all hardware or software based tokens entrusted to them for authentication or encryption purposes. (A token is usually a physical device that an authorized user is given to provide additional higher level security and to verify the user is who they say they are when logging into the network.)

10. Users should consult with their BLM Field Office ITSM for standards and approved methods for encrypting and deleting data. Users must comply with all current data encryption policies and practices as defined by agency policy.

11. Users must ensure that all agency data downloaded using remote access is erased when it is no longer needed.

Information Security Rules of Behavior

User Agreement

This step is required for you to complete the registration process of your GeoPlatform account. Once you have read the entirety of the **DOI Information Security Rules of Behavior: For External Partners**, please sign below and email a signed copy to your BLM point of contact to confirm that you have read and understand the DOI Information Security Rules of Behavior: For External Partners.

I,_____have read and acknowledge the "**DOI Information Security Rules of Behavior: For External Partners**" and agree to adhere to all statements and policies throughout the duration that I have access to any and all Bureau of Land Management devices, software, and/or non-public data or information.

_____ _____

Signature Date

_____

Agency/Company