GeoPlatform Rules of Behavior and Access Policy

The GeoPlatform is a U.S. Government information system[1] managed by the Federal Geographic Data Committee (FGDC). As a GeoPlatform user, I understand that I am personally responsible for my use and any misuse of my user account and must comply with these *Rules of Behavior* (ROB). I understand that by accessing a U.S. Government information system that I must comply with the following requirements:

1. Users must safeguard the information to which they have access at all times.

2. Any activity that violates Federal laws for information protection (e.g., hacking, phishing, spamming, etc) is prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

3. GeoPlatform user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism should never be shared or stored any place easily accessible.

4. I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 10 years in jail for the first offense for anyone who commits any of the following violations:

    a. Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure;

    b. Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system;

    c. Accesses a government information system without authorization, and alters, damages, or destroys information therein; and

    d. Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

5. Posting material or information that is unlawful, such as obscene materials, inappropriate content, or language on this site is prohibited. Users will be held responsible for any information posted and published to this website by them or by anyone using their access privilege that is in violation of this policy. Users are responsible for ensuring that any information or content posted/published is appropriate for the intended recipient(s).

6. Any fraudulent activities, including illegally using someone else's account to access GeoPlatform, post system messages, or email customers for personal gain or concerns, are prohibited.

[1] National Institute of Standards and Technology (NIST) Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, defines an “information system” as: “A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.”

7. Users may not use this website to breach the security of any system user or to gain access to another person's (internal or external) computer, software, or data.

8. Using tools to compromise system security of this website, such as password-guessing programs, cracking or packet sniffing tools, or any network probing tools, is strictly prohibited, and, the government may take legal action against you.

9. Any attempt to disrupt or deny operation of this website is strictly prohibited.

10. The user is responsible for assuring all transmissions to this site are free of viruses and other malware.

11. The user understands that the government cannot claim copyright of data that is in the public domain or has been released as open data.

12. Users must immediately notify the GeoPlatform Service Desk of any unauthorized use of your account or any other breach of security regarding these polices. The GeoPlatform Service Desk will investigate any and all suspected violations of these policies and reserves the right to take corrective or legal action against the violator. If an investigation is warranted, the GeoPlatform Service Desk may disable the user's account. As a system user, you are responsible for ensuring that your use of the system complies with the policies stated therein. Any system user who does not agree to be bound by these polices should immediately discontinue the use of this system and should notify the GeoPlatform Service Desk at servicedesk@geoplatform.gov to remove their account.

GeoPlatform Rules of Behavior for Privileged User Accounts

In addition to the Rules of Behavior stated above, users requesting elevated privileges must comply with the rules outlined below. These additional rules of behavior provides common rules on the appropriate use of all GeoPlatform information technology resources for all Privileged Users[2], including federal employees, interns, and contractors. Privileged User account roles have elevated privileges above those in place for general user accounts regardless of account scope (e.g., Community management, local, and domain administrator accounts). Potential compromise of Privileged User accounts carries a risk of substantial damage and therefore Privileged User accounts require additional safeguards.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively implement their own system-specific rules.

These rules apply to local, network, and remote use[3] of GeoPlatform information (in both electronic and physical forms) and information systems by any individual.

The PROB cannot account for every possible situation. Therefore, where the PROB does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.[4]

All users of Privileged User accounts for GeoPlatform information technology resources must read these standards and sign the accompanying acknowledgement form before accessing GeoPlatform data/information, systems, and/or networks in a privileged role.

I assert my understanding that:

- Use of GeoPlatform information and systems must comply with the Department of the Interior policies, standards, and applicable laws;
- Unauthorized access to information or information systems is prohibited; and
- Users must prevent unauthorized modification of information.

General Security Practices

I must:

- Accept that I will be held accountable for my actions while accessing and using GeoPlatform information and information systems.

---

[2] Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, privileged roles include, for example, key management, network and system administration, database administration, and Web administration.

[3] Refer to the glossary of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations for definitions of local, network, and remote access.

[4] U.S. Department of Interior Ethics Guide, available at http://www.doi.gov/ethics/index.cfm.

- Ensure that I have appropriate authorization to install and use software, including downloaded software on GeoPlatform systems and that before doing so I will ensure that all such software is properly licensed, approved, and free of malicious code.
- Use assigned unique identification and authentication mechanisms, including PIV cards, to access GeoPlatform systems and facilities.
- Permit only authorized GeoPlatform users to use GeoPlatform equipment and/or software.
- Take all necessary precautions to protect GeoPlatform information assets (including but not limited to hardware, software, personally identifiable information (PII) and federal records [media neutral]) from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and treat such assets in accordance with any information handling policies.
- Immediately report to the appropriate incident response organization or help desk all lost or stolen GeoPlatform equipment; known or suspected security incidents; known or suspected information security policy violations or compromises; or suspicious activity in accordance with Department of Interior procedures.
- Only use approved methods for accessing GeoPlatform information and GeoPlatform information systems.

Privacy

- Understand and consent to having no expectation of privacy while accessing GeoPlatform computers, networks, or e-mail.
- Collect information from members of the public only as required by my assigned duties and permitted by the Privacy Act of 1974, the Paperwork Reduction Act, and other relevant laws.
- Release information to members of the public including individuals or the media only as allowed by the scope of my duties and the law.
- Refrain from accessing information about individuals unless specifically authorized and required as part of my assigned duties.
- Use PII only for the purposes for which it was collected and consistent with conditions set forth by stated privacy notices such as those provided to individuals at the point of data collection and published System of Records Notices.

I understand that as a Privileged User, I must:

- Protect all Privileged User account passwords/passcodes/Personal Identity Verification (PIV) personal identified numbers (PINs).
- Comply with all system/network administrator responsibilities in accordance with GeoPlatform policy.
- Use my Privileged User account(s) for official administrative actions only.
- Notify system owners immediately when privileged access is no longer required.
- Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a Privileged User, I must **NOT**:

- Share Privileged User account(s) or password(s)/passcode(s)/PIV PINs.
- Install, modify, or remove any system hardware or software without system owner written approval.
- Remove or destroy system audit, security, event, or any other log data.
- Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls.
- Introduce unauthorized code, Trojan horse programs, malicious code, or viruses into GeoPlatform information systems or networks.
- Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses.
- Use Privileged User account(s) for day-to-day communications.
- Elevate the privileges of any user without prior approval from the *System Owner* (GeoPlatform system accounts) or *Federal Sponsor* (community accounts).
- Use privileged access to circumvent GeoPlatform policies or security controls
- Use a Privileged User account for Web access except in support of administrative related activities or modify security settings on system hardware or software without the approval of a system administrator and/or a system owner.
- Violate, direct, or encourage others to violate GeoPlatform policies or procedures.
- Circumvent security safeguards, including violating security policies or procedures or reconfiguring systems, except as authorized.
- Use another person's account, identity, password/passcode/PIN, or PIV card or share my password/passcode/PIN.
- Use GeoPlatform information, systems, and hardware to send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums.
- Exceed authorized access to information.
- Share or disclose information except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transmit, e-mail, remotely access, or download information unless such action is explicitly permitted by the manager or owner of such information.
- Use information for anything other than the purpose for which it has been authorized;
- Access information for unauthorized purposes.
- Use GeoPlatform data for private gain or to misrepresent myself or GeoPlatform or for any other unauthorized purpose.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information.
- Copy or distribute intellectual property including music, software, documentation, and other copyrighted materials without written permission or license from the copyright owner.

I must **REFRAIN** from the following activities when using GeoPlatform:

- Unethical or illegal conduct.
- Sending or posting obscene or offensive material.
- Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages.
- Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act[5].
- Conducting any commercial or for-profit activity.
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material.
- Creating and/or operating unapproved Web sites or services.
- Allowing personal use of GeoPlatform resources to adversely affect. GeoPlatform systems, services, and co-workers (such as using non-trivial amounts of storage space or bandwidth for personal digital photos, music, or video).
- Posting Department information to external newsgroups, social media and/other types of third-party website applications, or other public forums without authority, including information which is at odds with departmental missions or positions. This includes any use that could create the perception that the communication was made in my official capacity with the federal government, unless I have previously obtained appropriate Department approval.

All system users of GeoPlatform must follow the rules outlined in this document. Any abuse of these policies are punishable by law. Direct any questions regarding complaints and violations of this policy to the GeoPlatform Service Desk at servicedesk@geoplatform.gov for appropriate handling and resolution.

The GeoPlatform Service Desk supports and enforces the established policies set forth in this ROB to protect GeoPlatform website system users from the adverse impact that can result from violations of the ROB. If you believe you are the victim of activities that are in violation of this ROB, the GeoPlatform Service Desk will take appropriate action to investigate and attempt to resolve the alleged violation. To report a concern or incident, send an email to the GeoPlatform Service Desk at servicedesk@geoplatform.gov and include your name, telephone, email address, the date and time of the incident, log files (if appropriate), examples, and any other information that may be useful to the investigation and verification of the incident.

The GeoPlatform Service Desk reserves the right to disable your account access without notice for violation of these polices.

[5] For additional guidance refer to https://osc.gov/Services/Pages/HatchAct-Federal.aspx and 5 C.F.R. Part 2635: Standards of ethical conduct for employees of the executive branch.

Penalty

Unauthorized use of GEOPLATFORM by a user violates Federal law and could leave the user vulnerable to criminal action and/or financial liability. Anyone using GEOPLATFORM expressly consents to monitoring, and violators shall be reported to the proper authorities.

SIGNATURE PAGE

I have read the *GeoPlatform Rules of Behavior and Access Policy* and the *GeoPlatform Rules of Behavior for Privileged User Accounts* and understand and agree to comply with its provisions. I understand that violations of these rules or information security policies and standards may lead to disciplinary action and that these actions may include removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the *Rules of Behavior* must be authorized in advance in writing by the System Owner or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the *Rules of Behavior* draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name (*Print*): _____

User's Signature: _____

Date Signed: _____