General Usage

This Information Systems Acceptable Use Agreement ("Agreement") establishes a minimum set of rules of behavior for _____ **("Subcontractor")** while using or connecting to ICF's Information Technology resources ("IT resources") for services in support of _____ **("Client")**. IT resources include, but are not limited to: computers, networks, servers, mobile computing devices (e.g., laptops, smartphones), and other systems that maintain company or client data.

Subcontractor Employees ("Users") of IT resources who violate these rules of behavior may be subject to removal from network access and company disciplinary action at the discretion of appropriate management. Additionally, ICF system administrators or ICF cybersecurity personnel may remove or disable User's access in the event of a violation of the agreement. ICF reserves the right to monitor relevant activity and data on the network within legal boundaries.

Users are responsible for understanding and adhering to the full contents of the Acceptable Use Agreement and any applicable ICF security policies and information safeguarding.

Passwords and User IDs

Passwords for all IT resources are considered private and confidential. Users are prohibited from sharing any of their system passwords. If the User has any reason to question any aspect of the manner in which there is a request for credentials, User should request to speak with the ICF Program Manager or the ICF's Information Technology department.

To minimize the risk of compromising systems as a result of poor password selection and system safeguarding, Users are responsible for aligning with the following standards.

- Adhere to length and character requirements in accordance with each respective system.
- Password must be reset at least every 90 days.
- Do not share password.
- Avoid the reuse of previous passwords.
- Avoid using dictionary words, derivatives of User IDs, and common character sequences such as "123456", abc123, etc.
- Never allow another person to use or share your logon session. Be sure to logout of your application before allowing someone else to use your system.
- If User's password is exposed or compromised, User must change it immediately.
- User and ID passwords must not be physically written down and stored.
- User must lock workstation or log off any active sessions when leaving the workstation to prevent unauthorized use of account.

Data Confidentiality and Security

All data on the information system(s) is classified as Confidential Information, unless otherwise specified. Confidential Information is not considered available for public use unless specifically

authorized by ICF. If User is exposed to any sensitive information that is suspected to not be associated with User's specific duties, User must notify ICF Program Manager or the ICF Information Technology department immediately.

Unauthorized Access

Users are forbidden from taking actions that are intended to breach or may result in a breach of any ICF or individuals security, confidentiality, or privacy of information assets. These actions include, but are not limited to:

- Accessing the system from outside the United States unless authorized in writing by the ICF Information Technology and ICF Subcontracts Administrator.
- Accessing data using someone else's ID and password.
- Taking actions meant to capture information to which the User is not authorized, such as network sniffing, network mapping, port scanning or vulnerability scanning.
- Circumventing any authentication or security mechanism.
- Interfering with or denying service to any authorized use or process.
- Using tools or software to force or compromise access.
- Using unauthorized scripts to conduct work functions.

Computer Security Incidents

All computer security incidents or suspicious activity (viruses, intrusion attempts, system compromises, offensive emails, inadequate protection of sensitive data, data exposure, etc.) or if the system is lost or stolen must be reported to the ICF Subcontracts Administrator, and the ICF Information Technology department as soon as the incident or activity is discovered.

By signing below, I acknowledge that I have received and read the Agreement. I further understand that I must comply with this agreement to the best of my capabilities.

User Signature:_____

User First and Last Name:_____

Date:_____