Argonne National Laboratory Computer User Agreement

Introduction. As a condition of employment for or collaboration with Argonne National Laboratory (Argonne), you may have access to various Argonne IT Assets such as computer systems, networks, applications, data, email, and documents. Before this access is granted, you must agree to abide by usage and access policies and to use Argonne IT resources in a responsible and ethical manner, as described below. Please read this information carefully. Sign/click at the bottom to indicate your understanding of these conditions and your agreement to abide by them.

Your Responsibilities as a Computer User.
The following principles govern the use of Argonne IT assets, the details of which are described in Argonne's Cyber Security Program Plan (CSPP). You are expected to abide by these principles and the policies set forth in the CSPP.

- You are responsible for the proper use of the tools each computer system provides and for confidentiality of information entrusted to you.

- Your computer accounts are assigned to you alone and must not be shared with anyone, including coworkers, trainers, or computer support staff. You must protect your passwords, choose complex passwords and change them regularly in accordance with Argonne policies.

- You must not use Argonne IT resources for illegal or malicious purposes, such as harassment of others, disruption or unauthorized monitoring of electronic communications or unauthorized copying of copyrighted materials.

- You must refrain from unethical usage, including: unauthorized use of computer accounts and resources assigned to others, use of computing facilities for private business or political purposes or private gain, academic or scientific dishonesty, or violation of software licenses.

- You will respect the confidentiality and privacy of individuals to whose records you may have access in accordance with the Laboratory policy, ethical standards, and state and federal laws.

- You will be expected to read, understand, and comply with (as appropriate) any requests relating to cyber or information security.

- You should report to the cyber security program office or your local cyber security program representative any breach of security, policy violation, or suspicious activity.

- You should be aware that any or all computer and network systems and files on these systems may be monitored by appropriate authorities.

Violators of these standards may be subject to disciplinary action up to and including dismissal

ALCF Security Information/Training/Reminders:

- SSH access requires a cryptocard or SSH keys
- No group accounts allowed
- No sharing of accounts or cryptocards
- You agree to follow ANL Cybersecurity policies
- Your computer sessions will time-out after extended periods of inactivity
- You will keep your remote system secured and free of viruses, malware, spyware.
- You agree to run an automatic screen saver to protect your session after 15 minutes of inactivity.
- You will report suspicious activity or security breaches (including your remote system) to support@alcf.anl.gov

I understand and agree to abide by the conditions outlined above.