Argonne NATIONAL LABORATORY

Argonne National Laboratory Information Technology Access 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 General 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.
- Your general access Argonne IT account is provided to you with the least level of user privileges required to carry out your day-to-day assigned responsibilities.
- If supplied an Argonne desktop and/or laptop computer, you will be given system administrator rights to these computers only if you have a documented need. If you are given such rights, you must log on as system administrator only when you are carrying out system administrator functions.
- 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 acknowledge that any or all activity on Argonne IT assets may be monitored and that you have no expectation of privacy when using Argonne IT Assets.
- Your use of and access to Argonne IT Assets by any means is governed by Argonne's policies and procedures, all of which are hereby incorporated herein by reference.

Personally Owned Devices.
The following additional principles apply if personally owned computing devices (e.g. desktop, laptop, mobile or other devices) are used by employees and contractors to access Argonne IT assets.

- You will follow Argonne policy for the protection of laboratory sensitive information to protect the confidentiality of information entrusted to you.
- You will protect login access to the device by configuring PIN/password or equivalent and login timeout.
- You will keep current with operating system and application security patches.
- You will immediately notify the Laboratory Cyber Security Program Office if the device is lost, stolen or compromised to assess the impact of the data disclosure and apply the appropriate mitigations as determined by the Laboratory.
- You will ensure all Argonne data is removed before disposing of any device, upon termination of your Argonne employment or as requested by the laboratory to ensure compliance with Argonne, DOE, legal or regulatory requirements, policies or procedures.

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

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

_____
Signature

_____
Printed name
Date _____ Badge number(if applicable) _____

Non-Exhaustive List of Applicable Policies and Laws

Argonne Cyber Security Program Plan
LMS-PROC-18: Managing Employee Computer Accounts
LMS-PROC-22: Safeguarding Protected Personally Identifiable Information
Digital Millennium Copyright Act of 1998
Computer Fraud and Abuse Act of 1986
National Information Infrastructure Protection Act of 1996