Argonne National Laboratory Information Technology Access Agreement

Introduction

As a condition of receiving access to Argonne National Laboratory (Argonne or Laboratory) information technology (IT) resources, such as computer systems, storage devices, cloud services, networks, applications, data, email, and documents, 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. Read this information carefully. Sign/click at the bottom to indicate you understand and agree to abide by these conditions.

Your General Responsibilities as a Computer User

As part of your relationship with Argonne, you may be assigned government furnished equipment (GFE). The assigned device will be your primary device. Devices provided by other entities, including personally-owned devices, are for supplemental use only, and accessing Argonne IT resources with them comes with some restrictions, as stated in this agreement.

In the event that you separate from your relationship with Argonne, Argonne requires that you return assigned items on or before the final date of your relationship. Contact your division property representative or manager to arrange the transfer of these resources.

The following principles govern the use of Argonne IT resources, many of which are described in detail in separate Argonne policies and procedures. You are expected to abide by the principles and applicable policies cited in the paragraphs below and at the end of this document.

- You are responsible for the proper use of the tools each computer system provides and for confidentiality of information entrusted to you.
- Use your *anl.gov* email address for all Laboratory business if you have been provided with one.
- Argonne prohibits employees from using alternative email accounts when conducting Laboratory business.
- You must use approved methods and applications to access information related to Laboratory business, in accordance with LMS-POL-47, *Information Technology Access Agreement*. Also see LMS-PROC-22, *Protection of Controlled Unclassified Information.* You acknowledge that any or all activity on Argonne IT resources may be monitored, and that you have no expectation of privacy when using Argonne IT resources. See LMS-POL-47.
- You must not use tools or services, such as tunneling, third-party VPN providers, or relays, which have not been approved by the CSPO, which obfuscate actions or otherwise impair or impede cybersecurity controls implemented by Argonne.
- You must only conduct Laboratory business or process and store information related to Laboratory business on cloud services approved by the Cyber Security Program office (CSPO). See the BIS webpage Approved Cloud Applications. Applications that are not listed, such as Google Drive, Google Docs, and Dropbox, must not be used.
- Devices used to conduct Argonne business, including those provided by other entities and personally-owned devices, are subject to review by authorized Argonne personnel for any Argonne information that may be connected to a review, investigation, or litigation. Extraction of Argonne information from these devices may also be required. See LMS-PROC-20, *Legal Hold.*
- Your access to Argonne systems may be limited from certain countries. You will coordinate with the designated Argonne Information Assurance Representative if you plan to access Argonne IT resources from other countries. See LMS-PROC-108, *Remote Work Arrangements,* and LMS-PROC-244, *Use of Mobile Devices Off-site*, as applicable.
- Your login accounts are assigned to you alone. Passwords must not be shared with anyone, such as coworkers, trainers, or computer support staff.
- You must protect your passwords and multi-factor authentication, and change your passwords when notified to do so.
- You may only be given system administrator rights to Argonne IT resources if you have a documented need as required by LMS-PROC-18, *Managing Employee Computer Accounts and Information Access*. If you are given such rights, you must log on as system administrator only when you are carrying out system administrator functions.
- The use of Argonne IT resources for malicious, unethical, or illegal purposes is strictly prohibited. Such behavior includes, but is not limited to the following:
  - harassing others
  - disrupting or monitoring electronic communications or using or copying copyrighted materials without authorization
  - using login accounts or resources assigned to others without permission
  - conducting private business, political activities, or activities for private gain
  - engaging in research misconduct, or violating software licenses

  In addition, you must respect the confidentiality and privacy of individuals whose records you may have access to, according to Argonne's policies and procedures, ethical standards, and state and federal laws. See LMS-POL-51, *Employee Conduct*.
- You should report any breach of security, policy violation, or suspicious activity to the CSPO or your local cybersecurity program representative.

- Your use of and access to Argonne IT resources by any means is governed by Argonne's policies and procedures, all of which are hereby incorporated herein by reference. Employees may make occasional personal use of Argonne IT resources as defined in LMS-POL-44, *Limited Personal Use of Argonne Resources.*

Devices Owned by Other Entities, Including Personally-Owned Devices

If you choose to access Argonne IT resources from a personally-owned device, such as your desktop, laptop, tablet, or mobile phone, you agree to adhere to the following requirements, in addition to those above:

- You will follow Argonne policy for the protection of Laboratory information and to protect the confidentiality of information entrusted to you. This includes not using prohibited products in conjunction with any Argonne-related work. See list of Prohibited Products.
- Argonne may restrict or disallow access to certain IT resources, as well as limit functionality on devices owned by other entities, including personally-owned devices.
- You will install and utilize Argonne-selected software to enforce device compliance with Argonne policy.
- Any device owned by other entities, including personally-owned devices, and any personal or third-party cloud services used for conducting Argonne business must be made available to authorized Argonne personnel for review and/or extraction of any Argonne information connected to a review, investigation, or litigation. See LMS-PROC-20, *Legal Hold.*
- Special rules apply to accessing Argonne systems from other countries with devices owned by other entities, including personally-owned devices. You may not use such devices to access Argonne systems from countries of concern. See LMS-PROC-244, *Use of Mobile Devices Off-site*.
- You will immediately notify the CSPO if a device used to access Argonne IT resources is lost, stolen, or compromised, and cooperate with CSPO to assess the impact of the data disclosure and apply the appropriate mitigations as determined by Argonne.
- You will ensure all Argonne data is removed before disposing of any device, upon termination of your Argonne relationship, or as requested by the Laboratory to ensure compliance with Argonne, DOE, legal or regulatory requirements, policies or procedures.

Failure to abide by these standards may result in administrative and disciplinary action and civil and criminal penalties.

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

_____

Signature

_____

Printed name

Date _____ **Badge number** _____

Non-Exhaustive List of Applicable Policies and Procedures

This document incorporates requirements from the following list of Argonne policies and procedures.

- Argonne Cyber Security Program Plan (CSPP)
- LMS-MNL-18, *Property Management*
- LMS-MNL-25, *IT Asset Management*
- LMS-POL-44, *Limited Personal Use of Argonne Resources*
- LMS-POL-47, *Information Technology Access Agreement*
- LMS-POL-51, *Employee Conduct*
- LMS-PROC-18, *Managing Laboratory Computer Accounts and Information Access*
- LMS-PROC-20, *Legal Hold*
- LMS-PROC-22, *Protection of Controlled Unclassified Information*
- LMS-PROC-44, *New Worker Orientation*
- LMS-PROC-108, *Remote Work Arrangements*
- LMS-PROC-244, *Use of Mobile Devices Off-Site*