



Ames National Laboratory Information Technology (IT) Network Rules of Behavior

SUBJECT: Ames National Laboratory Information Technology (IT) Rules of Behavior for Computer Network Users of IT Systems and Resources that Access, Store, Receive, or Transmit Information

1. **Purpose.** This document sets forth the Ames National Laboratory's policy on IT Network Rules of Behavior. The IT Network Rules of Behavior implements the Federal policies and Department of Energy (DOE) directives provided within this document.
2. **Cancellation.** This policy cancels and supersedes revision 9.0 of the Network Rules of Behavior (Form 48400.019), dated 03-12-2024.
3. **Explanation of Change.**
 - a. Updated document to conform with DOE O 205.1D and DOE O 206.1A.
 - b. Added rules regarding Artificial Intelligence
 - c. Edited and updated all rules to reflect current user behavior requirements per DOE O 203.1A.
4. **Objectives.** To inform users of Ames Laboratory IT resources and applications regarding their responsibilities and expected standards of conduct for accessing laboratory information systems, networks, and data. This applies to government-furnished equipment (GFE) and resources, as well as university-owned equipment connected to the Ames Laboratory network, except where otherwise indicated in Section 8 of this document.
5. **Applicability.** This policy is applicable to all standard (non-privileged) users, including employees, contractors, visiting researchers, students, affiliates, and collaborators, using laboratory IT resources. The Ames Laboratory IT Network Rules of Behavior governs users at their primary of work, during teleworking, in any alternative workplace, and while traveling.
6. **Roles and Responsibilities.**
 - a. Supervisors are responsible for ensuring compliance with this order for their employees who access Ames Laboratory IT resources and applications.
 - b. All users are required to formally acknowledge these rules prior to their first use of any Ames Laboratory IT resource, and annually thereafter.
7. **Penalties for Non-Compliance.** Users are responsible for their conduct on the network. Failure to adhere to the Ames Laboratory IT Network Rules of Behavior may result in revocation of system access and/or disciplinary measures. Consequences may include verbal or written warnings, temporary suspension of system access, reassignment of duties, or termination of employment, depending on the nature and severity of the infraction.

IT Network Rules of Behavior. As an individual subject to this policy, I acknowledge and agree to adhere to the established rules of behavior:

Category	Rules of Behavior
Artificial Intelligence (AI)	1) Usage Authorization: Do not use generative AI unless explicitly authorized, as per AMES Use of AI and Generative AI Services Policy and DOE AI Compliance Plan. ▪ Do not input CUI, export-controlled, proprietary, or PII into unapproved AI tools ▪ Follow DOE and Ames Laboratory data protection policies ▪ Ensure sensitive data is only input to tools that have been approved and cleared for sensitive data. 2) Data Guidelines: Only use approved generalized, non-identifying, non-sensitive work data with online providers of generative AI found in KB0017082: Getting Started with Generative AI and KB0017254: Reference guide for approved AI-enabled tools and enterprise platforms.
Personal Use	1) Minimization: IT resources shall only be used for authorized government or laboratory purposes, with only limited personal use permitted as defined in DOE Order 203.1A Chg. 1, Limited Personal Use of Government Office Equipment Including Information Technology. 2) Prohibited Activities: Limited personal use of IT resources may be allowed provided that it: ▪ Does not interfere with DOE or Ames Laboratory's mission and operational responsibilities. ▪ Does not consume excessive resources or degrade system performance. ▪ Does not violate law, DOE policy, or laboratory standards. ▪ Does not involve inappropriate, offensive, or unlawful content. ▪ Is not used for financial gain, commercial purposes, profit-making activities, or lobbying.
Privacy	1) Monitoring: Pursuant with Clause I.99 of Ames National Laboratory Prime Contract (DEAR 952.204-77): Users acknowledge that: ▪ There is no expectation of privacy at any time when using or accessing government and laboratory resources (i.e., GFEs, networks, email). ▪ All activity is subject to monitoring, logging, inspected, and disclosed for security, legal, or administrative purposes. ▪ Use of government and laboratory systems and services constitutes consent to such monitoring there is no expectation of privacy while using government resources at any time. <i>Employees who wish for their personal activities to be private should not conduct such activities using authorized government resources.</i> 2) Data Protection: Encryption, access controls, data extracts, and physical security measures must be used to protect Personally Identifiable Information (PII), export controlled, patentable, proprietary and other Controlled Unclassified Information (CUI) from unauthorized disclosure, as described in Ames National Laboratory policies, DOE Order 206.1A Privacy Program and DOE Order 471.7 Controlled Unclassified information

Category	Rules of Behavior
Access	1) Password Safety: All computing devices connected to the network must be configured to comply with Ames Laboratory password policies. 2) Workstation Security: Lock your Ames Laboratory workstation (CTRL-AT-DELETE) and remove your authentication tokens (e.g., PIV card) at the end of the workday or when leaving your shared workspace. 3) Regular Restarts: Restart your Ames workstation weekly, or sooner if requested by Ames IT to help protect against malicious apps, phishing, and other attacks. 4) Re-authentication: Users authenticated to the Ames network daily in the performance of laboratory work.
Teleworking / Remote Access	<i>These additional rules apply to Ames Laboratory employees approved for teleworking at any alternative workplace:</i> 1) Security: Follow security practices at alternative workplaces that are the same as or equivalent to those required at primary workplace. 2) Physical Protection: Physically protect GFEs (laptops, mobile devices, desktops, storage devices) used for teleworking against loss, theft, damage, abuse, and unauthorized use, as described in Policy 48300.001, Program Management. 3) Data Protection: Protect all laboratory data at the alternative workplace. 4) Approved Methods: Use approved methods (e.g., Multi-Factor Authentication (MFA), Cisco AnyConnect, Virtual Private Network (VPN)) to remotely access the network, as described in Remote Work Resources.
Hardware & Software	1) Licensing and Intellectual Property: It is essential to comply with all software copyright laws. Users must not obtain, install, copy, or use any unlicensed software. The following principles apply: Abide by software copyright laws; do not obtain, install, replicate, or use unlicensed software. ▪ Do not copy or distribute any protected intellectual property – such as music, software, documentation, or other copyrighted materials – without proper permission or a license from the copyright owner. ▪ Only use software that has licensed and authorized by Ames Laboratory. ▪ Refer to KB0016456: Unauthorized Software List By Category, which details software applications that are not authorized or require approval before installation or use. 2) Obtaining Software: All licensed software must be obtained through the official procurement process unless specifically directed otherwise. Downloading untrusted software is strictly prohibited. 3) Prohibited Tools: Do not use tools or engage in activities designed to defeat software protection, discover passwords, identify security vulnerabilities, or decrypt files. 4) Patching and Rebooting: Promptly respond to any requests from Ames IT personnel regarding patching and rebooting of systems.

Category	Rules of Behavior
Government Furnished Equipment (GFE)	Resource Protection: It is your responsibility to protect Ames Laboratory IT resources in your possession from theft, destruction, or misuse. Specific guidelines include: - Safeguard all Ames Laboratory IT resources entrusted to you. - Ensure all laptops, mobile devices, and external storage devices used to store Ames Laboratory data are protected with FIPS compliant protection. International Travel: Request and use an Ames Laboratory loaner laptop when working internationally. Secure Usage: Turn off unused communications capabilities (e.g., cellular, Bluetooth, Wi-Fi) when not in use or when traveling. Ames Laboratory data shall only be stored on AMES approved and issued devices (i.e., laptops, desktops, external drives, USB drives, etc.)
Use Your Own Device / B.Y.O.D.	<i>When a personally owned device is approved for conducting official business, the following rules apply:</i> Sensitive Data: The download or storage of laboratory information – including research data, PII, CUI – on personal IT resources (e.g., laptops, mobile devices, home computers, removable media, personal email, or cloud storage) is strictly prohibited. Updates and Security: Operating system (OS) patches and antivirus (AV) software must be currently supported updated. For details on supported versions, refer to KB00015607: OS Support Lifecycle - Current, Supported, & EOL Connection Restrictions: Personal devices may only connect to laboratory systems with explicit authorization. Monitoring & Privacy: Ames Laboratory may perform security posture checks (e.g., OS version, encryption), access logs and authentication may be monitored. Ames Laboratory does not access personal content (e.g., photos, texts, personal email). <i>By using a personal device, you consent to these controls.</i>
Prohibited Usage	Ames Laboratory resources shall not be used for any actions that are illegal, unethical, or inappropriate activities which are expressly prohibited under the code of ethical behavior. Prohibited activities include, but are not limited to: Financial Gain: Using laboratory resources for private or personal for-profit endeavors; engaging in gambling or gaming. Political Activity: Engaging in any prohibited political activity under the Hatch Act. Copyright Compliance: Using, downloading, or distributing illegal copies of copyrighted materials including software, music, or videos; Inappropriate Content: Transmitting or viewing sexually explicit, offensive, abusive, discriminatory, or otherwise objectionable material. This includes browsing websites that are sexually explicit or promote hate; Defamatory Material: Sending any material that is libelous or defamatory; and Any Other Misuse of Government Resources: as specified in DOE O 203.1A.

Category	Rules of Behavior
Social Media	1) Approval and Compliance: Ames Laboratory social media accounts must be approved by the Communications Department and comply with the requirements in DOE ITC 18-04 - Social Media Security. Any Ames Laboratory social media account discovered to be noncompliant with DOE policy, standards, or guidelines will be frozen or terminated. 2) Personal Account Guidelines: Personal social media use must follow DOE' Social Media Security Policy Memorandum. This includes but is not limited to: ▪ Not disseminating non-public information; ▪ Not using official laboratory branding; and ▪ Adhering to the Hatch Act and the Standards of Ethical Conduct for Employees of the Executive Branch. 3) Personal Views Disclaimer: Employees are encouraged to state their social media posts reflect personal views, not those of Ames Laboratory or the United States.
Email	1) Official Business: Employees are required to use their @ameslab.gov email accounts for conducting official business; occasional personal use is authorized. 2) Non-Ames Laboratory Email: When non-ameslab.gov email addresses are used for official business, the email must be copied/forwarded to a laboratory account within 20 business days per the Federal Records Act (44 U.S.C. 2911 as amended by Pub. L. 113-187). 3) Automatic Forwarding Restrictions: Automatic forwarding of Ames Laboratory account to any other account (including iastate.edu), is strictly prohibited unless IT gives prior authorization. 4) Emailing Sensitive Information: Use DOE-mandated encryption procedures (Entrust) when transmitting sensitive information (e.g., CUI, PII) to non-ameslab.gov email addresses. 5) Large Attachments and Chain Letters: Never transmit nonbusiness-related large attachments, chain letters, unauthorized mass mailings, or malware.
Security Training	Mandatory Training: Complete the mandatory Ames Laboratory IT Security and Awareness Training each year.
Reporting	Security Incident Reporting: Employees must promptly report suspected or confirmed security incidents (e.g., lost passwords, improper or suspicious acts) related to laboratory systems or network and breaches of PII/CUI to the IT Help Desk immediately (call 294-8348 or email it@ameslab.gov .)
Recordkeeping	Recording Keeping Compliance: Understand DOE Order 243.1C, Records Management Program , which provides guidance on implementing recordkeeping requirements as both the development and the use of technology may create Federal records.



The Rules of Behavior contained in this document are to be followed by all users of the Ames National Laboratory network.

I acknowledge receipt of the Ames National Laboratory Network Rules of Behavior, understand my responsibilities, and will comply with the Rules of Behavior for the Ames Laboratory Network.

Name (please print clearly)

ISU ID Number

Signature of User

Ames Laboratory Employee #

Date