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 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 8.0 of the Network Rules of Behavior (Form 48400.019), dated 03-06-2024.
3. Explanation of Change.
    a. Updated links and clarified terminology throughout.
    b. Added new information to Section 8 on Recordkeeping.
4. Objectives. To communicate to users of Ames National Laboratory IT resources and applications their responsibilities and expected behavior in safeguarding those assets. This pertains to Government furnished equipment (GFE) and resources or Iowa State University-owned equipment connected to the Ames National Laboratory network unless otherwise specified in Section 8 of this document.
5. Applicability. This policy applies to all Ames National Laboratory employees, contributors, collaborators, and students using Ames National Laboratory IT resources and applications. The Ames National Laboratory IT Network Rules of Behavior applies to users at their primary workplace, while teleworking, at any alternative workplace, and while traveling.
6. Roles and Responsibilities.
    a. Supervisors must ensure their employees who access Ames National Laboratory IT resources and applications comply with this policy.
    b. All Ames National Laboratory employees, contributors, collaborators, students, and subcontractors must acknowledge these IT Network Rules of Behavior by signing this agreement prior to their first use of an Ames National Laboratory IT resource and annually thereafter as a part of required Annual Security Training.
7. Penalties for Non-Compliance. Users will be held accountable for their actions on the network. Users who do not comply with the Ames National Laboratory IT Network Rules of Behavior may have their system access revoked and/or incur disciplinary action. Disciplinary actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

8. IT Network Rules of Behavior. As a person subject to this policy, I agree I:

Category	Rules of Behavior
Personal Use	1) Shall not use Government property for other than authorized purposes, with only limited personal use allowed as described in DOE Order 203.1, Limited Personal Use of Government Office Equipment Including Information Technology. 2) Shall not allow personal use of Ames National Laboratory IT resources to interfere or prevent fulfillment of official duties. 3) Shall only access Ames National Laboratory IT systems or information in performance of official duties. 4) Shall never use Ames National Laboratory IT resources for personal gain, commercial purposes (including endorsement of products), or profit-making activities.
Privacy	1) Per **Clause I.99 of Ames National Laboratory Prime Contract (DEAR 952.204-77), have** no expectations of privacy when using any Government office equipment or services at any time, including email, remote access, business, and personal internet usage as all activities are subject to monitoring. 2) Must protect Personally Identifiable Information (PII), patentable, proprietary and Controlled Unclassified Information (CUI) from unauthorized disclosure, as described in Ames National Laboratory policies, DOE Order 206.1A , Department of Energy Privacy Program, and DOE Order 471.7, Controlled Unclassified information.
Bring Your Own Device	*These rules only apply to personal devices being used to conduct official business:* 1) Shall not store Ames National Laboratory information (e.g., research data, PII, CUI) to personal IT resources (e.g., laptop, mobile device, home computer, removable media, email, cloud storage). 2) Shall keep operating system (OS) patches and antivirus (AV) software running and updated. OS and AV software must be supported (not End of Life). 3) Shall download applications only from trusted sources.
Teleworking	*These additional rules apply to Ames National Laboratory employees approved for teleworking or remote work at any alternative workplace*: 1) Must follow security practices that are the same as or equivalent to those required at primary workplace. 2) Shall physically protect Government furnished equipment (laptop, mobile, desktop, storage device) used for teleworking or remote work against loss, theft, damage, abuse, and unauthorized use, as described in Policy 48300.001, Property Management. 3) Shall protect all Ames National Laboratory data at the alternative workplace.
Passwords	1) Shall ensure all computing devices connected to the network are configured to comply with Ames National Laboratory password policies: ▪ Must be at least eight (8) characters in length and include upper- and lower-case letters, numerals, and special characters. ▪ Must be changed every 180 days. ▪ Must be unique to Ames National Laboratory resources only. ▪ Must not be one used before. ▪ Must not consist of: NetID (username), first or last name, dictionary/common words or names (Betty, Fred, etc.), consecutive strings (abcde, 1234, etc.), simple keyword patterns (asdfh, qwerty, etc.), generic passwords (P@ssword1). 2) Shall protect passwords from disclosure. Never record passwords on paper.

Category	Rules of Behavior
	3) Shall never share passwords or provide to anyone, including system administrators. 4) If plain text passwords must be used (i.e., FTP, Telnet, other legacy applications), shall make my password significantly different from other Ames National Laboratory credentials. 5) Will take the same precautions with passwords used on websites, ISU, and other remote organizations. 6) Shall promptly change a password whenever its compromise is known or suspected to have occurred. 7) Understand that after ten (10) invalid password attempts, user account will be locked out for a period of 30 minutes. If reactivation of a user account is required before the lockout period expires, the user must contact the IT Help Desk in TASF 334 or at 294-8348.
Hardware	1) Shall not acquire, possess, or use hardware or software tools that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files. 2) Shall promptly respond to patching and rebooting requests from Ames National Laboratory IT personnel. 3) Shall protect Ames National Laboratory IT resources in your possession from theft, destruction, or misuse. 4) Shall not add, modify, or remove hardware, or connect unauthorized accessories or communications connections to Ames National Laboratory resources unless specifically authorized. 5) Shall not change any configurations or settings of the operating system and security-related software or circumvent and test the security controls of the system unless authorized through the documented configuration management procedures. 6) Shall ensure that all laptops, mobile devices, and external storage devices used to store Ames National Laboratory data will be protected with FIPS compliant encryption.
Software	1) Abide by software copyright laws and do not obtain, install, replicate, or use unlicensed software. 2) Obtain licensed software through procurement unless otherwise directed. Do not download untrusted software from the internet. 3) Shall not copy or distribute protected intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials). 4) Use only Ames National Laboratory-licensed and authorized software. 5) Understand that KB0016456 Unauthorized Software List By Category provides a list of software applications not authorized or require approval prior to installation and use.
Remote Access	Use approved methods (e.g., Multi-Factor Authentication (MFA), Cisco WebEx, Virtual Private Network (VPN)) to remotely access the network, as described in Remote Work Resources.
Mobile Security	1) Shall not use mobile applications that request Ames National Laboratory network credential unless pre-approved by IT Cyber Security. 2) Shall not bypass native mobile device operating system controls to gain increased

Category	Rules of Behavior
	privileges (e.g., jailbreaking or rooting the device). 3) Carry or store Ames National Laboratory-issued mobile device(s) in a way that prevents theft. 4) When traveling, shall turn off unused radios (i.e., Bluetooth, Wi-Fi, Cellular).
Prohibited Usage	1) Shall never convey any material that is sexually explicit, offensive, abusive, discriminatory, or objectionable. Never browse sexually explicit or hate-based websites. 2) Shall never transmit nonbusiness-related large attachments, chain letters, unauthorized mass mailings or malware. 3) Shall never use copyrighted or otherwise legally protected material without permission. 4) Shall never use Ames National Laboratory IT resources to "snoop" on or invade another person's privacy or break into any computer whether belonging to the Laboratory or another organization. 5) Shall never transmit any material that is libelous or defamatory. 6) Understand that peer-to-peer file sharing (also known as P2P) is not allowed on GFEs or the network. 7) Shall not access software which facilitates behaviors which are expressly prohibited under the code of ethical behavior, such as gaming, gambling, possession or distribution of pornographic materials, unauthorized transmission or sharing of copyrighted material, etc.
Social Media	1) Understand any Ames National Laboratory social media account must be approved by the Communications Department and must abide by the requirements contained in DOE ITC 18-04 - Social Media Security. Any Ames National Laboratory social media account discovered to be noncompliant with DOE policy, standards, or guidelines will be frozen or terminated. 2) Understand that personal social media account usage is also governed by DOE Social Media Security Policy Memorandum, including but 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) Understand that Ames National Laboratory employees are encouraged to use a disclaimer clarifying that their social media communications reflect only their personal views and do not necessarily represent the views of Ames National Laboratory or the United States.
Use of External Sites	1) Shall not re-use network identifiers (e.g., email addresses, usernames) or authentication secrets (e.g., passwords, token codes, PINs) for creating accounts on external sites/applications.
Email	1) Shall use @ameslab.gov email accounts for official business; occasional personal use is authorized. 2) 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) Shall never automatically forward Ames National Laboratory email to a non-Federal email account 4) Use DOE-mandated encryption (e.g., Entrust) procedures when transmitting sensitive information (e.g., CUI, PII) to non-ameslab.gov email addresses

Category	Rules of Behavior
Security Training	Shall complete the required Ames National Laboratory Annual Security Training each year.
Reporting	Shall 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 (or contact via 294-8348 or email it@ameslab.gov.)
Recordkeeping	Understand DOE Order 243.1C, Records Management Program, provides direction 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 IT Network Rules of Behavior, understand my responsibilities, and will comply with the Rules of Behavior for the Ames National Laboratory network.

Name of User

ISU ID Number

Signature of User

Ames Laboratory Employee #

Date