

## AMES LABORATORY NETWORK RULES OF BEHAVIOR

Ames Laboratory, a government-owned, contractor-operated facility, located on the Iowa State University campus, conducts theoretical and experimental research for the United States Department of Energy (DOE) under contract number DE-AC02-07CH11358. The official Ames Laboratory policy regarding computer usage conforms to Federal law, rules and regulations, and DOE requirements.

All computing resources within the Ames Laboratory production network are intended for the use of work authorized by the U.S. Government. All software used on computers within the Ames Laboratory production network must abide by all software licensing restrictions. Virus protection and precaution is required on end user computing devices. Creation and use of federally classified programs or files are not authorized on any Ames Laboratory computing resource, as all work here is unclassified.

### Protection of Resources from Theft, Damage, Viruses and Loss of Data

All use of Ames Laboratory computing resources must include reasonable effort to ensure resources are protected from theft, damage, viruses and data loss. To ensure protection:

- Be aware of social engineering such as e-mail scams, suspicious phone calls and unexpected mailings. Report these types of activities to the Assistant Cyber Security Manager (ACSM) or Information Systems (IS) Office ([abuse@ameslab.gov](mailto:abuse@ameslab.gov)).
- Lock computer systems when not in use.
- Report suspicious activity or system behavior to the ACSM or to IS.
- Guard accounts credentials carefully and choose passwords that are difficult to guess.
- Follow appropriate baseline configuration guidelines. This includes installing all system updates and patches and running up-to-date virus and spyware protection software.

### Protection of Copyright Licenses (Music or Software)

Allowing others to illegally copy or use copyright material (music or software) makes a user subject to laws such as the NET Act. Under the NET Act, it is a crime to make copyright material valued at more than \$1000 available to others, even if the material is made available without charge (see <http://www.justice.gov/criminal/cybercrime/>).

Software download and use is allowed for authorized Ames Laboratory work and limited personal use as outlined below. All software downloaded or obtained through other means must be used in accordance with the license terms. Peer to peer file sharing software, such as Kazaa, Gnutella, Bear share and others should not be used without prior authorization through the Information Systems Office.

Network activity logs will be reviewed to determine whether employees attempt to illegally download copyrighted materials.

### Unofficial Use of Government Equipment

While limited personal use of equipment is permitted, users should be aware that use of network resources for the following activities is **not** authorized:

- Accessing pornographic web sites and material
- Developing applications for personal gain



- Illegally downloading copyrighted material
- Accessing other offensive or questionable material
- Performing personal activities that may cause congestion, delays or disruptions of service to others
- Downloading software or modifying system configurations to bypass stated cyber security controls or policy, unless IS has been notified and has approved such activity.

Periodic waste, fraud and abuse reviews on all Ames Laboratory computers and network resources will be conducted to ensure that software and the usage of the computer comply with the above. Any unauthorized files found may be purged and misuse reported to the employee's supervisor, ACSM and Cyber Security Manager (CSM).

### **Work from Home or Alternate Sites**

Ames Laboratory directors, program directors and office managers can designate specific employees (e.g., critical job series, employees on maternity leave, or employees with certain medical conditions) as eligible for working from home. Any work from home arrangement should:

- Be in writing,
- Identify the time period the work from home will be allowed,
- Identify the government equipment and supplies needed by the employee at home and how the Laboratory and employees will transfer and account for the equipment and supplies,
- Identify telecommuting requirements (If telecommuting is authorized, a remote access account will need to be obtained from IS.), and
- Be reviewed by Ames Laboratory Human Resources Office prior to commencement.

### **Remote Access**

Remote access is obtained by requesting a remote access account. The form is available by contacting IS. It is understood that remote access can pose additional security risks, but is necessary for certain job functions. IS has access to logs and will review the logs and phone records as necessary when questions arise on the use of remote access accounts.

Users should verify that the off-site system they are using to gain access to Ames Laboratory complies with at least the following limited baseline guidelines:

- A current virus-scanner is installed and is kept up to date,
- The system uses a supported operating system and is up-to-date, and
- Any client software which will be interacting with Ames Laboratory systems is securely configured according to vendor documents and available best practices.

### **Connection to the Internet**

Most Ames Laboratory personnel have access to the Internet. Access to the Internet is controlled by IS.

- For general access, a request for an IP address needs to be authorized, and system baseline configuration guides must be followed prior to accessing the network.
- For external access to an Ames Laboratory device, an Internet Accessible System Authorization form must be completed. Requestors must indicate the IP address, host name, operating system and open ports for the Internet accessible system. All system administrators must apply

appropriate patches prior to external access. Periodic scans will be conducted on the externally accessible systems.

- Internal systems will be scanned daily for vulnerabilities.

### **Use of Passwords**

Password features include

- At least 8 characters in length and including the following character classes:
  - At least 1 digit, not in the first or last position
  - At least one upper case character
  - At least one lower case character
  - At least one special symbol
- Is not based upon the User ID or other public user information
- Is not based upon common words that would be in a dictionary

Users must keep passwords confidential and not share passwords with anyone.

If plain text passwords must be used, for instance with FTP, Telnet, and other legacy applications, ensure that the password is significantly different from other Ames Laboratory credentials. The same precautions must be taken with passwords used on web sites, Iowa State University and other remote organizations. The Ames Laboratory password should be unique to Ames Laboratory resources only.

### **System Privileges**

Users are given access to the network based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

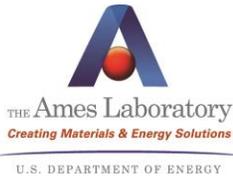
Programs and files utilizing private personnel information or proprietary information (moderate information) may be accessed only on Ames Laboratory computer resources. Moderate data should not be recorded on personal computer media. Unauthorized disclosure of moderate data should be avoided when Ames Laboratory employees work on patentable scientific projects or private personnel information.

### **Individual Accountability**

Users will be held accountable for their actions on the network. If an employee violates Ames Laboratory policy regarding the rules of the network, they may be subject to disciplinary action at the discretion of Ames Laboratory management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, to termination, depending on the severity of the violation.

### **Restoration of Service**

The availability of the network services is a concern to all users. All users are responsible for reporting problems with network connectivity to IS (4-8348). In the event that network devices or services are not operational, IS staff can effectively address the network issue to ensure the timely restoration of services.



### **Social Media/Networking Access**

- When accessing social media/networking and public websites, take all necessary precautions to protect Ames Laboratory information assets including, but not limited to, hardware, software, personally identifiable information (PII), and moderate level data from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse and treat such assets in accordance with any DOE or Ames Laboratory information handling policies.
- Professional social media/networking communication should be in compliance with existing Ames Laboratory and DOE policies and applicable laws. Harassing, obscene, discriminatory, defamatory, or threatening language are strictly prohibited.
- Ames Laboratory employees should use privacy settings to control access to their professional social media/networking sites to ensure only professional social media/networking communications only reach the intended audience.

### **DEAR Clause Compliance**

An individual accessing the Ames Laboratory network:

- Has no expectation of privacy in the use of a DOE computer.
- Consents to permit access by an authorized investigative agency to any DOE computer used during the period of access to information on a DOE computer, and for a period of three years thereafter.

### **More Information**

For more information about cyber security policies, procedures, forms, or other concerns, contact the IS office at 4-8348 or [is@ameslab.gov](mailto:is@ameslab.gov)

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

**I acknowledge receipt of the Ames 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)

\_\_\_\_\_  
Iowa State University ID Number

\_\_\_\_\_  
Signature of User

\_\_\_\_\_  
Ames Lab Employee Number

\_\_\_\_\_  
Date