Ames Laboratory Network Rules of Behavior
Introduction

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 under contract number DE-AC02-07CH11358. The official Ames Laboratory policy regarding computer usage conforms to Federal law, rules and regulations, and Department of Energy requirements.

All Ames Laboratory computer resources are for the sole use of Ames Laboratory in the performance of work authorized by the U.S. Government. All software used on Ames Laboratory computers must be for authorized Ames Laboratory work and abide by all software licensing restrictions. Virus protection and precaution is required on desktop devices, and encouraged on server devices. Creation and use of Federally Classified programs or files are not authorized on any Ames Laboratory computing resource, as all work here is Non-Classified.

Protection of resources from Theft, Damage, Viruses and Loss of Data

All use of Ames Laboratory computing resources must include reasonable attention to ensure that these resources are protected from theft, damage, viruses and data loss. This includes such actions as:

- Be aware of social engineering such as e-mail scams, suspicious phone calls, and unexpected mailings. Report this activity to the ACPM or Information Systems office.
- Log off of a system when not in use.
- Report suspicious activity or system behavior to the ACPM, or the Information Systems office.
- (1) Guard account credentials carefully, and choose difficult to guess passwords.
- Follow appropriate baseline configuration guidelines, including 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.cybercrime.gov/iplaws.htm#Xb).

Generally, 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

- Access pornographic web sights and material.
- Develop applications for personal gain.
- Illegally download copyrighted material.
- Access other offensive or questionable material.
- Perform personal activities that may cause congestion, delays or disruptions of service to others.
- Download software or modify system configurations to bypass stated cyber security controls or policy, unless the Information Systems office 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, ACPM (Assistant Computer Protection Manager) and CPPM (Computer Protection Program Manager).

Work at 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 at home. Any work at home arrangement should:

- Be in writing.
- Identify the time period the work at 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 the Ames Laboratory Information Systems (IS) Office.
- Be reviewed by Ames Laboratory Human Resources Office prior to commencement.

Everyone must abide by all known Ames Laboratory cyber security policy and procedures and additional cyber documentation on the cyber web page. http://www.internal.ameslab.gov/is/security

Remote access

Remote access is obtained by requesting a remote access account (SSH, VPN, or modem/dial-up). The form is available at the Ames Laboratory Information Systems office internal web site (http://www.internal.ameslab.gov/is/forms/newacct.htm) or by contacting the IS office. It is understood that remote access can pose additional security risks, but is necessary for certain job functions. The IS office 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.
- Current anti-spyware is employed and up to date (for Microsoft Windows systems).
- The system is reasonably maintained, and patches and updates are installed.
- Any client software which will be interacting with Ames Laboratory systems (ie. X-Win 32, SSH client) 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 the IS Office.

- 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 (http://www.internal.ameslab.gov/is/security/baselines/).
- 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 and all high vulnerabilities on high risk systems need to be addressed within 30 days. All moderate vulnerabilities must be addressed within 80 days.
- Internal systems will be scanned daily for vulnerabilities. High and moderate vulnerabilities on sensitive systems need to be addressed within 30 business days of discovery.
- For wireless access, the requestor must register the MAC address of the wireless device with IS on the "Request for IP Address" form.

Use of Passwords

Password features include

(2) (3) (4) (5) (6) (7) (8) (9)

- 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 UserID 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

(10) 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 (sensitive information) may be accessed only on Ames Laboratory computer resources. Sensitive data should not be recorded on personal computer media. Unauthorized disclosure of sensitive 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, or 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 the Information Systems (IS) Office (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 service.

More Information

For more information about cyber security policies, procedures, forms, or other concerns, see the internal Cyber Security web page at: http://www.internal.ameslab.gov/is/security/.

The Rules of Behavior contained in this document are to be followed by all users of the Ames Laboratory network. I acknowledge receipt of Rules of Behavior, understand my responsibilities, and will comply with the Rules of Behavior for the Ames Laboratory Network (ALNET).

_____

Name (please print clearly)

_____ _____

Signature of User Date