

Cyber Security Awareness Training

The requirement to develop a computer protection program is detailed in DOE Order 205.1A. Cyber security processes must be integrated into management and work practices at all levels for all staff to protect cyber assets under their control.

The Ames Laboratory Cyber Security Program is described in the Cyber Security Protection Plan at: https://wiki.internal.ameslab.gov/wiki/Cyber_Policies_and_Procedures

Roles and Responsibilities

Directors/Associate Directors: ultimate responsibility for the Laboratory's cyber security program and establishing the program's overall goals, objectives and priorities.

Cyber Security Team: day-to-day management and implementation of the cyber security program.

Assistant Computer Protection Managers (ACPM): act as the program/office point of contact for computer security and directs the day-to-day management of the cyber security program in his/her respective area.

Group Administrators: manage multiple computers and direct the day-to-day management of the cyber security program within their group.

Privileged Users: administer their own systems, including patch and configuration management.

Users: directly interact with computing systems to perform Ames Laboratory work. Users are responsible for following security procedures, reporting security problems, and completing required computer security training.

Cyber Security Highlights

User Accounts

Central accounts through the IS office provide access to PCs, e-mail, remote connectivity, central file storage, and other services. Each user maintains their account and password for system access.

A password is a key to Ames Laboratory computing resources, just as a door key provides access to buildings, and should be protected at all times.

The DOE requires that passwords:

- Be at least 8 characters long.
- Not be based on the username or a dictionary word.
- Be changed every 180 days, or when a compromise is suspected.
- Contain mixed case, symbols, and digits.
- Contain a nonnumeric character in the first and last position.

Different passwords should be used to access other Internet resources (i.e. an ISU or hotmail account). For users with multiple passwords, the use of a cryptographic password safe is recommended (see <http://passwordsafe.sourceforge.net/>).

When a user leaves, all accounts used by that individual must be disabled. E-mail may be forwarded upon request for up to 90 days.

Baseline Configuration

All computer systems that reside on the Ames Laboratory network are required to apply baseline settings. Baseline guides for supported OSES are available at: https://wiki.internal.ameslab.gov/wiki/Baseline_Guides

Baseline requirements include, at minimum, the use of Antivirus software (freely available from ISU), Anti-spyware software (for Windows systems), and installation of current vendor patches for operating systems and applications. If a system is in use, but no longer supported by the vendor, it must be isolated from other Ames Laboratory computers and monitored more closely. Contact the IS department for more information on securing legacy systems.

Systems are required to join the AMESLAB-IOWA domain for Windows systems, or run configuration agents (for Linux and Mac systems) described in the baseline guides.

Pre-baselined systems are available to all users from the storeroom. Administrative users must purchase these systems or provide justification outlining why the provided systems are not sufficient.

Certain exceptions can be made for specific cases using the Baseline Guidelines Exception form at http://www.ameslab.gov/files/forms/Form_48400.025_Rev0.pdf

Configuration Management

Users are responsible for ensuring that changes to the system do not diminish security and that changes to the system are reflected in system documentation. This includes activities such as installing third party software, providing physical system access to others, and installing or configuring hardware devices.

Contingency Plans and Backups

Users should document the procedures, equipment, and personnel necessary to recover computing capabilities and data in the event that computer system operations are disrupted.

Significant computing resources should have a written contingency plan including system backup details, a system recovery checklist or guide, key personnel, and

up to date system configuration data (e.g. key applications, important configuration settings, and anything that would need to be re-established to recover the computing resource).

Backups are critical to contingency preparedness. Backups should be stored securely and periodically tested for usability. It is important to differentiate data which should be backed up from data considered temporary, or an acceptable loss.

All users need to plan for contingencies to enable the speedy recovery of data and to minimize the negative impact on Ames Laboratory systems. Contact the IS office for information on centrally available data backup options or for assistance in writing a contingency plan.

Mobile Devices and Portable Storage

Users of mobile devices (e.g. laptops, PDAs) and portable media (e.g. USB keys) are responsible for the security of these devices when used in other environments. Users are encouraged to make complete backups of data prior to travel, and to utilize central imaging and scanning facilities for laptops and removable media.

Pre-verified USB keys are available from the storeroom for purchase. Use of other USB keys is also permitted with approval on a case-by-case basis. A USB scanning station is available in the IS office.

Login Banners

The DOE requires login banners on all interactive access points (e.g. console login, SSH, and web site access) and on all non-interactive access points that provide a human readable response. Banners are displayed prior to system resource access, and users must acknowledge compliance before accessing those resources. Systems which do not support pre-login banners must display a warning at or immediately after login. If electronic banners and warnings are not supported at all, clearly visible printed banners may be used for console access.

The approved warning banner is available at: https://wiki.internal.ameslab.gov/wiki/Banner_Text Printed banner stickers may be obtained from the IS office.

Physical Security

Ames Laboratory is an open campus with unlocked buildings during the day. Students and the general public may use buildings at any time. It is important the computers and data are secured. For instance, locking office and laboratory doors if unattended, and ensuring that computer screens are password protected when users are not at the terminal.

Sensitive and Personally Identifiable Information

Users are responsible for the identification and safe handling of Sensitive but Unclassified Information (SUI) and Personally Identifiable Information (PII). These data types include projects covered by Non-Disclosure Agreements (NDA's), Work for Others confidentiality agreements, Official Use Only, and data including personal information such as Social Security Numbers, medical data, birth date, and other non-public information on individuals.

Network and Internet Access

Network access is provided to users and visitors upon request. To request network access, use the IP request form available from the IS office.

All network users are required to agree to, sign, and return the Rules of Behavior located at:

https://wiki.internal.ameslab.gov/wiki/Cyber_Policies_and_Procedures

In addition, foreign national network users must submit a Foreign National Access Request form (available from the IS office) listing the computing resources they will be using.

Appropriate Use of Computer and Network Resources

The DOE grants employees permission to use computing resources for limited personal use provided that such activity is not for personal financial gain, illegal, or detrimental to Ames Laboratory's mission.

Specifically, users may not:

- Access pornographic web sites and material,
- Develop applications for personal gain,
- Illegally download copyrighted material,
- Access potentially offensive material,
- Perform personal activities that cause congestion, delays or disruptions of service to others.
- Install applications which are considered dangerous, including peer to peer (P2P) software, vulnerability scanning tools, and other software listed at:
https://wiki.internal.ameslab.gov/wiki/Authorized_Software_Tiers

As indicated in the login banner, users of computer and network resources do not have a right to, or expectation of, privacy at any time, including when they are accessing the Internet applications such as social networking sites or personal e-mail.

In addition, while activities such as the use of social networking sites, online radio, or chat programs are not prohibited, users may be asked to limit such activity if they expose the laboratory to elevated risks.

If circumstances create a need for an exception from these constraints, contact the IS office.

Computer Software License Agreements

It is the responsibility of each computer user to follow

the licensing agreement of all software that is being used and to keep documentation, sales receipts, original diskettes, purchase orders, registration certificates, etc., proving the software was purchased legally. It is illegal to make or use unlicensed copies of software. Ignorance is no excuse under the Copyright Protection Act. Violation of licensing agreements is punishable by fines and/or imprisonment. It is Ames Laboratory's policy to adhere to all copyright agreements of software owned by or used by Ames Laboratory personnel.

Cyber Security Incidents

A Cyber Security Incident is defined as an adverse event that threatens the security of information resources. Incidents must be reported immediately to a group administrator, ACPM, or the IS office with your name and computer system's IP address (similar to 147.155.xxx.xxx). An investigative team will examine the system, acquire an image, and provide further assistance to facilitate data and system recovery.

Examples of reportable Cyber Security Incidents include:

- Compromise/Intrusion: Intentional or unintentional instances of system compromise by unauthorized users.
- Malicious Code: Instances of malicious code such as viruses, Trojan horses, or worms.
- Unauthorized Use: Use of a computer to obtain data without authorization, obtaining or using illegal material, or hacking.
- Loss or Theft: The physical loss or theft of any computer system; the loss or theft of digital media containing Sensitive but Unclassified Information (SUI).
- Information Compromise: Any unauthorized disclosure of information.

Additional information on handling and reporting cyber security incidents is available at:
<http://www.internal.ameslab.gov/is/security/training/>

How to Recognize a Cyber Attack

Signs indicating a computer system is under attack may include unusually sluggish or non-responsive applications, unexpected changes in system behavior, and missing or corrupt data. When a cyber attack is suspected, report the incident to your group administrator, ACPM, or the IS office.

Phishing attacks and other forms of social engineering are also cyber attacks. Unexpected e-mails or phone calls, unsolicited CVs, resumes, or requests for information should all be reported to abuse@ameslab.gov. Any publicly available information may be used to make a message appear legitimate, including logos, personal e-mail addresses, and official documents. A social engineering training course is recommended, call 4-9972 to register.



THE Ames Laboratory
Creating Materials & Energy Solutions

U.S. DEPARTMENT OF ENERGY

CYBER SECURITY GUIDE

NOTE

This guide, supporting documents, and reference materials are available at the Ames Laboratory IS Office, 334 TASF, Ames Laboratory, Iowa State University, Ames IA 50011. Please call the IS Help Desk (4-8348) for more information on the topics covered in this guide.

Guide No. 50000.001 Rev. 12 11/10