INFORMATION TECHNOLOGY SECURITY

TABLE OF CONTENTS

I. POLICY 2
- A. What does this policy do? 2
- B. What is the AMS policy on computer security? 2

II. GENERAL SECURITY REQUIREMENTS FOR AMS USERS 2
- A. As a user of AMS computer information systems, what security requirements must I follow? 2
- B. Why is computer security so important? 2

III. SECURITY AWARENESS AND TRAINING REQUIREMENTS 2
- A. What are the security awareness and training requirements? 2
- B. How often must I take security training? 3
- C. How do I get security awareness training? 3

IV. USERNAME AND PASSWORD REQUIREMENTS 3
- A. What is the AMS policy on selecting passwords? 3
- B. May I share my username with someone? 3
- C. May I share my password with someone? 4
- D. How often should I change my password? 4
- E. Whom should I contact about getting an NFC or NITC username and password? 4
- F. Whom should I contact about NFC or NITC password problems? 4
- G. How does the AMS ensure that separated employees and contractors no longer have access to agency IT systems? 4
- H. How does AMS ensure that employees and contractors only have the access privileges necessary to perform their duties? 5

V. SECURING COMPUTERS CONNECTED TO THE NETWORK 5
- A. Are there any special security practices I must follow if my computer is connected to the AMS network? 5
- B. Can exceptions be made if a security practice jeopardizes an essential business function? 5
- C. Who ensures that all appropriate software patches and updates are applied to my computer? 6
- D. What special requirements are there for servers that host systems with a life-cycle cost of one million dollars or more or with critical or sensitive information? 6

VI. RESTRICTIONS ON THE USE OF SOFTWARE AND HARDWARE 7
- A. What are my responsibilities regarding the use of Government office equipment? 7
- B. What is copyrighted software? 7

C. What restrictions are there on the use of copyrighted software? 7
D. What is an IT Restricted Space? 7
E. How do I secure an IT Restricted Space? 7

I. POLICY

A. What does this policy do?

This policy provides AMS employees with direction concerning information technology (IT) security and ensures that employees are aware of the required security methods to protect AMS IT assets. You must comply with this policy if you have access to AMS IT resources.

B. What is the AMS policy on computer security?

All AMS employees, Federal or contractor, are required to protect the confidentiality, integrity, and availability of Federal Government IT resources.

II. GENERAL SECURITY REQUIREMENTS FOR AMS USERS

A. As a user of AMS computer information systems, what security requirements must I follow?

If you have access to or use the AMS computer system, you must follow the procedures in this policy. These include taking the required security training, properly handling sensitive data, and protecting copyrighted software.

B. Why is computer security so important?

A security breach on one AMS computer can potentially compromise the entire AMS network. As long as the AMS computers are attached to the Internet, they are at risk and will be attacked. We must all take the necessary precautions to defend against these attacks. If everyone does their job in protecting our AMS information assets, we will be less vulnerable to these attacks. Attacks can range in severity from being a nuisance to a complete shutdown of the AMS network, leading to a significant loss in productivity, time, and money.

III. SECURITY AWARENESS AND TRAINING REQUIREMENTS

A. What are the security awareness and training requirements?

The Computer Security Act of 1987 and OMB Circular A-130 require AMS to provide periodic training in computer security awareness and accepted computer security practices for all employees who manage, use, or operate a Federal computer system. This includes contractors as well as AMS employees.

B. How often must I take security training?

Before you receive a username to access the AMS wide area network, you must submit a signed certification statement verifying that you have read and understand the requirements in this Directive and the requirements in AMS Directive 3300.1, Use of Government Office Equipment. You must also agree to complete follow-on security awareness training provided by the Information Technology Group (ITG) within 60 days of receiving network access.

You are required to take refresher security training as determined necessary by the Agency, typically at least once each calendar year. Other security training may be necessary when there is a significant change in the Agency's information security environment or procedures, or when you enter a new position that has different security clearance requirements.

C. How do I get security awareness training?

Contact your Program Area Security Representative or, if not available, the AMS Information Systems Security Program Manager (ISSPM). The ISSPM will provide training materials and monitor completion of this training. The list of Program Area Security Representatives can be found on the AMS intranet security site.

IV. USERNAME AND PASSWORD REQUIREMENTS

A. What is the AMS policy on selecting passwords?

1. Use unique passwords with a minimum length of eight characters and a maximum length of 14 characters. At least one character should be numeric.

2. Do not use passwords that are easily associated with you, such as your name, Social Security number, tag number, telephone number, street address, username, spouse, significant other, child, or pet.

3. Do not use passwords that contain common words from an English dictionary or a dictionary of another language with which you are familiar.

4. Do not use passwords that contain commonly used proper names, including the name of any fictional character or place.

5. Do not use passwords that contain any simple pattern of letters or numbers such as "abcdefgh" or "12345678."

6. Do not use a password that you have used before. NOTE: The operating system will not allow you reuse of one of your previous five passwords.

B. May I share my username with someone?

No. A unique username must be established for each individual user.

C. May I share my password with someone?

No. You may not share your password with anyone. If someone gains access to your password, change it immediately. Additionally, you need to take the following precautions to help avoid a possible compromise of your password:

1. Do not write your password down, such as on a post-it-note stuck to your monitor, or on any electronic device, except when logging in.

2. Do not type a password while anyone is watching. This will prevent an unscrupulous person from seeing your password. This is called shoulder surfing.

D. How often should I change my password?

1. You should change your password every 90 days or less.

2. You must change your password whenever you believe that your password has been compromised (seen or used by someone else).

E. Whom should I contact about getting an NFC or NITC username and password?

Contact your supervisor. Your supervisor will forward the request to your Administrative Office, who will forward the request to the AMS Client Security Officer in the Technical Resource Center (TRC) (202-720-1111). The AMS Client Security Officer is the Agency liaison with the National Finance Center (NFC) and the National Information Technology Center (NITC) and will forward the request on to the appropriate Center. When the Client Security Officer receives the username and temporary password from NFC or NITC, he or she will forward them along to the requestor in the Program's Administrative Office, who will then forward them along to you. You will be prompted to change your temporary password the first time you log on to the system.

F. Whom should I contact about NFC or NITC password problems?

Contact the AMS Client Security Officer in TRC (202-720-1111).

G. How does AMS ensure that separated employees and contractors no longer have access to Agency IT systems?

Program Area Security Representatives are responsible for ensuring that separated employees and contractors no longer have access to Agency IT systems. Program Area Security Representatives are responsible for ensuring that the username of a separated employee or contractor is suspended or deleted at the time of the person's departure. NOTE: ITG will perform monthly reviews of AMS network system accounts and suspend all accounts that have not been accessed for 30 days. These accounts will be referred to the appropriate Program Area Security Representative for validation.

H. How does AMS ensure that employees and contractors only have the access privileges necessary to perform their duties?

Program Area Security Representatives are responsible for conducting annual reviews of user access levels to Program, Agency, and Departmental information systems to ensure that employees and contractors only have those access privileges necessary to perform their duties. ITG will send annual notices to the representatives to remind them when it is time to perform these reviews.

V. SECURING COMPUTERS CONNECTED TO THE NETWORK

A. Are there any special security practices I must follow if my computer is connected to the AMS network?

Yes. Because the AMS network is directly connected to the Internet, AMS employees must follow several key practices to protect their systems. These are:

1. Computers (all workstations, laptops, and servers) connected to the AMS network must have an approved anti-virus program installed and running with current virus data definition files. System Administrators are responsible for setting up the automatic updates to these files.

2. Computers (all workstations, laptops, and servers) connected to the AMS network **must not** run Internet-aware hosting services, such as a Web service (Internet Information Service [IIS]), e-mail services (SMTP), or file hosting services (File Transfer Protocol or services similar to Napster).

3. Computers (all workstations, laptops, and servers) connected to the AMS network by a local area network **must not** also have a modem connected to a public phone line. However, computers at a remote worksite may use a modem and a public dial-up phone line to access the AMS network through the AMS virtual private network (VPN) service.

4. Computers (all workstations, laptops, and servers) connected to the AMS network must use one of the Agency's standard operating systems as specified by AMS Directive 3130.5, Information Technology Standards. This directive can be found on the AMS intranet site.

B. Can exceptions be made if a security practice jeopardizes an essential business function?

Yes. If an essential business function requires an exception to one or more of these security practices and the security risks can be appropriately mitigated, the AMS Chief Information Officer (CIO) can grant a written waiver. Requests for waivers must be submitted to the CIO in writing from the Program that operates the computers which require the waiver. The request shall describe the business function that requires the exception, the measures taken by the Program to minimize security vulnerabilities, and the Program's plans and timeline to eliminate the exception and comply with the standard security practices. If you feel that the waiver request

should be indefinite and the elimination of the exception should be waived, you must provide this justification in your waiver request.

C. Who ensures that all appropriate software patches and updates are applied to my computer?

Program Area Security Representatives are responsible for ensuring that monthly scans of your Program's computers are accomplished using special Agency-owned security tools in order to identify and eliminate all vulnerabilities due to insufficient patching and updating. If a vulnerability is identified and eliminated, they must perform a follow-up scan to ensure that the vulnerability has been successfully removed. They will then document all detected vulnerabilities and the corrective actions taken in an on-line tracking system.

D. What special requirements are there for servers that host systems with a life-cycle cost of one million dollars or more or with critical or sensitive information?

1. System Administrators must enable logging features and perform weekly reviews of audit logs on those servers, or use automated server management tools that provide equivalent capability.

2. Program Area Security Representatives must coordinate and prepare annual security plans for these servers in accordance with the Department's Cyber Security Manual, Series 3500, CS-002 Annual Information Cyber Security Plan

3. All personnel responsible for making changes on these systems (e.g., application upgrade, OS patches, etc.) must document the items listed below, ensure appropriate segregation of duties in the change process, and receive all appropriate management and program technical approvals for the proposed changes prior to making them.

<u>CHANGE MANAGEMENT CHECKLIST</u>

- Requestor of the change
- Description of the change
- Reason for the change
- Impact on customers during implementation
- Date and time the change is scheduled
- Is there a system outage required? If so, what is the duration of the outage?
- Will users be notified in advance of the proposed change? If so, how and when will they be notified?
- What are the risks associated with the change -- what problems or symptoms are likely if the implementation is not successful?
- Who will test the change? How will it be tested?
- Who will review the test results?
- Describe the procedures for implementing the change
- Describe the back-out procedures for the change (briefly describe each back-out strategy in order of priority of use)

- Impact on customers if implementation is successful
- Impact on customers if back out is necessary

VI. RESTRICTIONS ON THE USE OF SOFTWARE AND HARDWARE

A. What are my responsibilities regarding the use of Government office equipment?

Essentially, you must use Government equipment for Government business only. For detailed information, see AMS Directive 3300.1, Use of Government Office Equipment, on the AMS intranet site.

B. What is copyrighted software?

Copyrighted software is software that is provided under licensing agreements as authorized by Title 17 of the U.S. Code. Section 106 of this Title gives copyright owners exclusive rights to reproduce and distribute their material. Section 504 states that copyright infringers can be held financially liable for damages to the copyright owner. Title 18, U.S. Code, Section 2319 also imposes criminal penalties for some types of software copyright violations.

C. What restrictions are there on the use of copyrighted software?

Copyrighted software must be used in accordance with the license agreement. A valid license must be purchased for all commercially available copyrighted software used on an AMS system.

D. What is an IT Restricted Space?

This is an IT facility that contains critical network hardware or essential Agency information systems, such as the AMS Server Room.

E. How do I secure an IT Restricted Space?

You must secure these locations in accordance with Cyber Security Manual, Series 3500, Cyber Security Guidance on Physical Security in USDA Information Technology (IT) Restricted Space, CS-005 – Revised. This includes ensuring that controls are in place to limit physical access to authorized AMS employees and contractors that have a recurring business need for access. All visitors and non-AMS individuals requiring access to one of these locations must have appropriate identification and be accompanied by an authorized AMS employee during their visit.

/s/

A. J. Yates
Administrator